

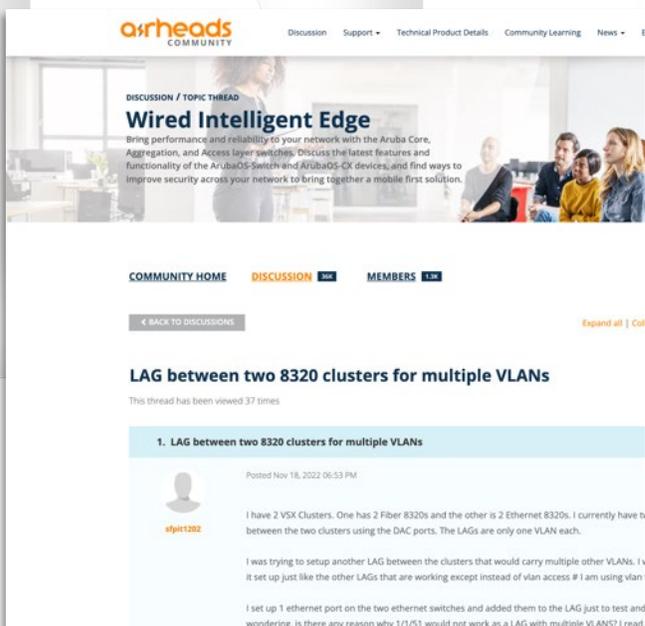
atmosphere'23

BELGIUM

CX Switching Application Recognition and Control

Vincent GILES, Distinguished Technologist

October 29th, 2023



arheads

COMMUNITY

Join Today!

www.community.arubanetworks.com

Agenda

1 Aruba CX Edge Insights Overview

2 Application Recognition

3 IPFIX

4 Traffic Insight

5 Application-Based Policy

Aruba CX Edge Insights Overview

The background of the slide features a complex, abstract pattern of overlapping white shapes. These shapes, which resemble stylized letters or geometric forms, are layered to create a sense of depth and movement. Each shape has a soft, grey drop shadow, making it appear as if it's floating above the others. The overall effect is a clean, modern, and dynamic visual backdrop.

Aruba CX Edge Insights

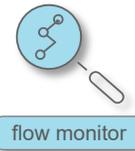
Application Recognition

- Application identification with DPI engine
- set the app-id in the IP flow table



IP Flow Information Export (IPFIX)

- Record and export flow information
- include the application information (when app-recognition enabled)
- Export to external collector and/or to traffic-insight



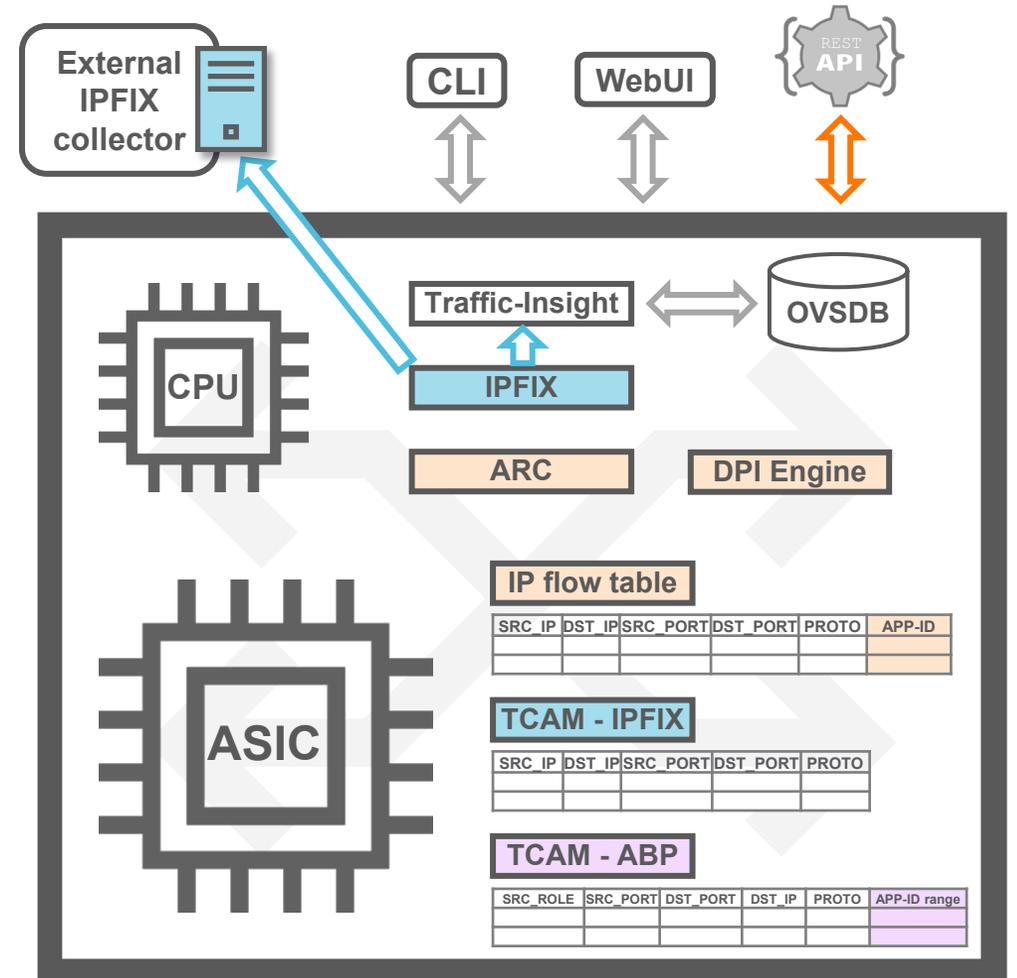
Traffic-Insight

- Collect and aggregate IPFIX data
- Extract and report topN talkers and app-flows
- CLI and webUI display.
- Flow Telemetry API
- Client-Insight (DNS latency)



Application-based Policy

- Allow or block specific applications identified by ARC per authenticated user access role



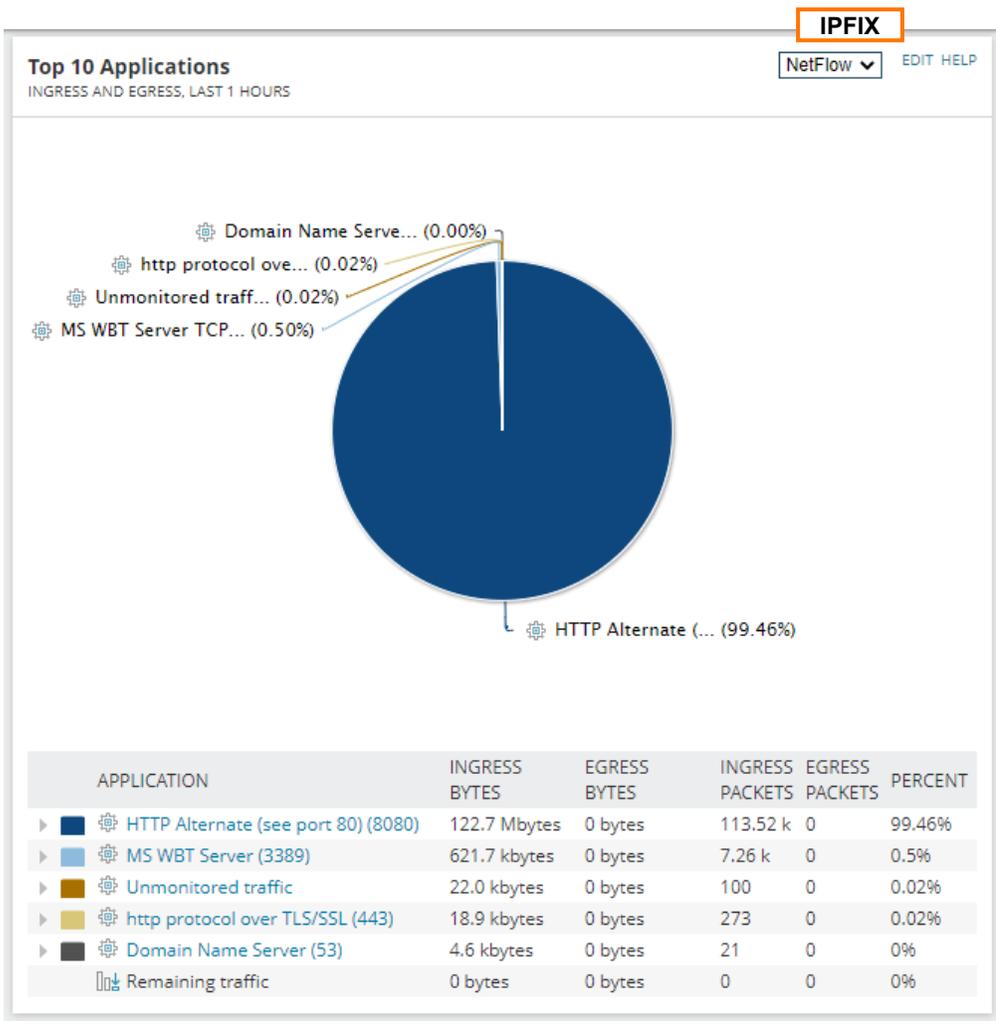
Aruba CX Edge Insights

	Supported platforms	Application Recognition	App-based Policy	IPFIX	Traffic Insight	Results / Outcomes
➔ 1	6300/6400	●	●	●	●	Best experience for application analytics reporting and application filtering.
2	6300/6400	●	●	●		Application visibility report to external collector and application filtering.
3	6300/6400	●	●			Application filtering.
4	6300/6400	●				No operational outcome: troubleshooting only
➔ 5	6300/6400	●		●	●	Best experience for application analytics reporting.
6	6300/6400	●		●		Application visibility report to external collector.
7	6300/6400		●			Invalid use-case (app-recognition must be enabled for DPI)
8	6300/6400/8100/8360			●		IPFIX traditional reporting to external collector (well-known ports, no app-id)
9	6300/6400/8360			●	●	IPFIX traditional reporting to external collector and internal analytics reports (well-known ports, no app-id). (DNS-only TI monitor on 8360).
10	6300/6400/8360				●	No outcome as TI requires IPFIX.

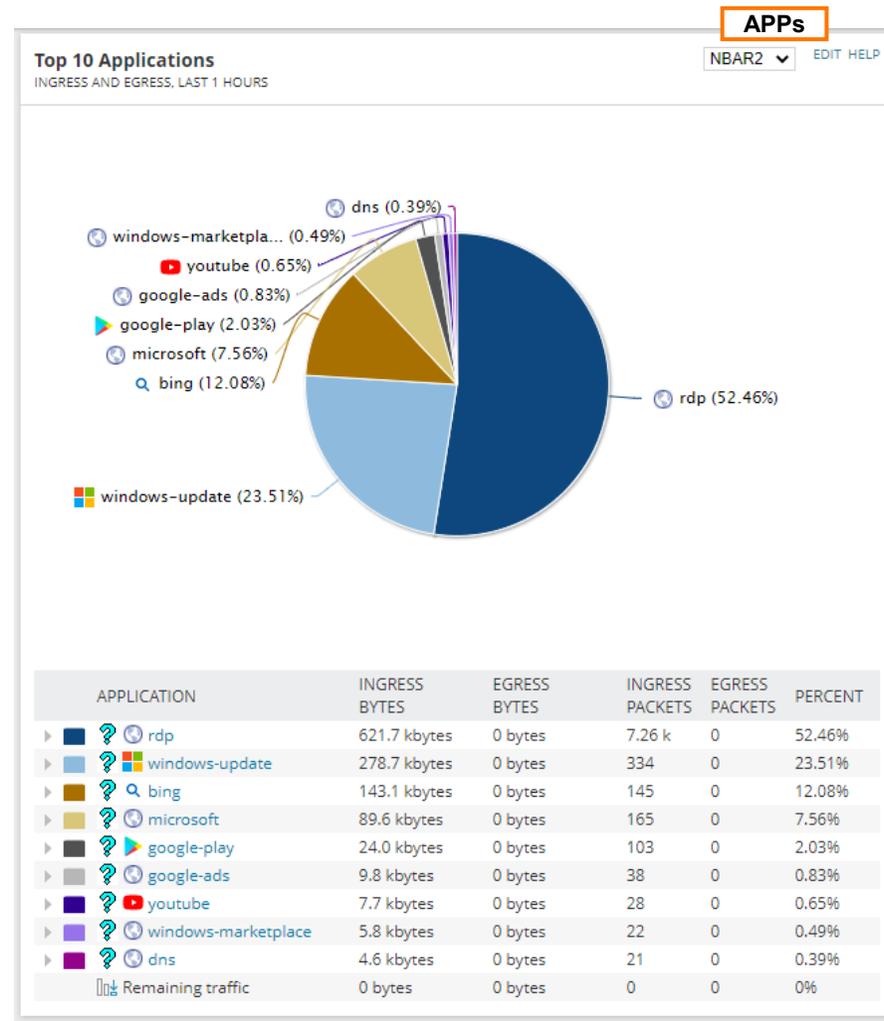
- Aruba CX Edge Insights in AOS-CX 10.11 provides, with **Application Recognition + IPFIX + Traffic Insight**, the best experience for **Application Visibility** and analytics at the access layer.
- With Aruba CX Edge Insights addition in AOS-CX 10.12, **Application-Based Policy** allows to **Control Application** usage with permit/deny rules based on recognized applications.

Application Recognition

Outcome for Network Admin: Application Visibility



enable application recognition



Traffic report with IPFIX only

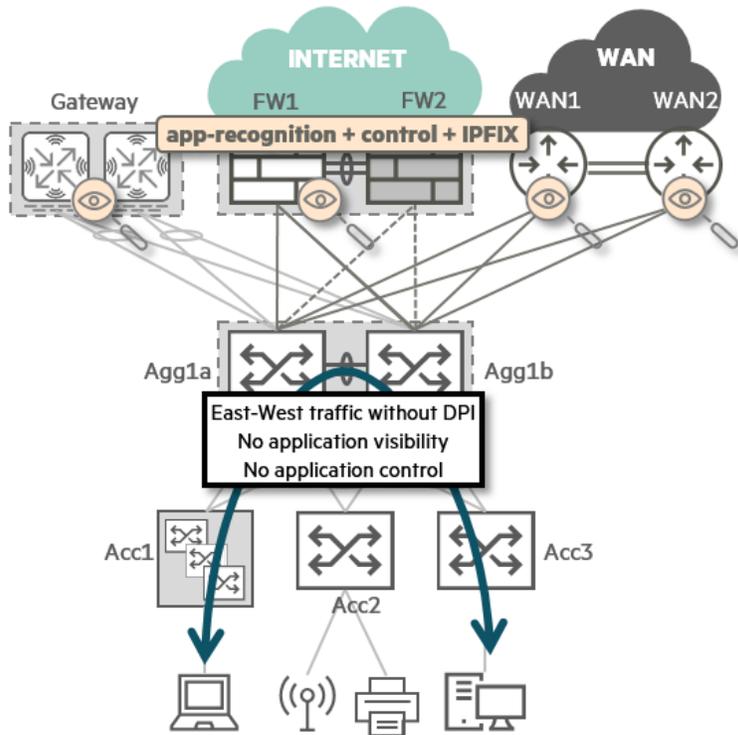
IPFIX + APP-RECOGNITION

Application Recognition Overview

- **Deep Packet Inspection @ Layer7:**
 - HTTPs-based applications: L4-port based identification is not possible.
 - DPI engine analyses information like certificates, SNI, signature patterns...
- Application Recognition allows to:
 - report per flow, the application-name, application-ID, and application category as defined by the DPI engine.
 - embed this application information in IPFIX export-data
 - provide applications visibility with traffic statistics exported to external IPFIX collector or to Cloud platforms
 - deploy application control per user role with application-based policy
- Available for wired-client directly connected to a switch port.
Feature is enabled **on the port** or **on the port-access role**.
- **IPv4 and IPv6 Unicast** traffic only. **UDP/TCP** based applications.
- ~ **3800** supported applications: Office365, Skype, Sharepoint, Facebook, Gmail, Yahoo, Twitter, Instagram, Youtube.
- Supported on **6300** (incl. VSF) and **6400v2**.

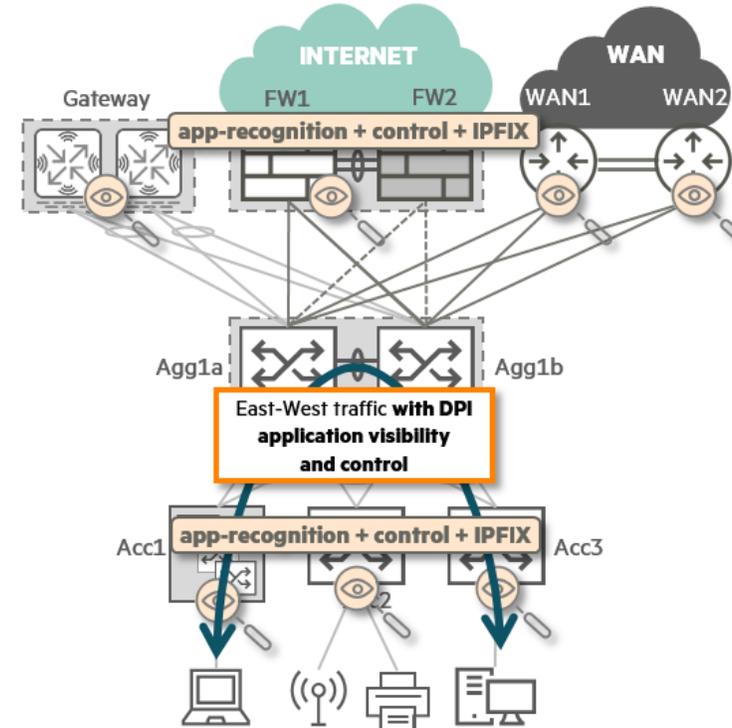
Deep Packet Inspection (DPI) at the Network Edge

Centralized model (legacy)



- DPI and IPFIX only at a centralized function: mobility-gateway for User Based Tunneling (UBT) or firewall or WAN router will inspect North/South traffic
- East/West non UBT traffic at access layer is NOT inspected

Distributed model (new)



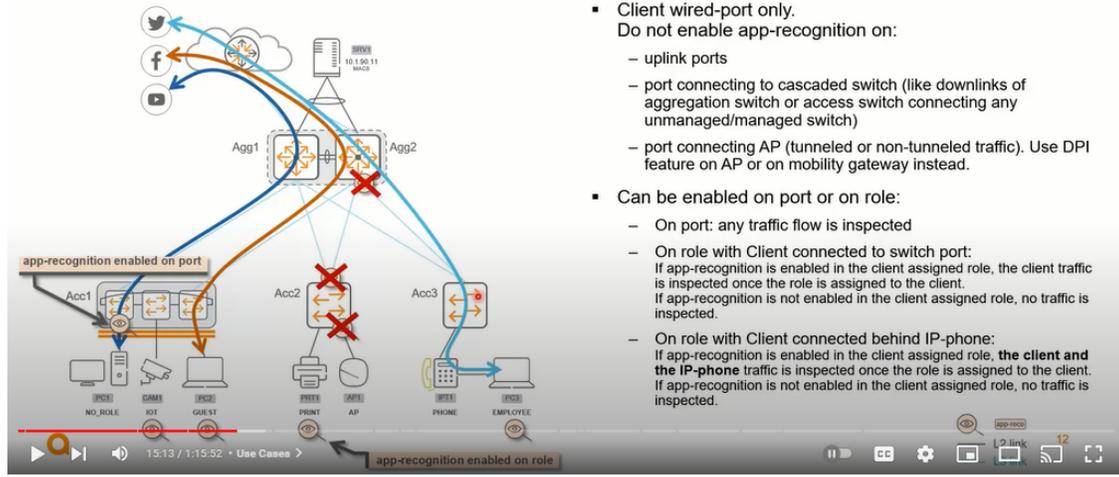
- Distributed DPI and IPFIX at the access layer
- Complement Centralized model
- East/West non UBT traffic at access layer is inspected for application visibility and reporting within the Campus

Campus Use Case and DPI Process Details

Campus Use-case

Campus Use-case – Application Visibility

Access ports only: per port or per user-role



- Client wired-port only.
Do not enable app-recognition on:
 - uplink ports
 - port connecting to cascaded switch (like downlinks of aggregation switch or access switch connecting any unmanaged/managed switch)
 - port connecting AP (tunneled or non-tunneled traffic). Use DPI feature on AP or on mobility gateway instead.
- Can be enabled on port or on role:
 - On port: any traffic flow is inspected
 - On role with Client connected to switch port:
If app-recognition is enabled in the client assigned role, the client traffic is inspected once the role is assigned to the client.
If app-recognition is not enabled in the client assigned role, no traffic is inspected.
 - On role with Client connected behind IP-phone:
If app-recognition is enabled in the client assigned role, **the client and the IP-phone** traffic is inspected once the role is assigned to the client.
If app-recognition is not enabled in the client assigned role, no traffic is inspected.

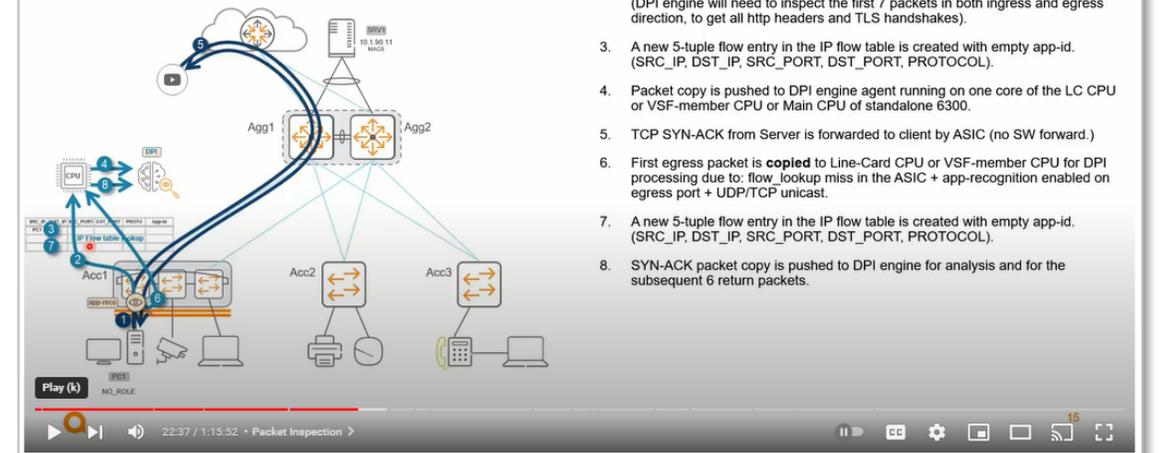
<https://youtu.be/C1kogaM07l8?t=785>



DPI Process details

Application Recognition

DPI process (simplified overview)



1. TCP SYN: PC1 initiates TCP traffic to application server (after DNS resolution). Packet is forwarded to destination by ASIC (no SW forwarding).
2. This first ingress unicast TCP or UDP packet is **copied** to Line-Card CPU or VSF-member CPU for DPI processing due to: flow_lookup miss in the ASIC + app-recognition enabled on ingress port + UDP/TCP unicast. (DPI engine will need to inspect the first 7 packets in both ingress and egress direction, to get all http headers and TLS handshakes).
3. A new 5-tuple flow entry in the IP flow table is created with empty app-id. (SRC_IP, DST_IP, SRC_PORT, DST_PORT, PROTOCOL).
4. Packet copy is pushed to DPI engine agent running on one core of the LC CPU or VSF-member CPU or Main CPU of standalone 6300.
5. TCP SYN-ACK from Server is forwarded to client by ASIC (no SW forward.)
6. First egress packet is **copied** to Line-Card CPU or VSF-member CPU for DPI processing due to: flow_lookup miss in the ASIC + app-recognition enabled on egress port + UDP/TCP unicast.
7. A new 5-tuple flow entry in the IP flow table is created with empty app-id. (SRC_IP, DST_IP, SRC_PORT, DST_PORT, PROTOCOL).
8. SYN-ACK packet copy is pushed to DPI engine for analysis and for the subsequent 6 return packets.

<https://youtu.be/C1kogaM07l8?t=1064>



Platform Support, Scale and Performance

Platform	6300	6400 (v2)
Application Recognition	Yes	Yes (v2-default profile only)
Max flows * (IP flow hash-table)	24,576	Acc LC: 24,576 Core LC: 61,440
Max bidi-flows (IP pairs/connections)	12,288	Acc LC: 12,288 Core LC: 30,720
Max pps (COPP) (packets of new flows copied to LC CPU)	3,500 ingress + 3,500 egress	3,500 ingress + 3,500 egress
Max new connection/s per LC (new conn. processed by LC CPU)	500 cps	500 cps

* IPv4 and/or IPv6. IPv6 scale is the same than IPv4.

1 cps = 1 ingress flow/s + 1 egress flow/s

Application Recognition

Examples

```
6300# show app-recognition app ssh
```

```
NAME       : ssh
ID         : 198
CATEGORY   : encrypted
DESCRIPTION : Secure Shell
```

```
6300# show app-recognition app youtube
```

```
NAME       : youtube
ID         : 240
CATEGORY   : streaming
DESCRIPTION : Youtube.com
```

```
6300# show app-recognition app facebook
```

```
NAME       : facebook
ID         : 244
CATEGORY   : social-networking
DESCRIPTION : Facebook
```

```
6300# show app-recognition app twitter
```

```
NAME       : twitter
ID         : 503
CATEGORY   : social-networking
DESCRIPTION : Twitter
```

```
6300# show app-recognition app | count
```

3831

~ 3800 recognized applications

```
6300# show app-recognition app | include zoom
```

```
zoomtanzania      2785  web           ZoomTanzania
zoom               2928  instant-messaging  Zoom
```

```
6300# show app-recognition app zoom
```

```
NAME       : zoom
ID         : 2928
CATEGORY   : instant-messaging
DESCRIPTION : Zoom
```

```
=== ARCD Global FLOW Data ===
```

SRC IP	DST IP	SRC Port	Dst Port	Proto	VRF	Agent	State	App Id
10.80.2.217	10.6.100.10	8080	53651	6	1	0	READY	240
10.6.100.10	10.80.2.217	3389	52491	6	1	0	READY	159
10.6.100.10	10.80.2.217	53631	8080	6	1	0	READY	562
10.80.2.217	10.6.100.10	8080	53650	6	1	0	READY	0
10.6.100.10	10.80.2.217	53629	8080	6	1	0	READY	2821
10.80.2.193	10.6.100.10	52676	3389	6	1	0	READY	159
10.80.2.217	10.6.100.10	8080	53652	6	1	0	READY	240
10.6.100.10	10.80.2.217	53651	8080	6	1	0	READY	240
10.6.100.10	10.80.2.217	8080	8080	6	1	0	READY	0
10.6.100.10	10.80.2.217	53639	8080	6	1	0	READY	1122
10.80.2.217	10.6.100.10	8080	53639	6	1	0	READY	1122
10.80.2.217	10.6.100.10	8080	53643	6	1	0	READY	0
10.80.2.219	10.6.100.10	53	52491	17	1	0	READY	32
10.6.100.10	10.80.2.219	52491	53	17	1	0	READY	32
10.6.100.10	10.80.2.217	53652	8080	6	1	0	READY	240
10.80.2.193	10.6.100.10	60926	3389	17	1	0	READY	159
10.6.100.10	10.80.2.217	53643	8080	6	1	0	READY	0
10.6.100.10	10.80.2.193	3389	60926	17	1	0	READY	159

Total Number of Flows : 18

Extract from "diag-dump arc basic"

IPFIX



IP Flow Information Export (IPFIX) Overview

- IPFIX is an IETF standard-based monitoring technology (RFC7011 and more). Sometime called Netflow v10.
- IPFIX monitoring solution comprises:
 - **IPFIX exporter** that runs on a switch/router.
 - **IPFIX collector** that receives monitoring information from IPFIX exporters.
- IPFIX defines **flow records** with **match fields** and **collect fields**:
 - match key fields defining IPv4 or IPv6 5-tuple flow and exported in the IPFIX export-data
src_ip, dst_ip, src_port, dst_port, protocol
 - collect non-key fields specifying what flow information is collected such as:
*flow volume (bytes and/or packets), flow start-time, flow end-time, **application identity***
- **CX Switching IPFIX support**:
 - ingress direction only
 - IPv4 and IPv6 version
 - unicast and multicast traffic
 - ICMP
 - L2 port, L2 LAG, VSX LAG, L3 port (ROP), L3 LAG
 - platforms: **6300** (incl. VSF), **6400v1/v2**, **8100** and **8360**
- No sampling: 1 counted packet out of 1 packet seen on data-plane (new flow < max COPP)

IPFIX exported DATA

with Application recognition

IPFIX EXPORT DATA

```
> Frame 12: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface \Device\NPF_
> Ethernet II, Src: ArubaaHe_ae:73:c1 (88:3a:30:ae:73:c1), Dst: VMware_8e:d8:b2 (00:50:56:8e:d8:b2)
> Internet Protocol Version 4, Src: 16.1.38.244, Dst: 16.1.38.113
> User Datagram Protocol, Src Port: 42501, Dst Port: 4739
▼ Cisco NetFlow/IPFIX
  Version: 10
  Length: 88
  > Timestamp: Nov  4, 2022 12:00:41.000000000 Central Europe Standard Time
  FlowSequence: 1214
  Observation Domain Id: 2267500826
  ▼ Set 1 [id=257] (1 flows)
    FlowSet Id: (Data) (257)
    FlowSet Length: 72
    [Template Frame: 11]
    ▼ Flow 1
      SrcAddr: 10.1.12.16
      DstAddr: 10.1.10.18
      SrcPort: 42690
      DstPort: 22
      Vlan Id: 12
      Protocol: TCP (6)
      IPVersion: 4
      Flow End Reason: End of Flow detected (3)
      Padding: 00000000000000
      [Duration: 0.006815188 seconds (microseconds)]
      Octets: 6036
      Packets: 46
      InputInt: 1
      Ingress Physical Interface: 1
      Classification Engine ID: PANA-L7 (13)
      Selector ID: 0000c6
```

IPFIX EXPORT OPTIONS DATA with app-recognition enabled

```
> Frame 14: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface \Device\NPF_
> Ethernet II, Src: ArubaaHe_ae:73:c1 (88:3a:30:ae:73:c1), Dst: VMware_8e:d8:b2 (00:50:56:8e:d8:b2)
> Internet Protocol Version 4, Src: 16.1.38.244, Dst: 16.1.38.113
> User Datagram Protocol, Src Port: 42501, Dst Port: 4739
▼ Cisco NetFlow/IPFIX
  Version: 10
  Length: 132
  > Timestamp: Nov  4, 2022 12:00:41.000000000 Central Europe Standard Time
  FlowSequence: 1215
  Observation Domain Id: 2267500826
  ▼ Set 1 [id=273] (1 flows)
    FlowSet Id: (Data) (273)
    FlowSet Length: 116
    [Template Frame: 13]
    ▼ Flow 1
      Classification Engine ID: PANA-L7 (13)
      Selector ID: 0000c6
      ApplicationName: ssh
      Padding: 000000
      Application Category Name: encrypted
      Padding: 000000
      ApplicationDesc: Secure Shell
      Padding: 000000
```

IPFIX / sFlow comparison

sFlow

- Flow **sampling** (1 out of n packets) technology
- Does not report flow duration
- Sample includes datagram (up to 9000 bytes payload)
- No URL tracking
- No ASIC-table resource consumed
- **CPU intensive** (protected by COPP)

Port Speed	sFlow Sampling Rate
10 Mb/s	1 in 200
100 Mb/s	1 in 500
1 Gb/s	1 in 1000
10 Gb/s	1 in 2000
25 Gb/s	Default (1 in 4096)
40 Gb/s or 100G/b	Default or less frequent

IPFIX

- **No sampling:** 1 out of 1.
Once flow is programmed in TCAM, any packet of that flow is counted. Even a “single-packet flow” is reported.
- Provides flow duration
- Allows to specify proprietary information into a Flow and export it out to the collector for further analysis.
- Allows variable length fields for information export such as URLs.
- IPFIX will export a summary of every flow seen on a port once flow is terminated (TCP FIN or timeout)
- Consumes ASIC resource
- **Not CPU intensive**

IPFIX

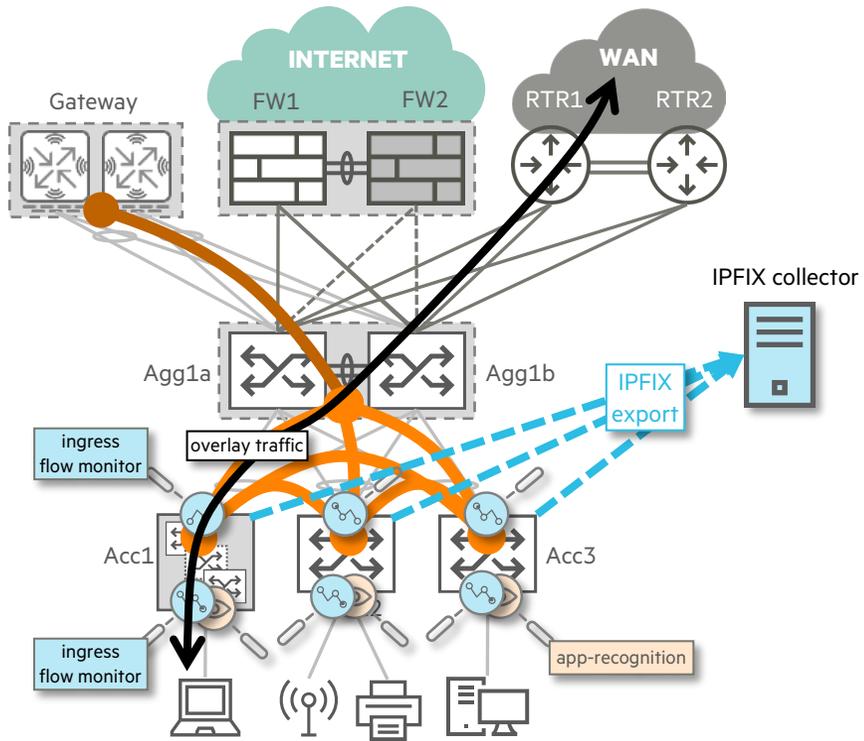
sFlow versus IPFIX for VXLAN traffic

Platform	sFlow		IPFIX	
	Ingress sFlow on port receiving VXLAN	Egress sFlow on port sending VXLAN	Ingress IPFIX on port receiving VXLAN	Egress IPFIX on port sending VXLAN
6300 6400 8100 8360	Sampling done before VXLAN decapsulation.	Sampling done after VXLAN encapsulation.	Monitoring done after VXLAN decapsulation.	<i>Not available</i>
8325 8400 9300 10000	sFlow statistics are related to underlay.	sFlow statistics are related to underlay.	IPFIX statistics are related to overlay.	<i>Not available</i>

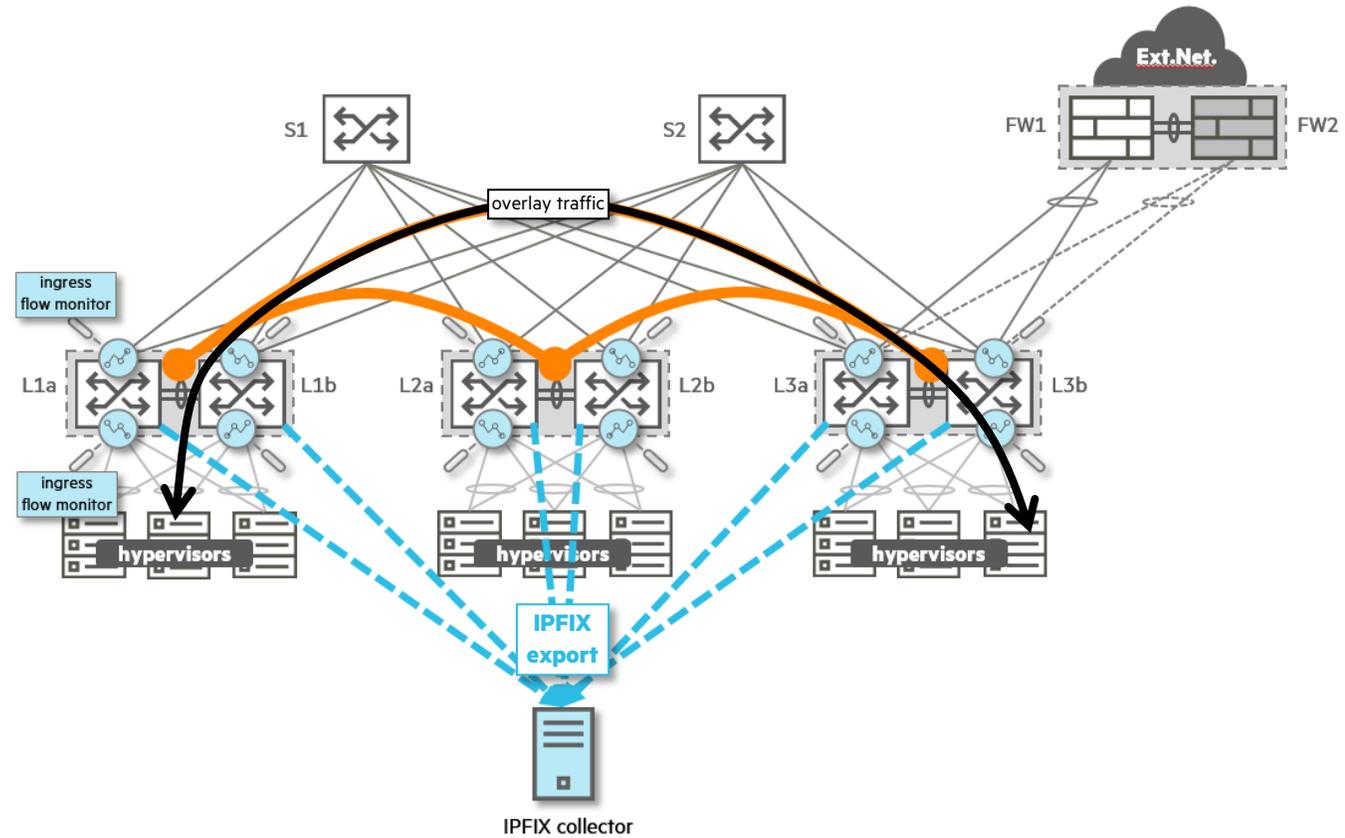
- For **underlay** VXLAN encapsulated traffic: use **sFlow**.
- For **overlay** traffic visibility inside VXLAN tunnels: use **IPFIX**
- Both sFlow and IPFIX can be enabled on the same interface.

Use Cases

Campus



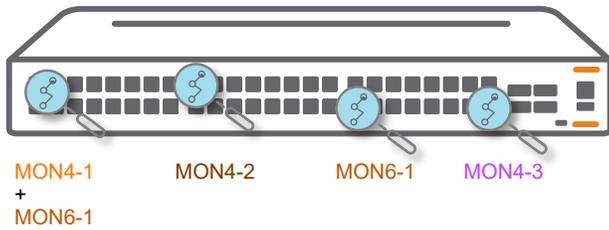
Data Center



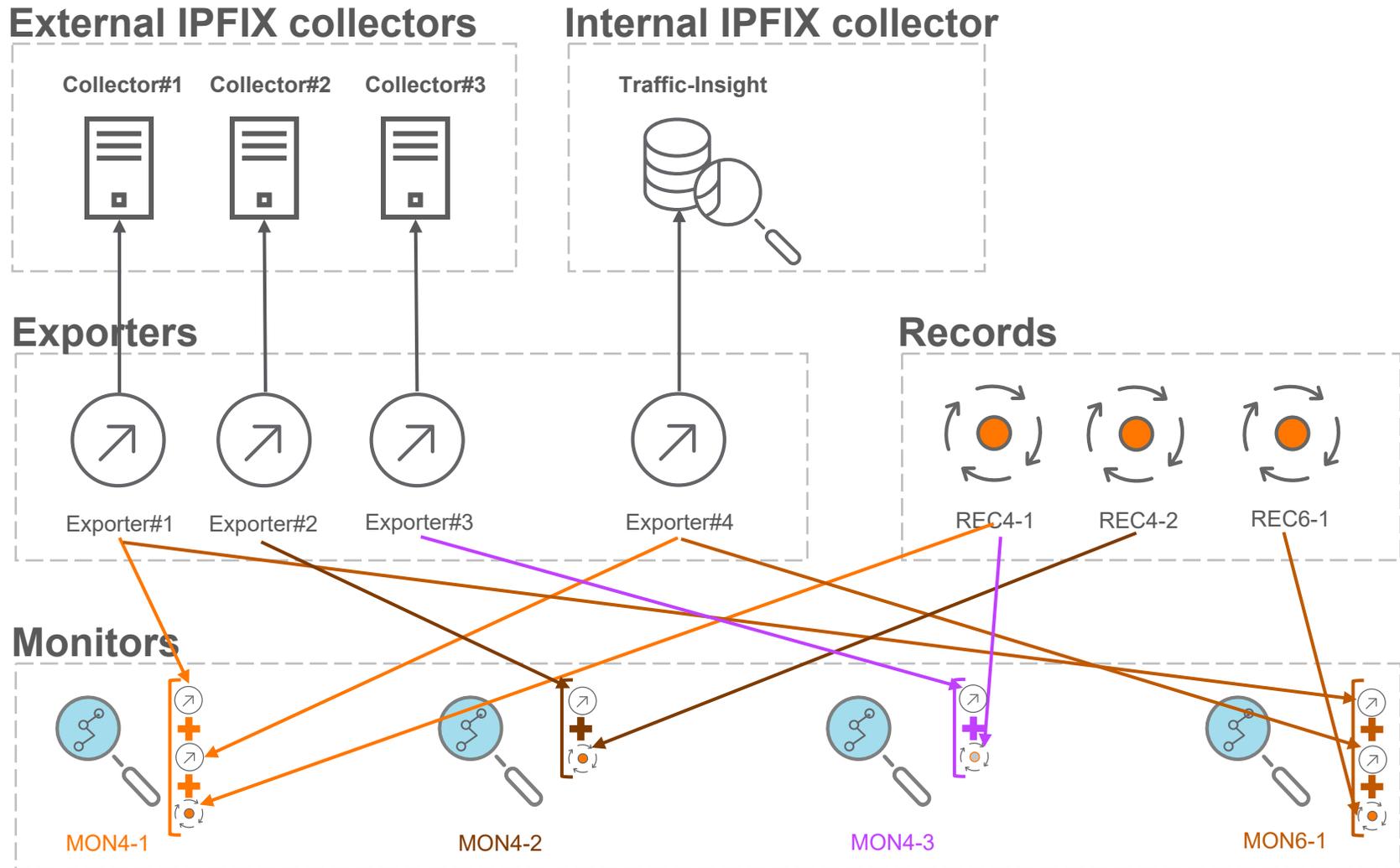
IPFIX

Component relation

Ingress IPFIX monitors / port



- A flow exporter can only send flow reports to one destination.
- Only one record can be attached to a flow monitor.
- A flow exporter can be assigned to one or more flow monitors
- Up to 2 flow exporters can be assigned to a flow monitor.



Platform Support, Scale and Performance

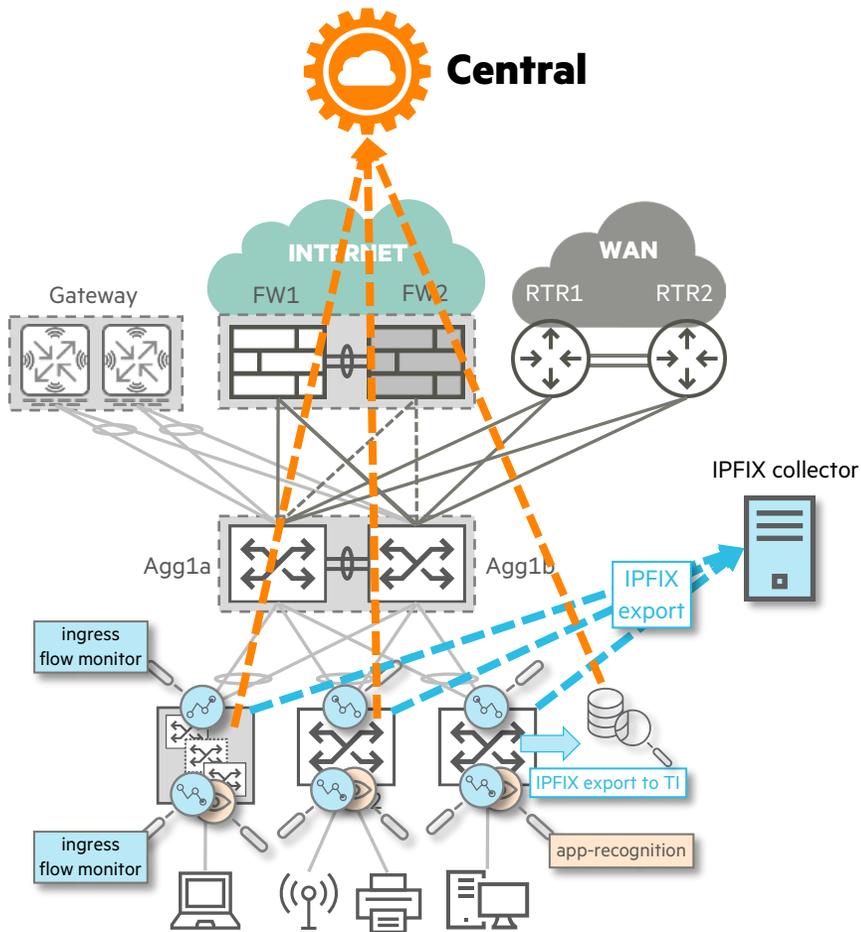
Platform	6300	6400 (v1/v2)	8100	8360 (v1/v2)
Ingress IPFIX	Yes	Yes	Yes	Yes
Egress IPFIX	No	No	No	No
Max IP flows (IPFIX TCAM)	IPv4: 19,632 IPv6: 4,908	IPv4: 64,688 IPv6: 16,172	IPv4: 15,536 IPv6: 3,884	IPv4: 64,688 IPv6: 16,172
Max IP bidi-flows (IP pairs/connections)	IPv4: 9,816 IPv6: 2,454	IPv4: 32,344 IPv6: 8,086	IPv4: 7,768 IPv6: 1,942	IPv4: 32,344 IPv6: 8,086
Max pps (COPP) (packets of new flows copied to LC CPU)	2,500 (default)	2,500 (default)	2,500 (default)	2,500 (default)

Traffic Insight



Use Case for Traffic Insight

IPFIX aggregator and flow analytics offload



- **IPFIX external collector**
receives all exported flow reports from all edge switches
- **On-premise versus Cloud**
 - IPFIX external collector is appropriate for on-premise
 - Not so scalable for a multi-tenant Cloud-based solution
- **Flow aggregator and analytics at the edge switch**
 - reduce the amount of data to be exported
 - provide API for Cloud platform consumption

Traffic Insight Overview

- **CX Internal IPFIX collector**
TI receives the same data set than an external IPFIX collector configured in the same flow monitor + SRC/DST MAC.
- **Aggregates** flow data information into OVSDB which can then be consumed through **API** by Aruba Central for analytics reporting.
- **Visualization** of the topN flows report for easy monitoring and troubleshooting in **web-UI**.
- Filters, aggregates and sorts the data based on user flow monitor requests:
 - tracks different “**monitor requests**” simultaneously
 - provides “**monitor reports**” per request
- 3 monitor types: **topN flows**, **application-flows** and **DNS average latency**.
- Up to **5 monitors**, among which:
 - one single “DNS latency” monitor
 - one single “application flows” monitor

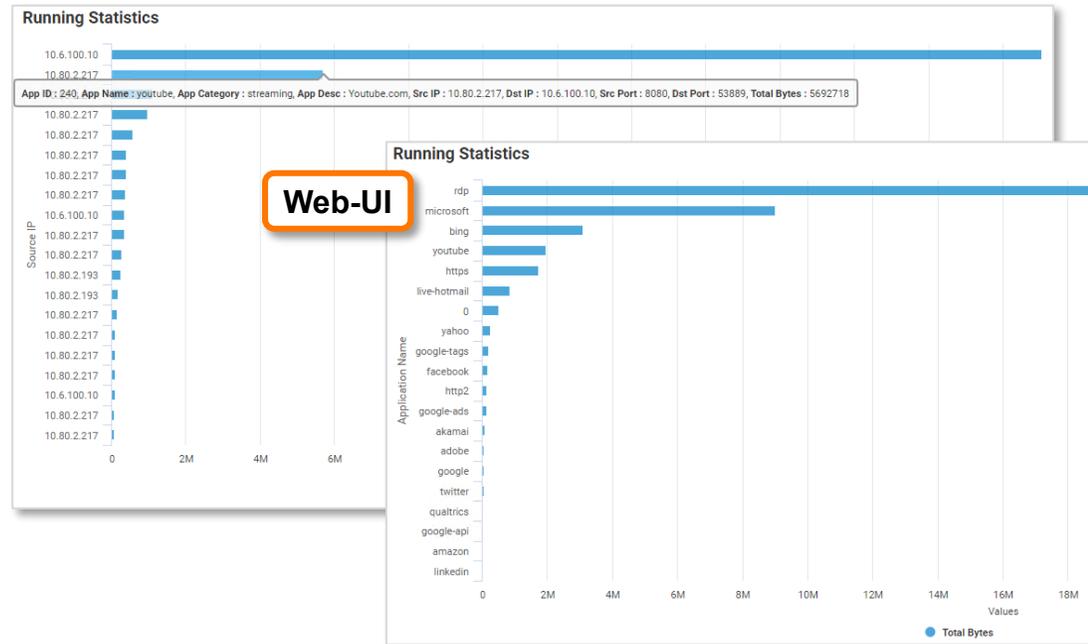
Traffic Insight

topN-flows

CLI

```
Name      : topN1
Group By  : None
Entries   : 20
Filter By : None
Running Statistics Timeout : 2700
```

Rank	srcip	dstip	ipproto	srcport	dstport	appname	Bytes
1	10.6.100.10	10.80.2.193	udp	3389	52457	rdp	1821807
2	10.80.2.217	10.6.100.10	tcp	8080	61979	youtube	1569700
3	10.80.2.217	10.6.100.10	tcp	8080	61938	bing	793565



- Monitors IPv4 and IPv6 traffic flowing through the switch and captures **topN volume flows** (by bytes).
- Number of top captured flows: 5 (default), up to **20**.
- Top-N flow reports are generated **every 5 min** once (timer not configurable).
- The running-statistics period is 45 min (by default), configurable down to 6 min. After this period, the statistics are cleared.
- To get **app-id**, **application-name** and **application category** populated, **app-recognition must be enabled** on the client-facing port; otherwise reported values will be zero or unknown.
- “**Filter-by**” is a filter that can be used to reduce the displayed data set based on the filter category.
- “**Group-by**” can be used to group flows based on the grouping category.

Traffic Insight

Application flows

```
show traffic-insight TI monitor-type application-flows app
```

Name	:	app			
Type	:	application-flows			
Dataset	:	Last 14 mins			
client_mac	src_ip	dst_ip	app_id	Rx (Bytes)	Tx (Bytes)
00:50:56:9e:2c:48	10.6.100.10	10.80.2.193	159	4975828	10108622
00:50:56:9e:2c:48	10.6.100.10	10.80.2.217	68	1537525	229327
00:50:56:9e:2c:48	10.6.100.10	10.80.2.219	32	284	156
00:50:56:9e:2c:48	10.6.100.10	10.80.2.217	1284	61450	24153
00:50:56:9e:2c:48	10.6.100.10	10.80.2.217	3662	34669	4950

```
show traffic-insight TI monitor-type application-flows app app-details
```

Name	:	app				
Type	:	application-flows				
Dataset	:	Last 14 mins				
client_mac	app_id	app_name	app_category	app_description	Rx (Bytes)	Tx (Bytes)
00:50:56:9e:2c:48	159	rdp	thin-client	Remote Desktop Protocol (Windows	4975828	10108622
00:50:56:9e:2c:48	68	https	web	HyperText Transfer Protocol Secu	1537525	229327
00:50:56:9e:2c:48	32	dns	network-service	Domain Name Service	284	156
00:50:56:9e:2c:48	1284	akamai	web	Akamai Technologies CDN	61450	24153
00:50:56:9e:2c:48	3662	qualtrics	web	Qualtrics	34669	4950

- Analyze **all the IPv4/IPv6 flows** that is collected by IPFIX.
- Aggregates both **Client-to-Server** and **Server-to-Clients** ingress flows to merge them into **one single bi-directional flow** of the client/server connection per application, providing Rx and Tx byte details.
- Traffic Insight update this bidirectional flow **into the OVSDB database** which will be exported via APIs in order to report the application traffic per client (to Central for instance).
- To get **app-id**, **application-name** and **application category** populated, **app-recognition must be enabled** on the client-facing port, otherwise reported value will be zero for app-id and unknown for application-name.

Traffic Insight

dns-average-latency

Traffic-Insight

```
Name : dns
Type : dns-average-latency
Start time for latency calculation : 10/18/2022 10:11:15.564822 UTC
End time for latency calculation : 10/18/2022 10:16:15.592663 UTC
-----
client_mac      dns_server_ip  dns_average_latency(usec)  number_of_dns_requests
-----
00:50:56:9e:2c:48  10.80.2.219      50928                      4
```

- Measure the average latency of the DNS request and response **from the client viewpoint**.
- The DNS traffic data is extracted from IPFIX data.
- The DNS average latency is calculated from DNS request and response packets from the servers for different clients.
- When enabled, **Client-Insight** will use this DNS average latency, which can then be consumed through Client-Insight API for reporting to Central.

Client-Insight

Displaying client entries with (mac) as key.
Total number of entries: 1

MAC : 00:50:56:9e:2c:48

Overall on-boarding status : timeout
Overall on-boarding failure reason : l3_onboarding_failed

L2 on-boarding detail

L2 on-boarding status : successful
L2 on-boarding failure reason : -
L2 on-boarding start time : 10/13/2022 17:25:05.023453 UTC
L2 on-boarding end time : 10/13/2022 17:25:05.105563 UTC
L2 on-boarding latency : 0 min, 0 sec, 82110 us
802.1x RADIUS latency : -
MAC-Auth RADIUS latency : 0 min, 0 sec, 80911 us

L3 on-boarding detail

IP on-boarding status : timeout
IP on-boarding failure reason : no-dhcp
L3 on-boarding latency : -

VLAN : 1006

IP details

IPv4 on-boarding status : -
IPv6 on-boarding status : -

DHCPv4

Status : -
Failure reason : -
Start time : -
End time : -

DHCPv6

Status : -
Failure reason : -
Start time : -
End time : -

DNS details

Server IP: 10.80.2.219

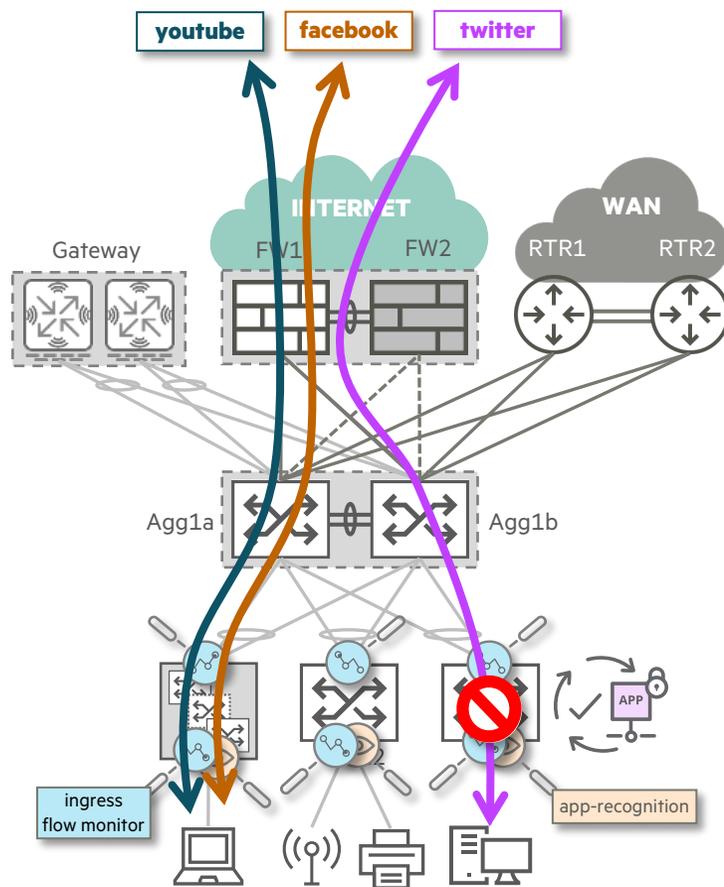
Average latency : 50928
DNS start time for latency calculation : 10/18/2022 10:11:15.564822 UTC
DNS end time for latency calculation : 10/18/2022 10:16:15.592663 UTC
Number of DNS requests : 4

Application-Based Policy

AOS-CX 10.12

policy action = { drop }

Application-Based Policy Overview



- **Allow or block** authenticated user access to **specific applications** or protocols identified by app-recognition.
- Policy is applied on **user role**.
- Port access authentication (802.1X or MAC auth) must be configured, with **local** or **downloadable** user roles.
- **IPv4 and IPv6 Unicast** traffic only. **UDP/TCP** based applications.
- Application Control **operation** overview:
 - ABP rules use application-name
 - Hence, first few packets (max 7) of each new flow are allowed until the application is recognized by DPI engine.
 - Once flow classification is completed, ABP actions are applied via rules being programmed in the ASIC TCAM.
 - An implicit deny rule is applied if the traffic flow doesn't match any configured ABP rules.

Configuration and ABP Session Limit Exceed Action

■ Configuration:

```
class abp-ip abp-class1
  10 match udp any any app-category web app youtube-music count
  20 match tcp any any app-category any app facebook
  30 ignore any any 10.0.0.10/255.255.255.0 app-category standard app unknown
  40 match udp any any any app-category standard app unknown
class abp-ip abp-permit
  10 match any any any app-category any app any
!
port-access abp abp-policy
  10 class abp-ip abp-class1 action drop
  20 class abp-ip abp-permit
```

```
gbp role test 100
!
port-access role test
  app-recognition enable
  associate abp abp-policy
  vlan access 12
```

- If the number of app flows exceed the size limit of the flow table
=> ABP rule enforcement for flows in excess of the table size would fail (missing app-id)
- This is a potential network security vulnerability:
a malicious user could bypass ABP by flooding the switch with flows and overflowing the flow table
- User-configurable flow table overflow behavior when max threshold (80% of flow table size) is exceeded:
 - By default, drop new flows for source roles on affected system, line card, or VSF member
 - Or generate warning messages in switch event log

Policies combination

- Port access supports three different traffic policy types to associate with a port access role:
 - **Port access policy**, applied on traffic sourced from user role
 - **Group based policy**, applied on traffic destined to user-role
 - **App-based policy**, applied on traffic sourced from user-role with actions based on application identity
- ABP, GBP and port-access policies can co-exist.
- Since **ABP** matches and acts based on the layer 7 application information, it is a more specific policy and hence has **higher precedence over the GBP or PAC policies**.
- When multiple policies match a packet and at least one of them intends to drop it, then the packet is dropped.

Conclusion



Next-Gen Aruba Central – Atmosphere 2023 keynote demonstration

Application Visibility with data from Traffic-Insight

Applications

Name	Experience	Category	Host Type	Security Risk	Usage
Unknown	Poor performance	Unknown	Public	Unknown	7.53 GB
DNS	Fair performance	Network Service	Public	Unknown	1.42 GB
Youtube.com	Poor performance	Streaming	Public	Trustworthy	681.85 MB
Incomplete virtual...	Poor performance	Standard	Public	Unknown	456.63 MB
GitHub	Good performance	Web	Public	Unknown	301.98 MB
Netflix.com	Fair performance	Streaming	Public	Unknown	33.3 MB
Adobe	Good performance	Adobe SAAS	Public	Unknown	4.77 MB
Google Generic	Fair performance	Google SAAS	Public	Unknown	1.08 MB
Fast	Fair performance	Web	Public	Trustworthy	1.63 KB
Amazon Web...	Good performance	Amazon SAAS	Public	Low	

Atmosphere '23 Technical Keynote Live Stream

Aruba, a Hewlett Packard Enterprise company

4.6K views Streamed 2 weeks ago

Power Your Transformation Journey to Prepare for What Comes Next. Delivering business value requires an agile, scalable, and secure network that adapts as your business changes. Join David Hughes, Chief Product and Technology Officer, HPE Aruba Networking and his team of experts as they reveal the right fit for solving business and IT challenges—from reducing cybersecurity risk to streamlining IT operations. [Show more](#)

<https://youtu.be/Yui5w56MIKs?t=1957>



Role/Application Policies

Network Overview

Access your network organization, configuration and operations from a single pane of glass.

Library

Site Collections 5 collections

Sites 14 sites

Devices 62 devices

Device Groups 10 groups

CREATE RULE

Description *
Block Dan AppStore

Source *
Access Role

Access Role
DanTheMan

Destination *
Any

Service/Application *
Appstore

Application *
Appstore

Action *
Allow

Atmosphere '23 Technical Keynote Live Stream

Aruba, a Hewlett Packard Enterprise company

4.6K views Streamed 2 weeks ago

Power Your Transformation Journey to Prepare for What Comes Next. Delivering business value requires an agile, scalable, and secure network that adapts as your business changes. Join David Hughes, Chief Product and Technology Officer, HPE Aruba Networking and his team of experts as they reveal the right fit for solving business and IT challenges—from reducing cybersecurity risk to streamlining IT operations. [Show more](#)

<https://youtu.be/Yui5w56MIKs?t=2115>



Airheads Broadcasting – YouTube channel

AOS-CX Software Release Technical Update



Application Recognition
Outcome for network admin



Aruba AOS-CX Software Release Technical Update

Airheads Broadcasting
167 videos • 2,487 views • Last updated on Mar 4, 2023

Play all Shuffle

Question, suggestion, comment, please request you to ask on Aruba Airheads Community <https://community.arubanetworks.com>.
This Video Series will cover about Aruba CX Switching - Listen to Product Quick Start Videos: <https://www.youtube.com/playlist?list=PLsYGHuNuBZca1Rh4vnmJTmoFBq2WjixwK>
Next-Gen, Cloud-native Switching
Designed for the Network Operator, Edge Access to Data Center!
To learn about Aruba AOS-CX Software Release Technical Update
https://www.youtube.com/playlist?list=PLsYGHuNuBZcbWPEjjiHuVMqP-Q_UL3CskS

To learn about Aruba Central & Aruba AOS-CX Better Together:
<https://www.youtube.com/playlist?list=PLsYGHuNuBZca8eGDVxgypKSELnJQ7AIXx>

AOS-CX User Guides:
https://www.arubanetworks.com/techdocs/AOS-CX/help_portal/Content/home.htm

Unavailable videos are hidden

- **HPE Aruba CX Edge Insight**
Airheads Broadcasting • 538 views • 3 months ago
- **Aruba AOS-CX 10.11: Application Recognition Software Upgrade Technical Update**
Airheads Broadcasting • 1.2K views • 3 months ago
- **Aruba AOS-CX 10.11: VSF Enhanced Software Upgrade Technical Update**
Airheads Broadcasting • 1.4K views • 4 months ago
- **Aruba AOS-CX 10.11: Autoneg, Speed, and Device Type Knobs in addition to a FEC Mode**
Airheads Broadcasting • 318 views • 4 months ago
- **Aruba AOS-CX 10.11: No Reboot Required for LLFC PFC Technical Update**
Airheads Broadcasting • 266 views • 4 months ago
- **AOS-CX 10.11: PTP Peer to Peer Delay Technical Update**
Airheads Broadcasting • 262 views • 5 months ago
- **Aruba AOS-CX 10.11: Multi Fabric VXLAN GBP Technical Update**
Airheads Broadcasting • 434 views • 5 months ago
- **AOS-CX 10.11: Aruba CX 9300 100G 40G transceiver & AOC Technical Update**
Airheads Broadcasting • 252 views • 5 months ago
- **Aruba AOS-CX 10.11 Multicast SSM-Map Technical Update**
Airheads Broadcasting • 205 views • 5 months ago
- **AOS-CX 10.11: LLDP TLVs (Type-Length-Value) Technical Update**
Airheads Broadcasting • 332 views • 5 months ago



https://www.youtube.com/playlist?list=PLsYGHuNuBZcbWPEjjiHuVMqP-Q_UL3CskS

Thank You

aruba_switching_tme@hpe.com