How to Adopt Zero Trust using SD-Access

and Default-Deny without tears

Raphael Lienard – Solutions Engineer

BRKENS-3810

Agenda

- Introduction
- Segmentation Strategy
- Observability Pipelines
- Deploy Allow-List Model
- Conclusions

Raphael Lienard

- Technical Solutions Architect
- Enterprise Networking (with focus on SD-Access)
- > 10 years as network engineer / architect
- Based in Luxembourg

Webex App

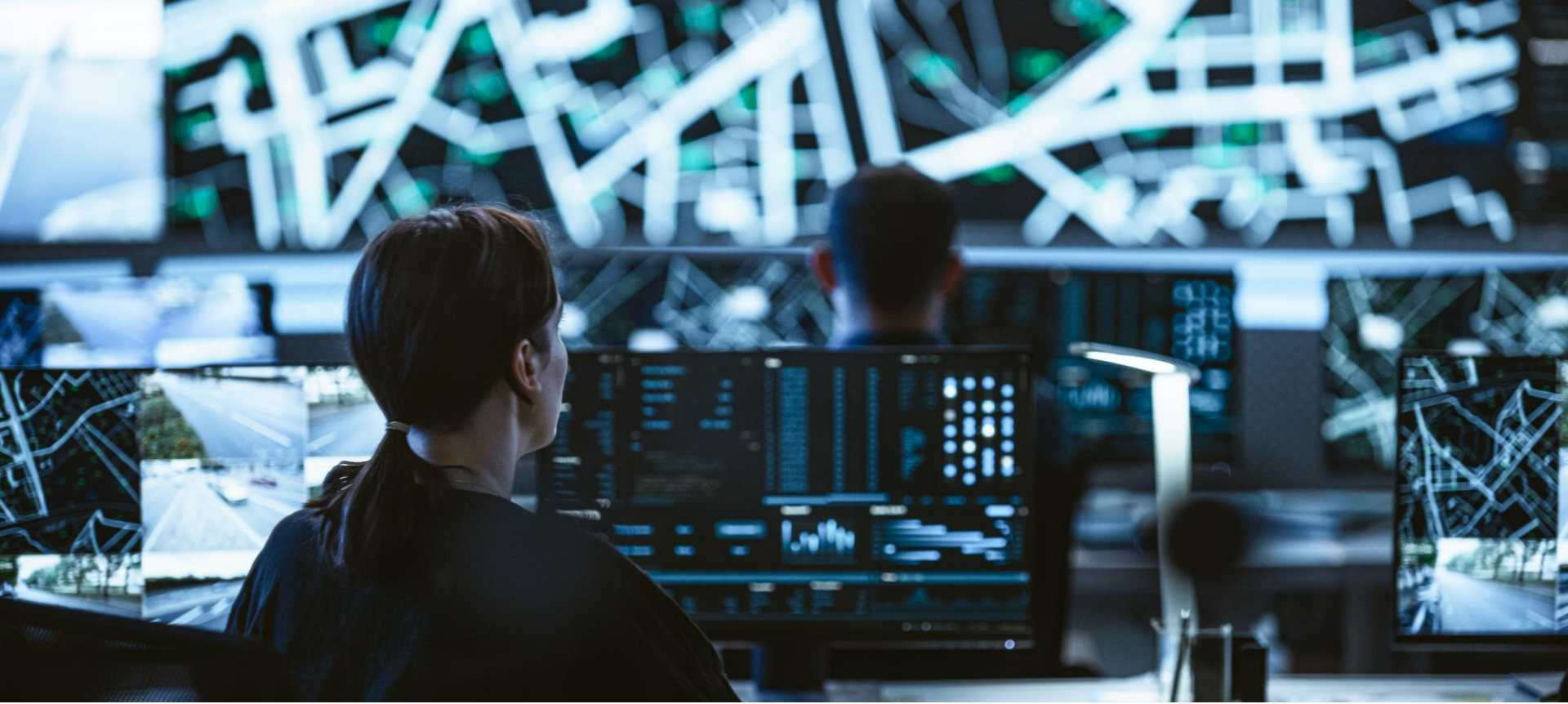
Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.



“ Default-Deny using SD-Access is a no-brainer ”

Expectations

What's inside ?

- Get all the building blocs to activate the Allow-List model on SDA.
- Understand how to extend visibility on the network using Splunk.

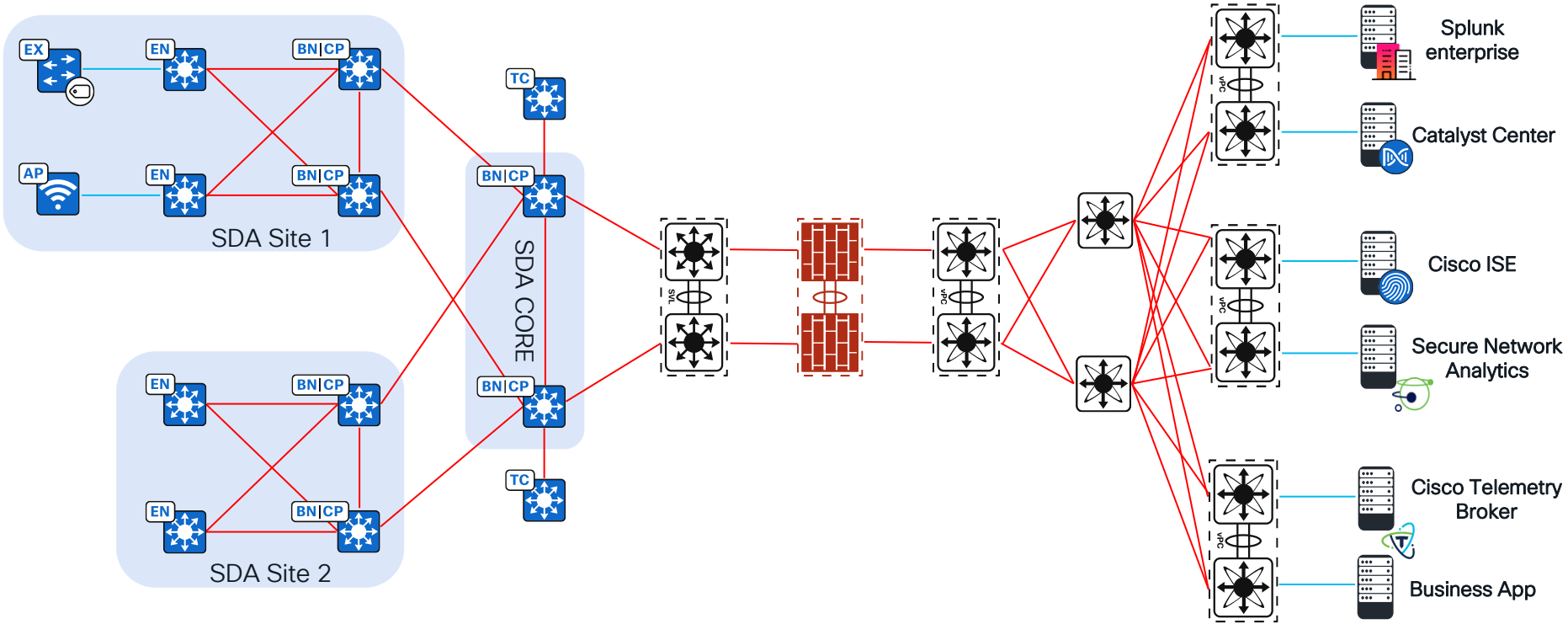
Disclaimers

- This is an advanced session, you should know how SDA works.
- Focus on the Policy Plane of SDA.
- Not a troubleshooting session.
- There are slides marked "for your reference"

For your reference

Reference Architecture

For your reference

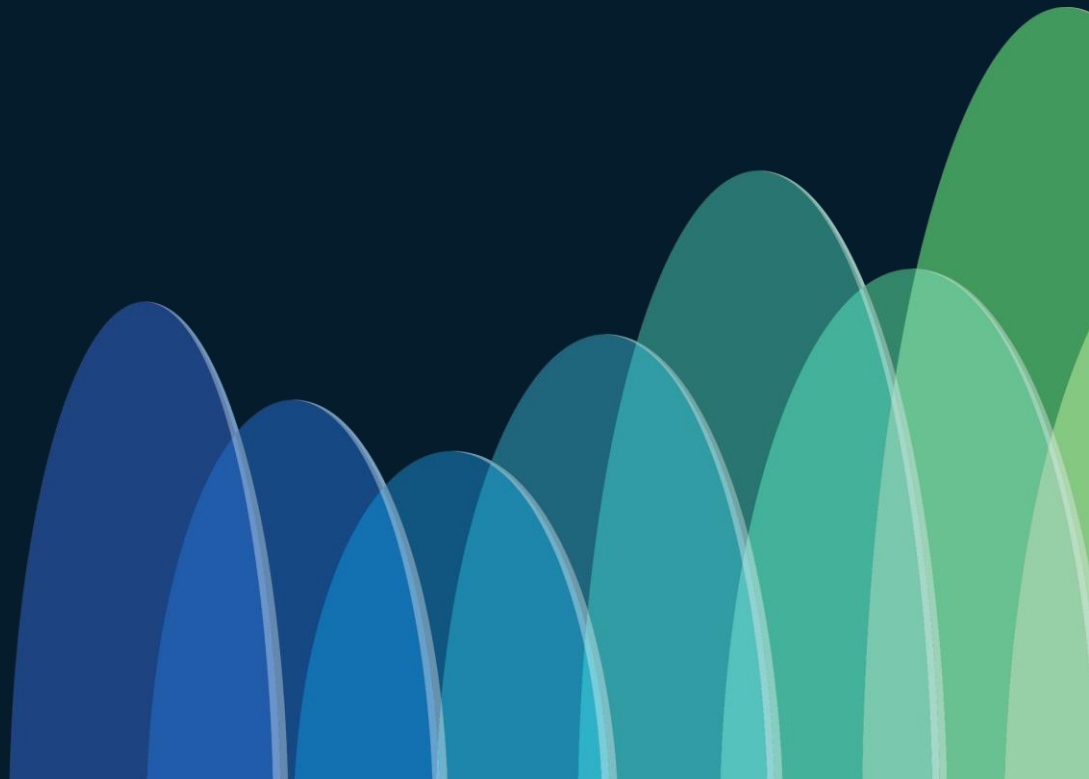


“ Zero Trust assumes that threats are already inside ”

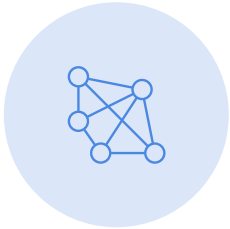
Agenda

- Introduction
- Segmentation Strategy
- Observability Pipelines
- Deploy Allow-List Model
- Conclusions

Classification



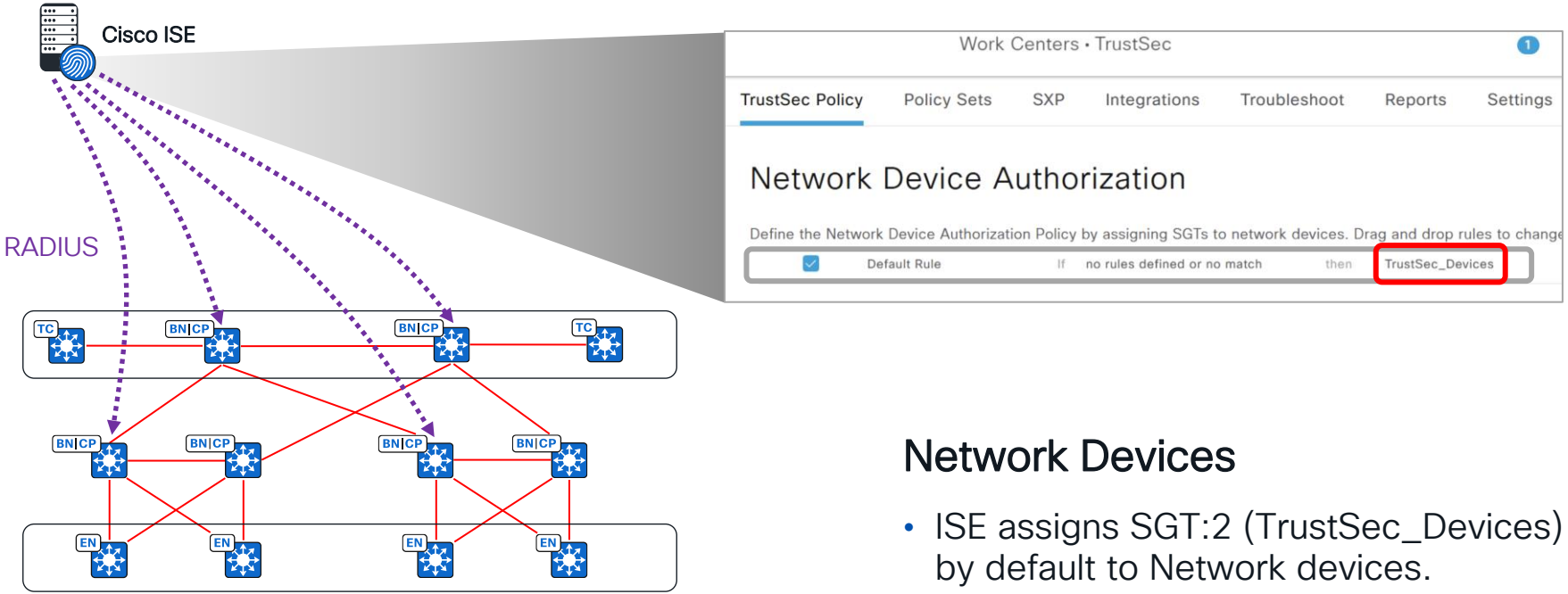
Classification



UNDERLAY

OVERLAY

Classification – Network Devices



Network Devices

- ISE assigns SGT:2 (TrustSec_Devices) by default to Network devices.

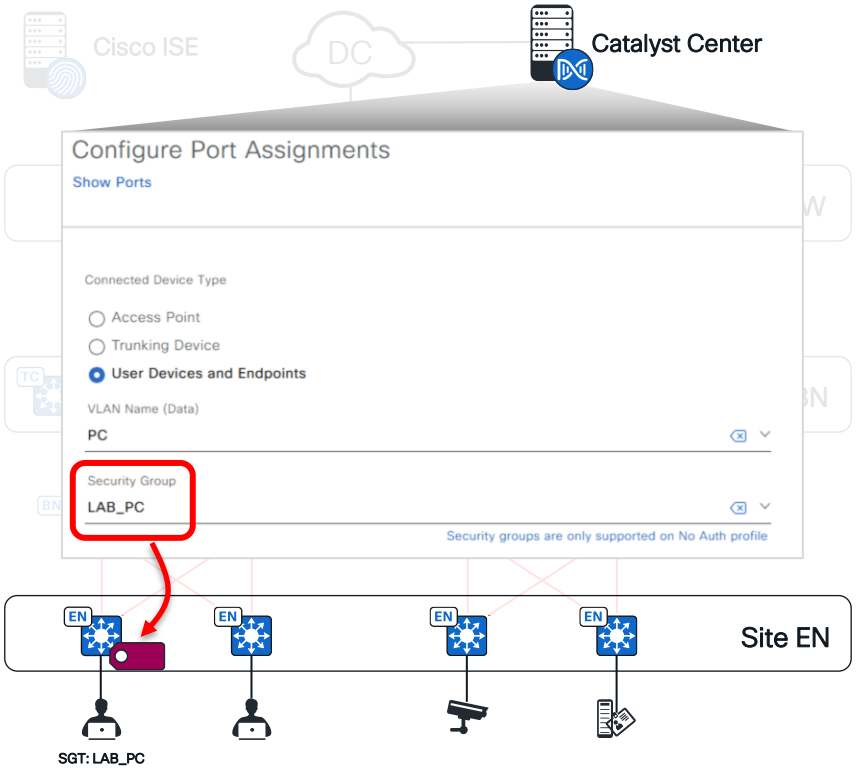
Classification

UNDERLAY

OVERLAY

Edge Nodes

Classification – Internal Endpoints



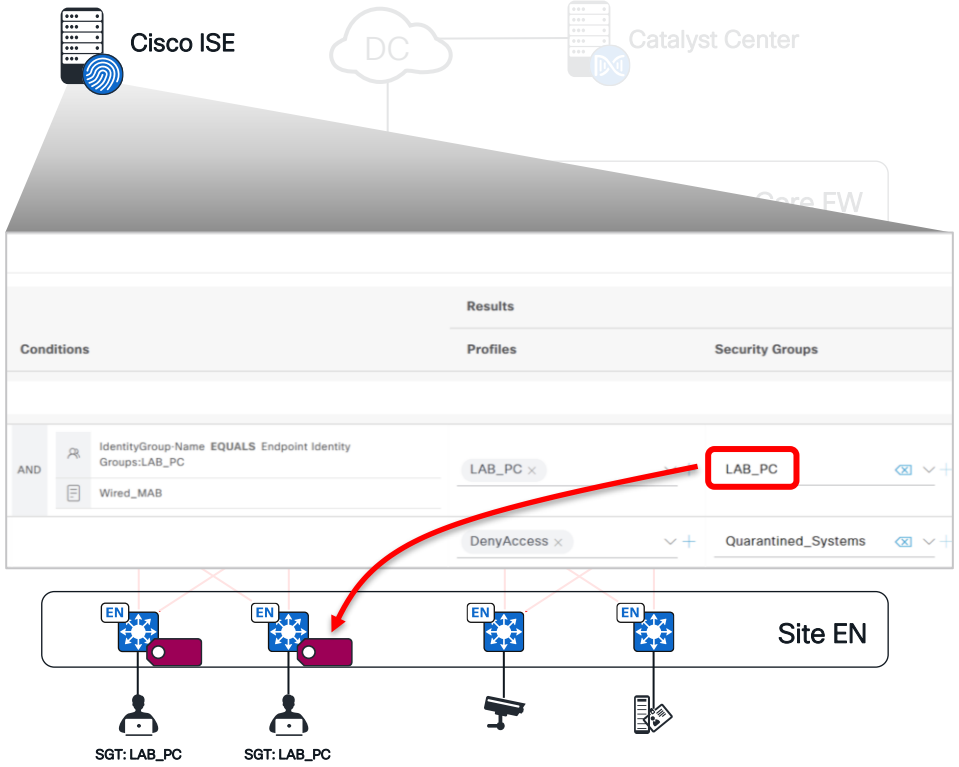
Edge Nodes

- Static per Interface
- Dynamic (802.1x)
- Static per VLAN

Recommendation

- Security Groups should not be left empty (especially if Static per VLAN SGT is empty)

Classification – Internal Endpoints



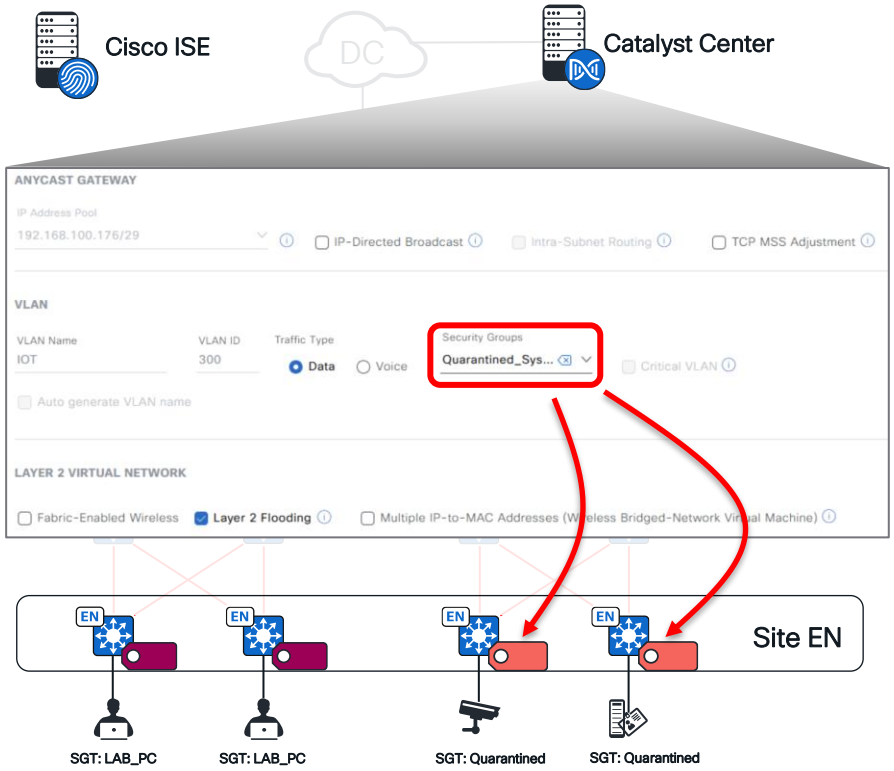
Edge Nodes

- Static per Interface
- Dynamic (802.1x)
- Static per VLAN

Recommendation

- Security Groups should not be left empty (especially if Static per VLAN SGT is empty)

Classification – Internal Endpoints



Edge Nodes

- Static per Interface
- Dynamic (802.1x)
- Static per VLAN

Recommendations

- Security Groups should not be left empty.
- Use a default Quarantine SGT as much as possible

Classification – Internal Endpoints

Edge Nodes

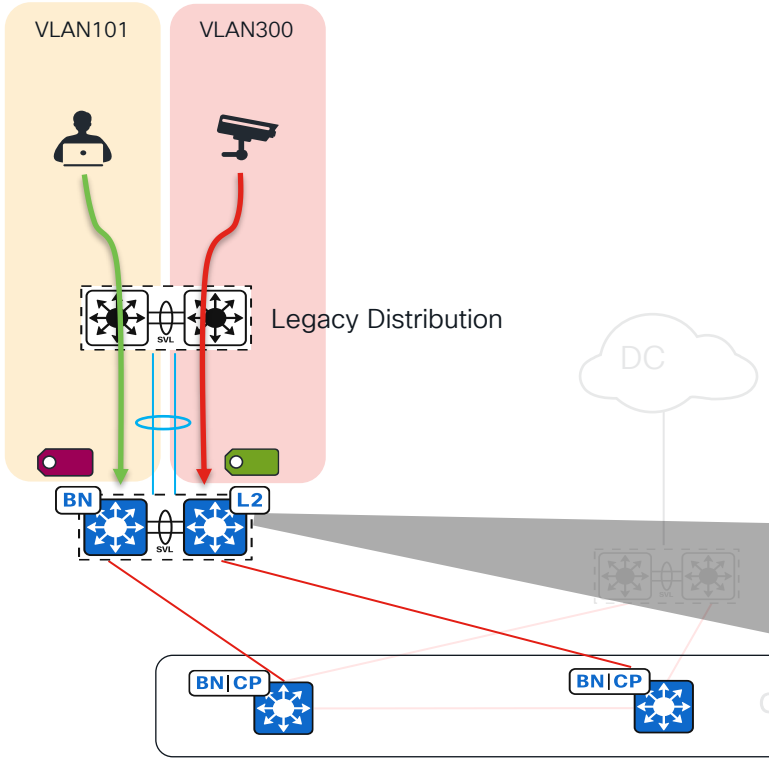
- Static per Interface
- Dynamic (802.1x)
- Static per VLAN

Recommendation

- Override the Quarantine SGT with the correct Endpoint SGT in ISE Authorization policy.

Border Nodes

Classification – External Endpoints (L2 Handoff)



Border Nodes

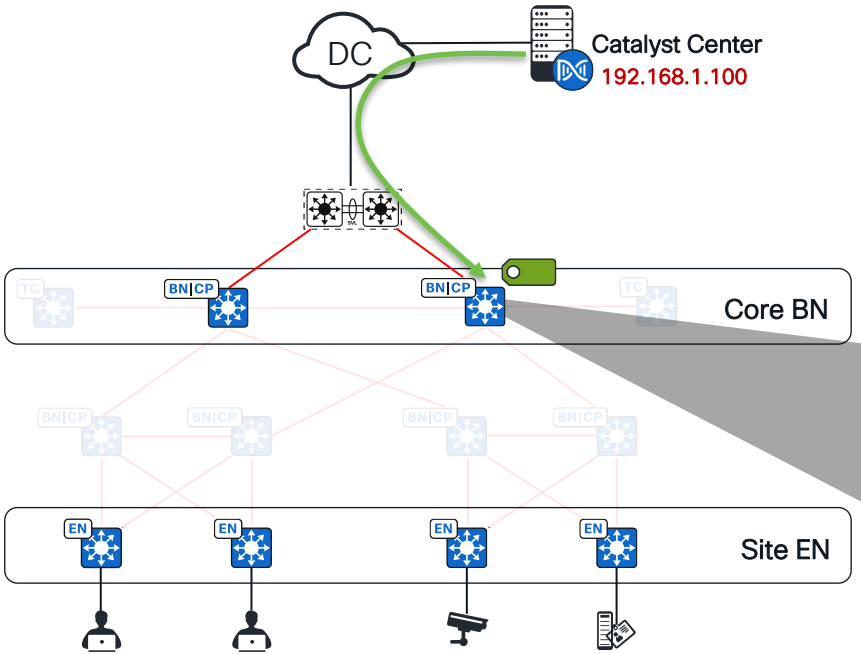
- Static VLAN to SGT Mapping

Use-cases

- Migration scenarios

```
DC-Border-3# sh run | i role-based
cts role-based sgt-map vlan-list 101 sgt 18
cts role-based sgt-map vlan-list 300 sgt 19
```

Classification – External Endpoints (L3 handoff)

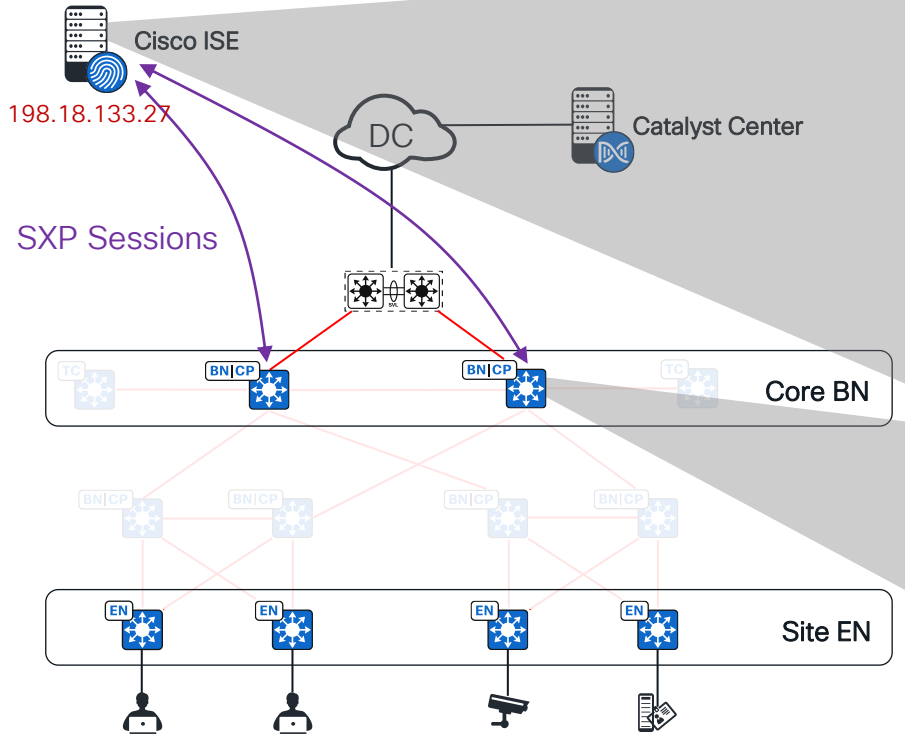


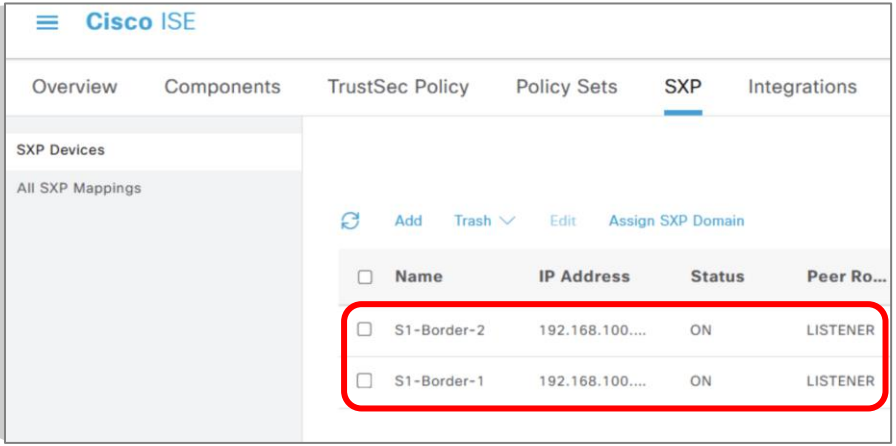
Border Nodes

- Static per IP or Subnet

```
DC-Border-2# sh run | i sgt-map
cts role-based sgt-map vrf CORP_VN 192.168.1.100 sgt 23
```

Classification – External Endpoints



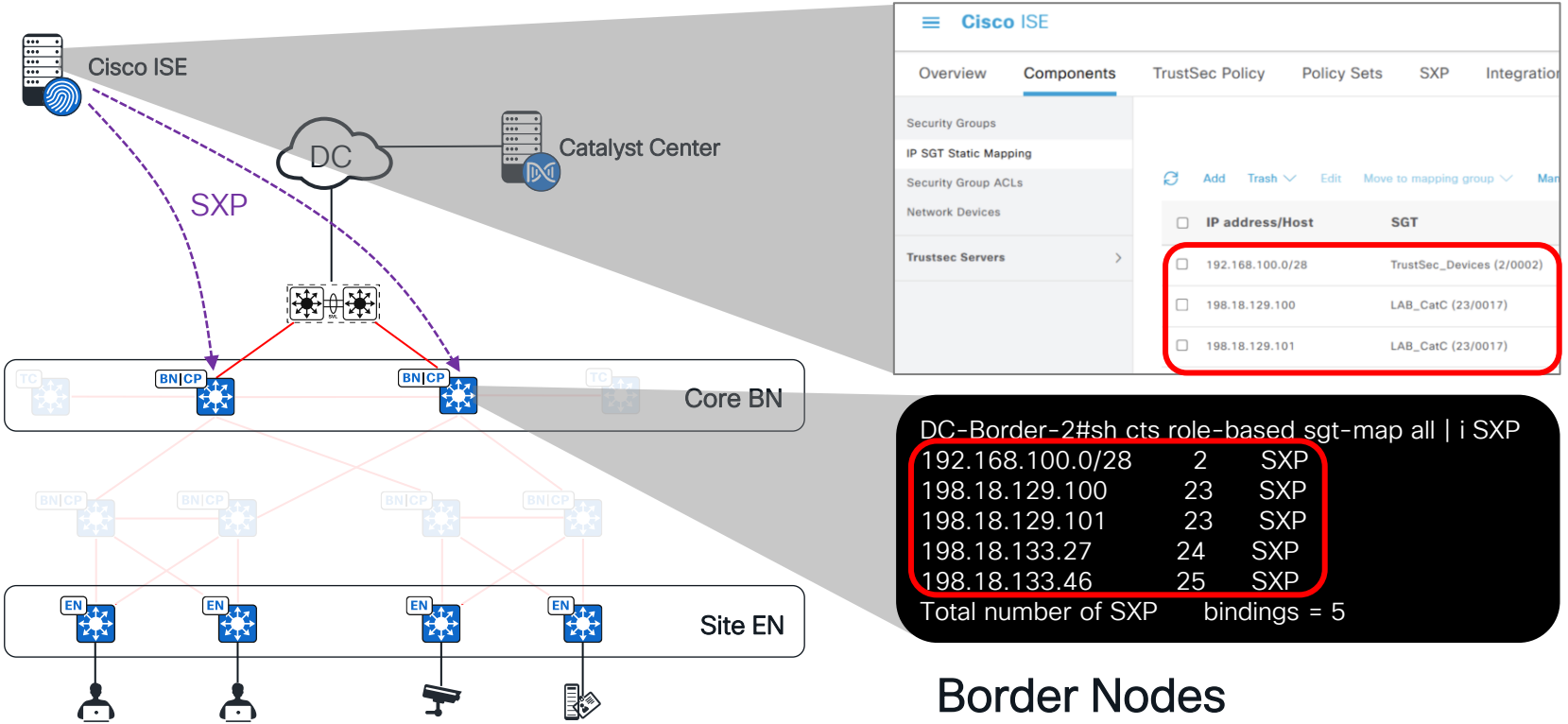



```
DC-Border-2#sh run | i sxp
cts sxp enable
cts sxp default password 7 13211913085D56796A
cts sxp connection peer 198.18.133.27 source 192.168.100.11
password default mode local listener hold-time 0 0
```

Border Nodes

- Dynamic (SXP)

Classification – External Endpoints

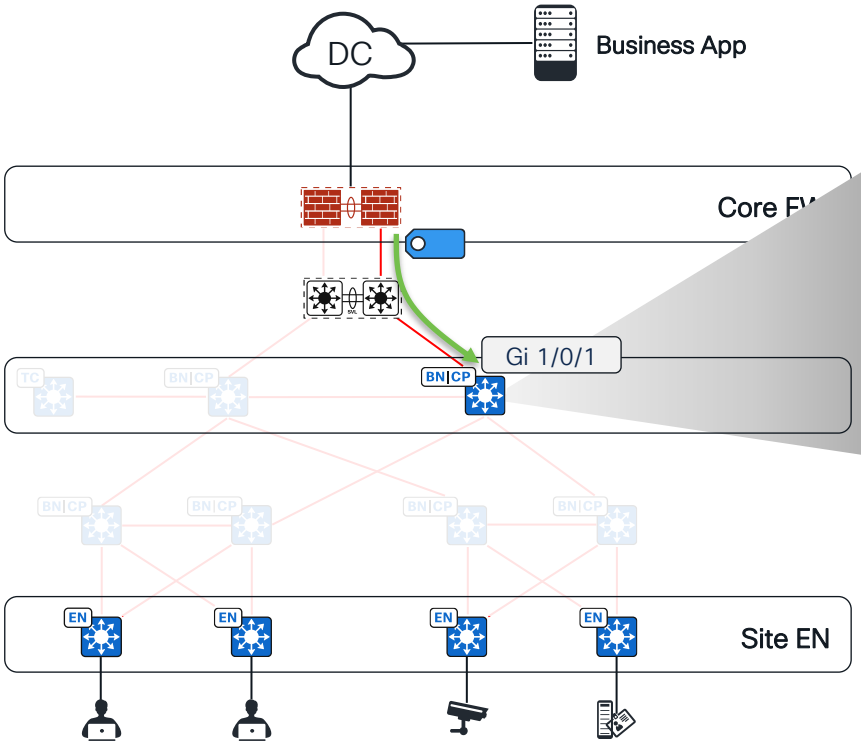



```
DC-Border-2#sh cts role-based sgt-map all | i SXP
192.168.100.0/28      2      SXP
198.18.129.100        23     SXP
198.18.129.101        23     SXP
198.18.133.27         24     SXP
198.18.133.46         25     SXP
Total number of SXP       bindings = 5
```

Border Nodes

- Dynamic (SXP)

Classification – External Endpoints



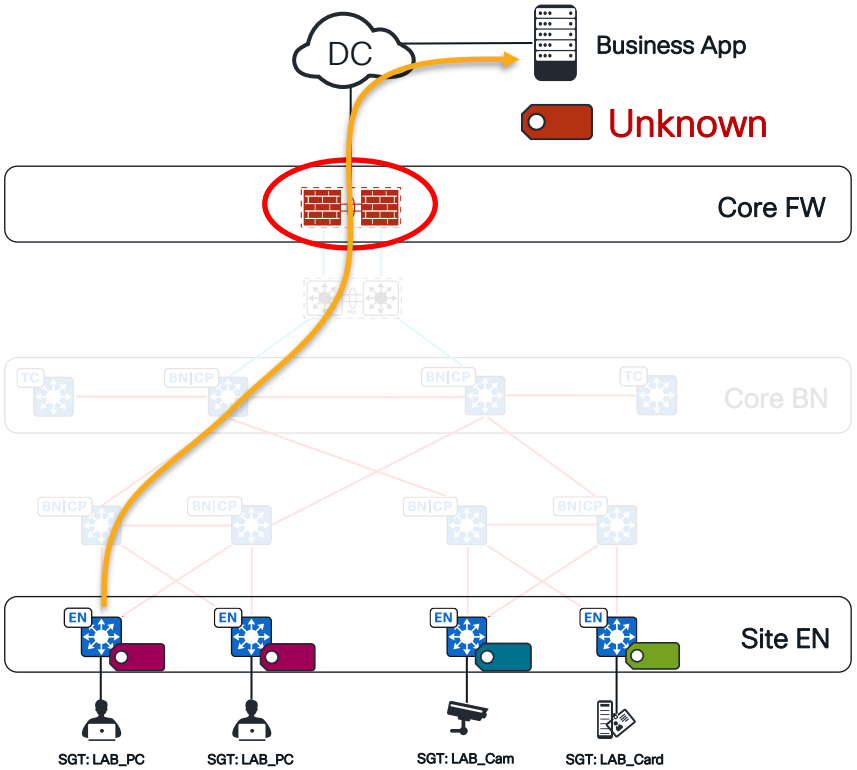

```
DC-Border-2# sh run int Gi1/0/1
...
interface GigabitEthernet1/0/1
 description L3-Handoff link
 cts manual
  policy static sgt 8000 trust
  propagate sgt (hidden)
 ...
```

Trusted Classification

- Trust SGT in the incoming CMD headers.
- If no CMD header is found, classify the packet with SGT 8000

Rules of thumbs

Classification – Unknown Endpoints

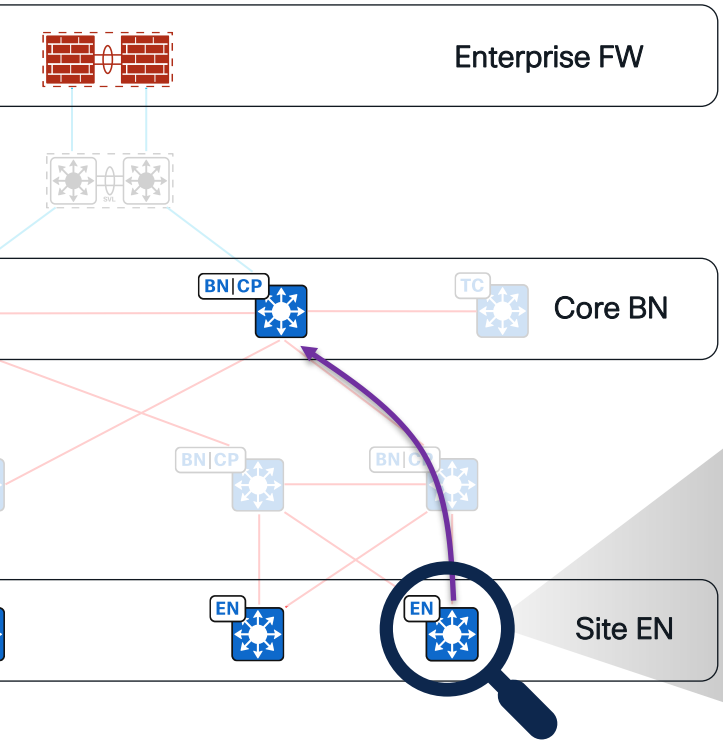


Rules of thumbs

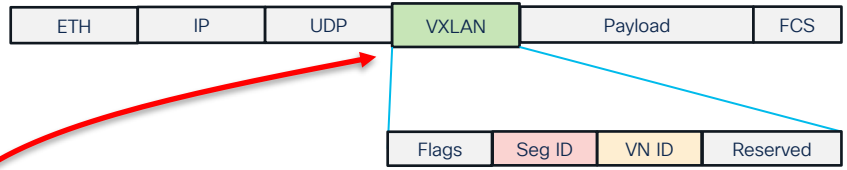
- SGT 0 (Unknown) should be left outside the fabric behind a Firewall.
- Following this rule will greatly simplify Enforcement policies.

Propagation

Propagation – Dataplane

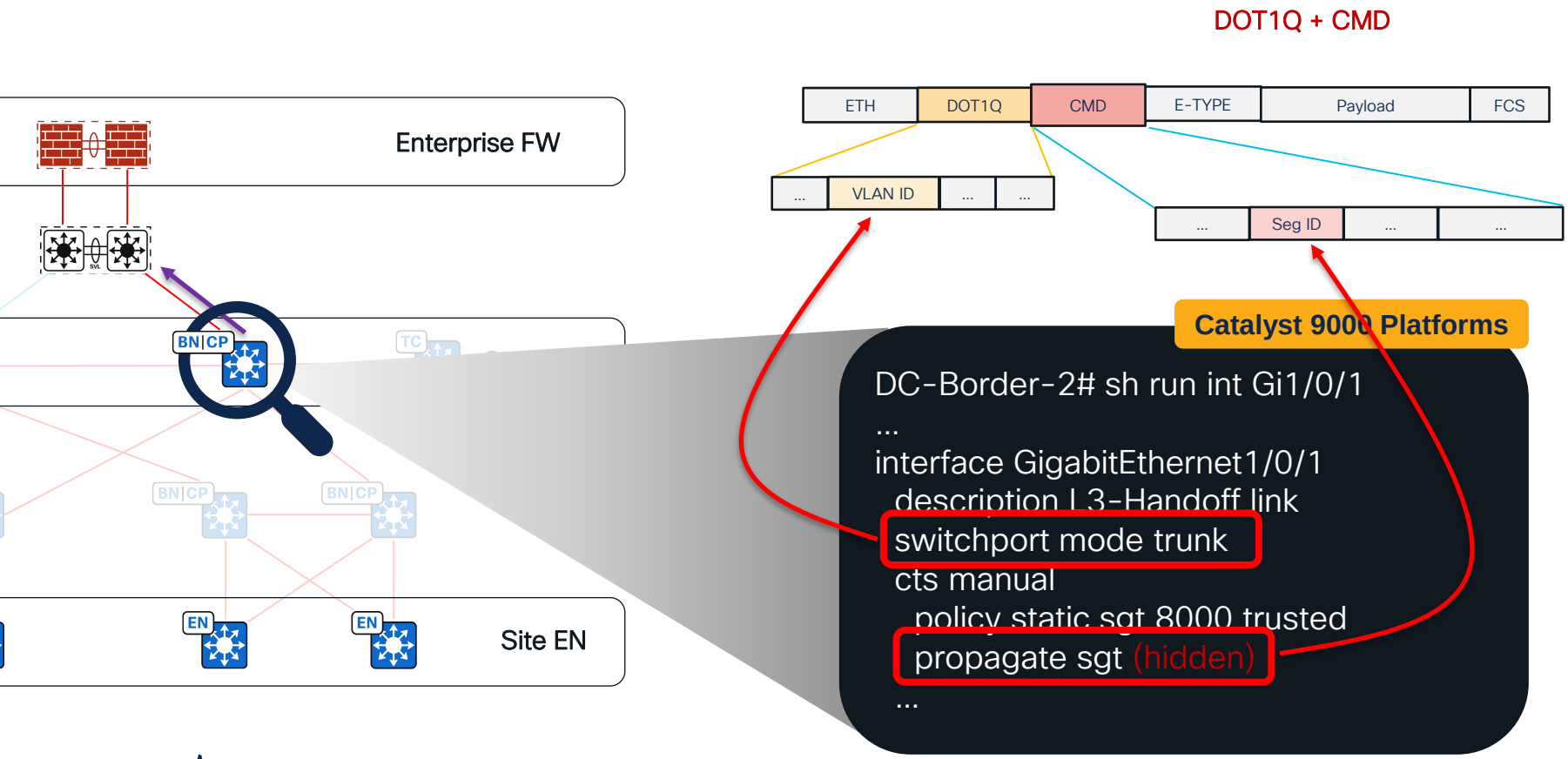


VxLAN-GPO

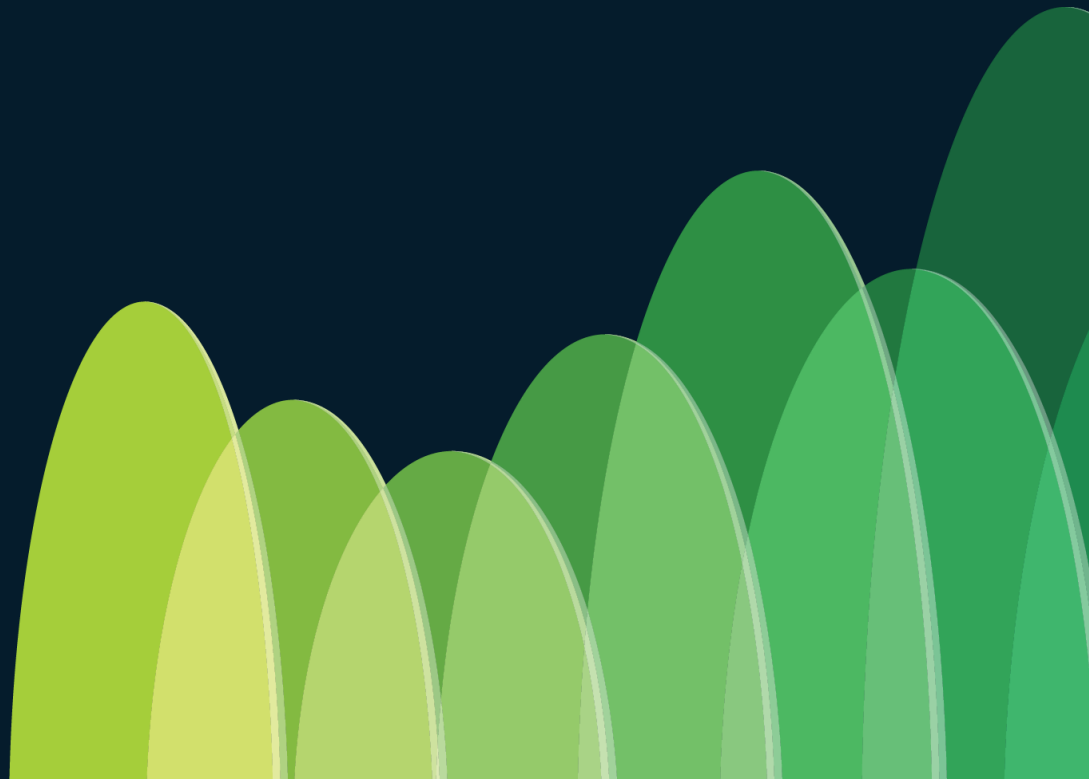



```
router lisp
 domain-id 502766789
 locator-table default
 locator-set rloc_abcff49d-e0a6-4cc5-9f86-9d67136d740a
  IPv4-interface Loopback0 priority 10 weight 10
  exit-locator-set
 !
 locator default-set rloc_abcff49d-e0a6-4cc5-9f86-9d67136d740a
 service ipv4
  encapsulation vxlan
  itr map-resolver 192.168.100.11
  itr map-resolver 192.168.100.12
  etr map-server 192.168.100.11 key 7 065E5E244A1C5F1C0146410A08507C7A71
  etr map-server 192.168.100.11 proxy-reply
  etr map-server 192.168.100.12 key 7 1241541214595A012E7A77293761744252
  etr map-server 192.168.100.12 proxy-reply
  etr
  sgt
  no map-cache away-eids send-map-request
  proxy-itr 192.168.100.14
  exit-service-ipv4
 !
```

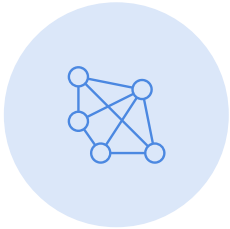
Propagation – Dataplane



Enforcement



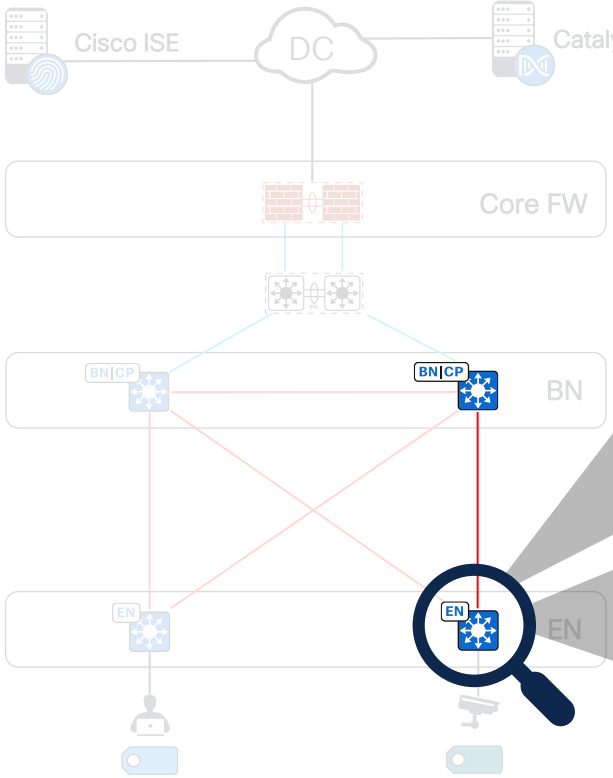
Enforcement



UNDERLAY

OVERLAY

Enforcement – Edges



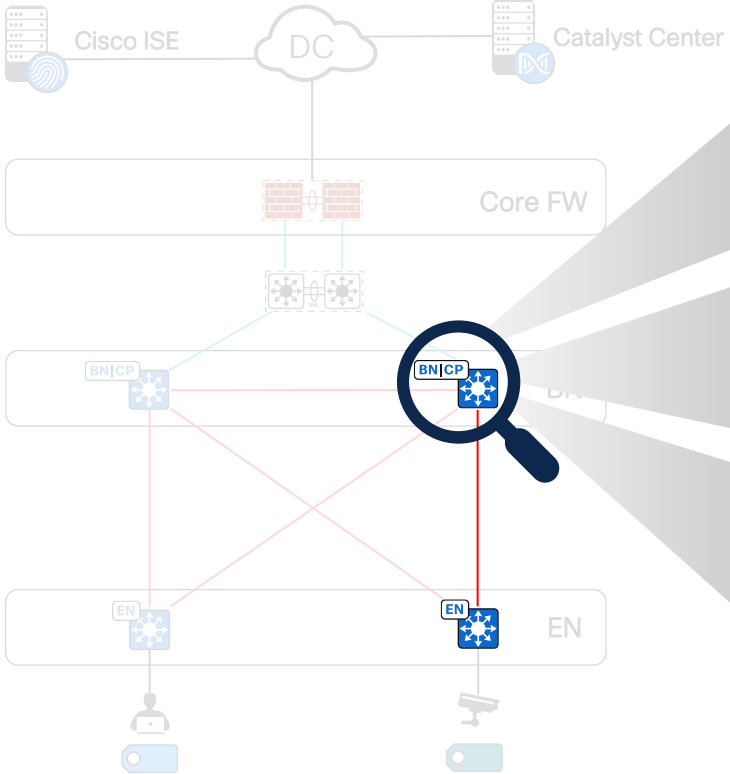
LAN Automated prior Catalyst Center 2.3.7.4

```
S1-Edge-2# sh run all
...
cts role-based enforcement
...
interface GigabitEthernet1/0/2
 description Fabric link
 cts role-based enforcement (hidden)
 ...
```

LAN Automated by Catalyst Center 2.3.7.4

```
S1-Edge-2# sh run all
...
cts role-based enforcement
...
interface GigabitEthernet1/0/2
 description Fabric link
 no cts role-based enforcement
 ...
```

Enforcement – Borders



LAN Automated prior DNAC 2.3.3.x

```
S1-Border-2# sh run all
...
interface GigabitEthernet1/0/2
 description Fabric link
 cts role-based enforcement (hidden)
 ...
```

LAN Automated by DNA Center 2.3.3.x

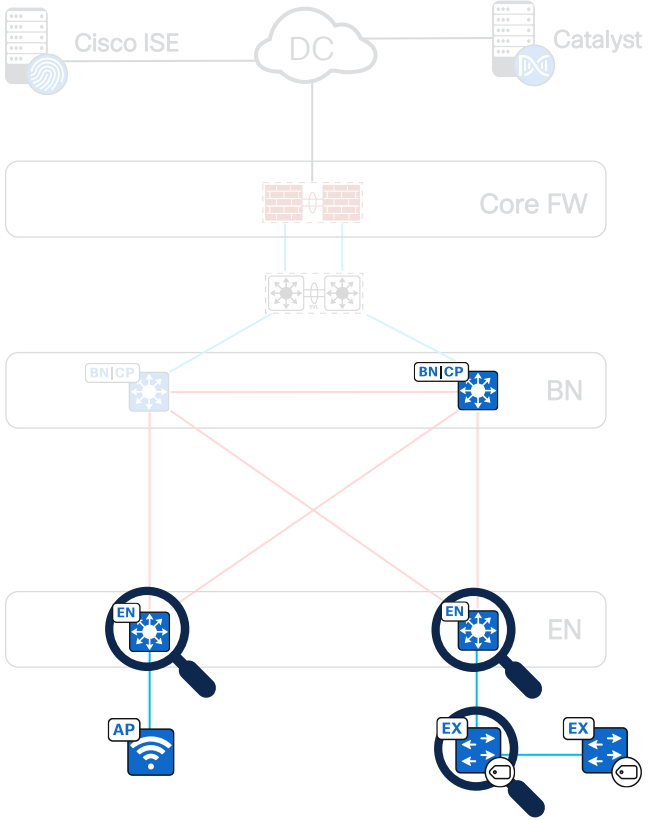
```
S1-Border-2# sh run all

cts role-based enforcement
...
interface GigabitEthernet1/0/2
 description Fabric link
 cts role-based enforcement (hidden)
 ...
```

LAN Automated by Catalyst Center 2.3.7.4

```
S1-Border-2# sh run all
...
cts role-based enforcement
...
interface GigabitEthernet1/0/2
 description Fabric link
 no cts role-based enforcement
 ...
```

Enforcement – (P)EN and Fabric AP Mgmt VLANs



Starting from Catalyst Center 2.3.7.6

- CTS role-based enforcement on AP & PEN/SBEN VLANs is disabled.
- CTS role-based enforcement on Edge Node downlinks facing PEN/SBEN is disabled.
- CTS role-based enforcement on PEN/SBEN uplink/downlinks connecting to Edge or PEN/SBEN is disabled.

Enforcement

UNDERLAY

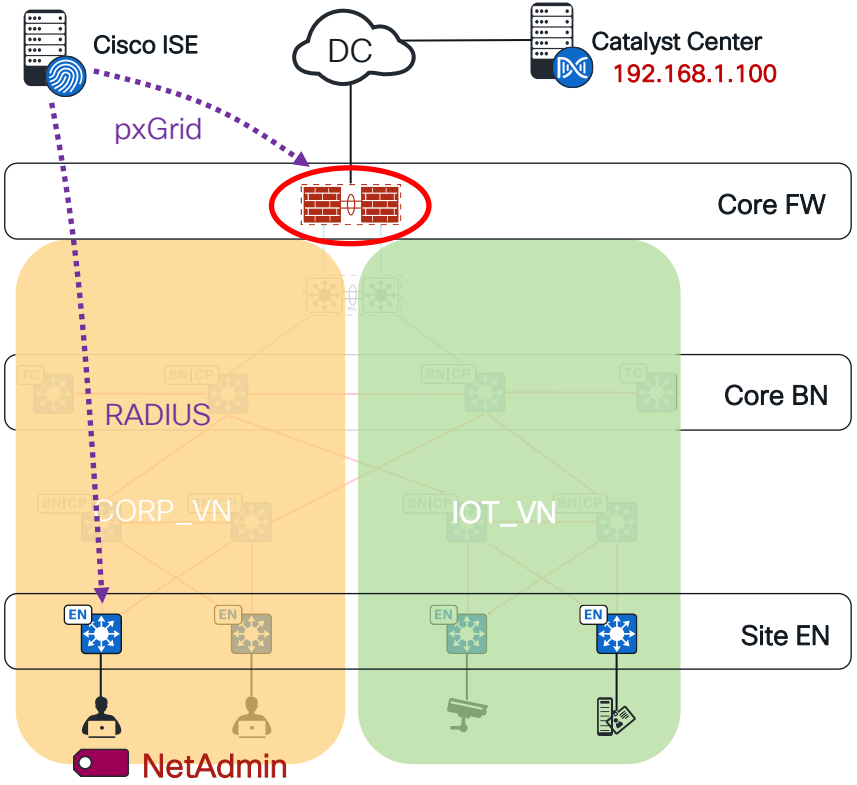
OVERLAY

Enterprise Firewall

(Macro-Seg)

cisco Live!

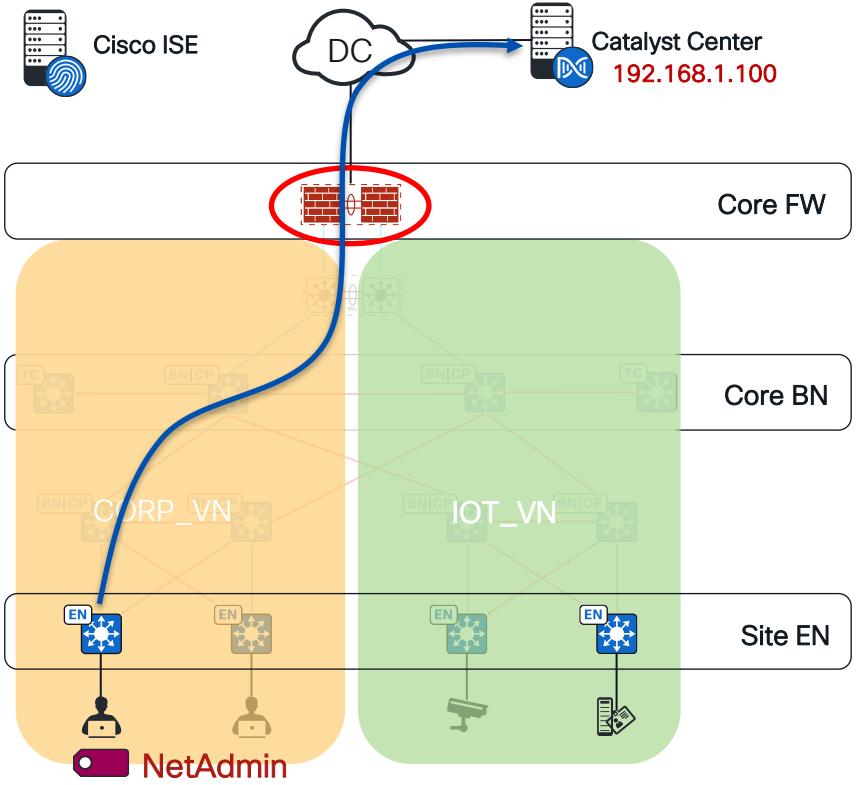
Enforcement



Enterprise Firewall

- Stateful inspection
- SGT sharing through pxGrid
- SGT to IP ruleset
- Protect North <-> South traffic
- Protect VN-to-VN communications

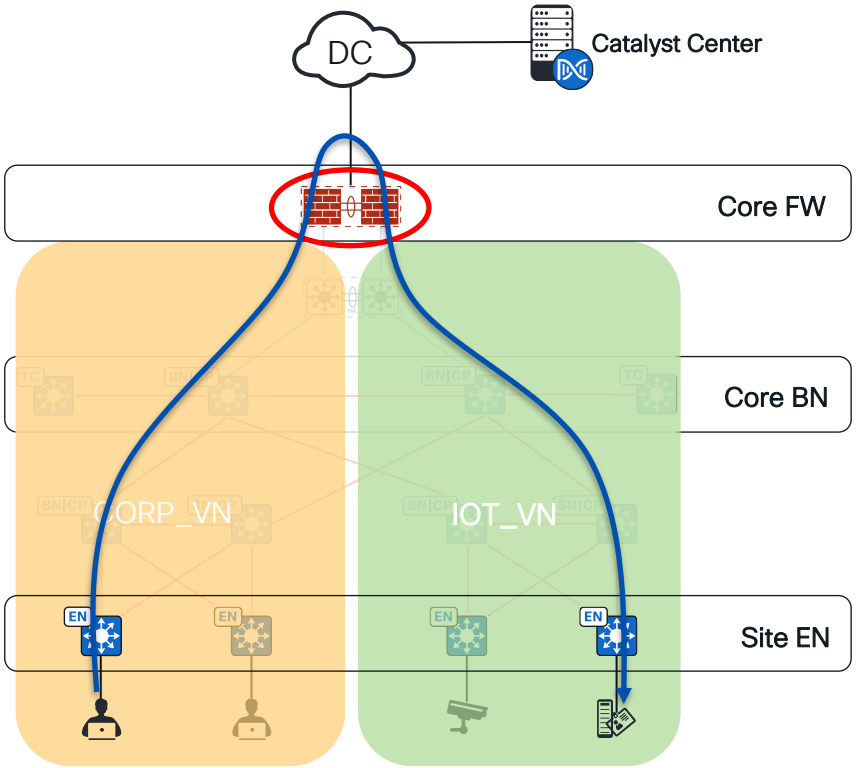
Enforcement



Enterprise Firewall

- Stateful inspection
- SGT sharing through pxGrid
- SGT to IP ruleset
- Protect North <-> South traffic
- Protect VN-to-VN communications

Enforcement

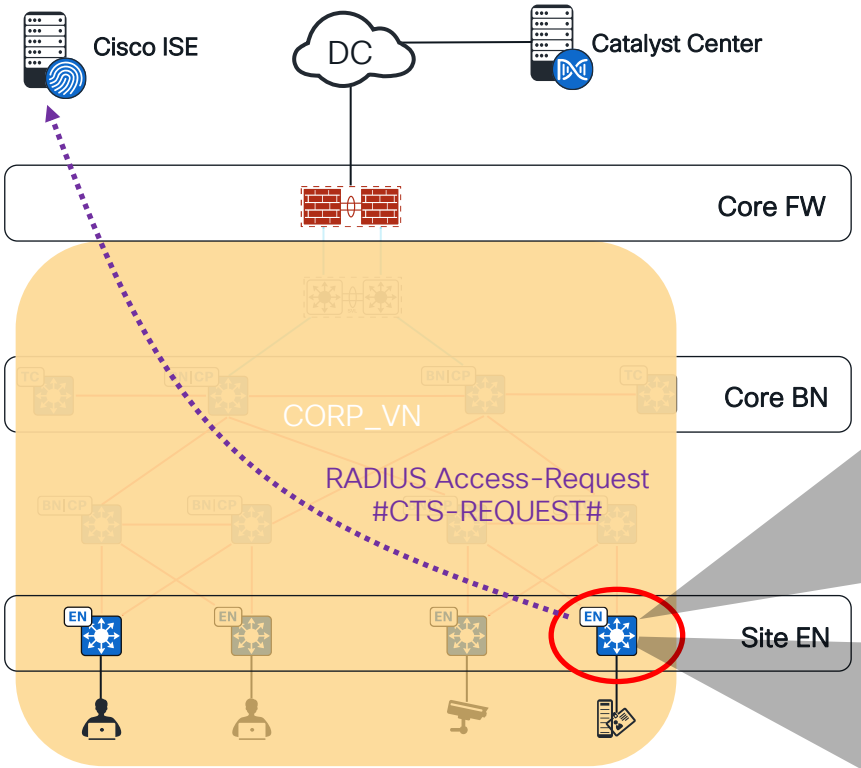


Enterprise Firewall

- Stateful inspection
- SGT sharing through PxGrid
- SGT to IP ruleset
- Protect North <-> South traffic
- Protect VN-to-VN communications

Edge Nodes (Micro-Seg)

Enforcement



Edge Nodes

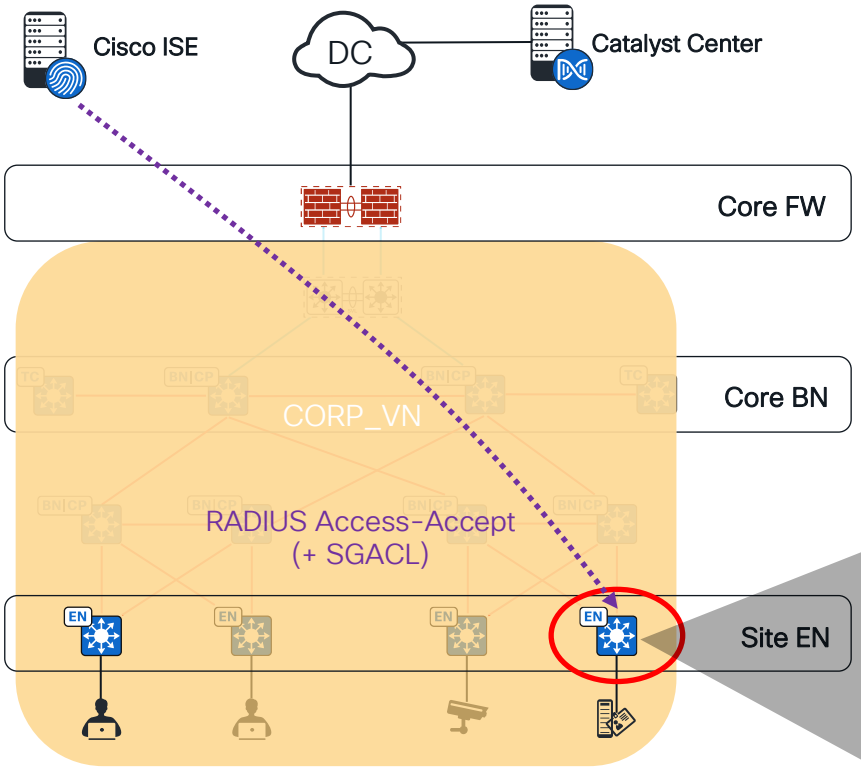
- Stateless inspection
- Protect East <-> West traffic

```
S1-Edge-2#sh run | i enforcement
cts role-based enforcement
cts role-based enforcement vlan-list 101,300
```

```
S1-Edge-2#sh cts role-based sgt-map vrf IOT_VN all
%IPv6 protocol is not enabled in VRF IOT_VN
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
192.168.100.177         2       INTERNAL
192.168.100.179         20      LOCAL
```

Enforcement

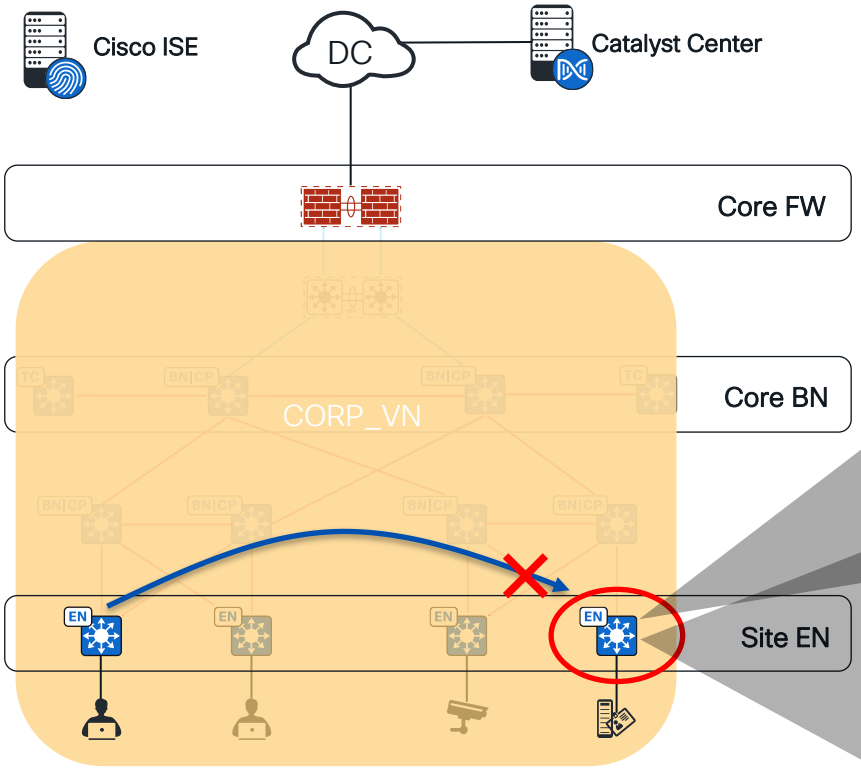


Edge Nodes

- Stateless inspection
- Protect East <-> West traffic

```
S1-Edge-2#sh cts role-based permissions
IPv4 Role-based permissions default:
       Deny_IP_Log-00
IPv4 Role-based permissions from group 18:LAB_PC to group Unknown:
       Permit IP-00
IPv4 Role-based permissions from group 19:LAB_Cameras to group Unknown:
       Permit IP-00
IPv4 Role-based permissions from group 20:LAB_CardReaders to group Unknown:
       Permit IP-00
IPv4 Role-based permissions from group 22:LAB_Printer to group Unknown:
       Permit IP-00
IPv4 Role-based permissions from group 23:LAB_CatC to group 2:TrustSec_Devices:
       Permit IP-00
IPv4 Role-based permissions from group 24:LAB_ISE to group 2:TrustSec_Devices:
       Permit IP-00
```

Enforcement



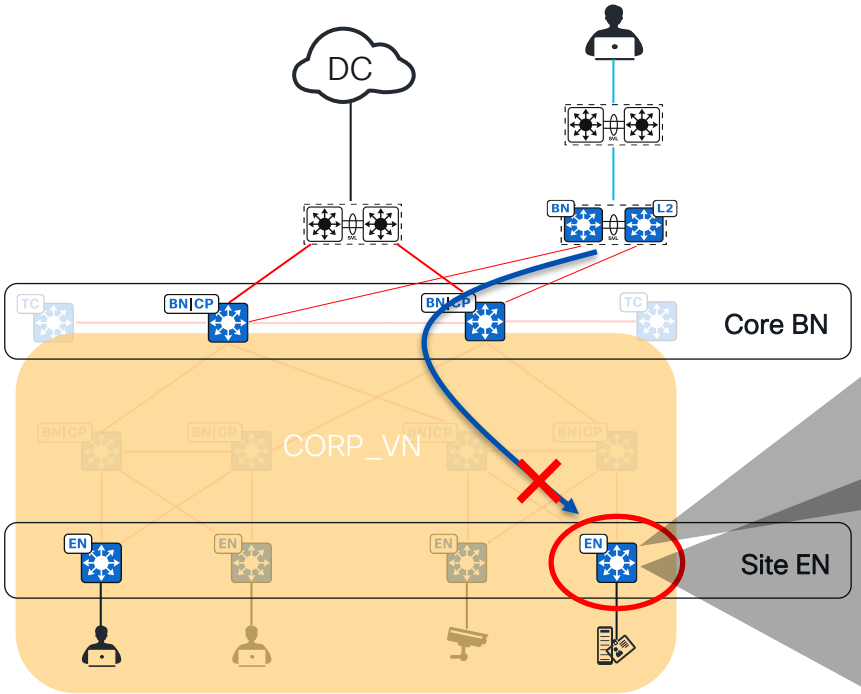
Edge Nodes

- Stateless inspection
- Protect East <-> West traffic

```
S1-Edge-2#sh run | i enforcement
cts role-based enforcement
cts role-based enforcement vlan-list 101,300
```

```
IPv4 Role-based permissions default:
        Deny_IP_Log-00
        Permit IP-00
IPv4 Role-based permissions from group 19:LAB_Cameras to group Unknown:
        Permit IP-00
IPv4 Role-based permissions from group 20:LAB_CardReaders to group Unknown:
        Permit IP-00
IPv4 Role-based permissions from group 22:LAB_Printer to group Unknown:
        Permit IP-00
IPv4 Role-based permissions from group 23:LAB_CatC to group 2:TrustSec_Devices:
        Permit IP-00
IPv4 Role-based permissions from group 24:LAB_ISE to group 2:TrustSec_Devices:
        Permit IP-00
```

Enforcement



Edge Nodes

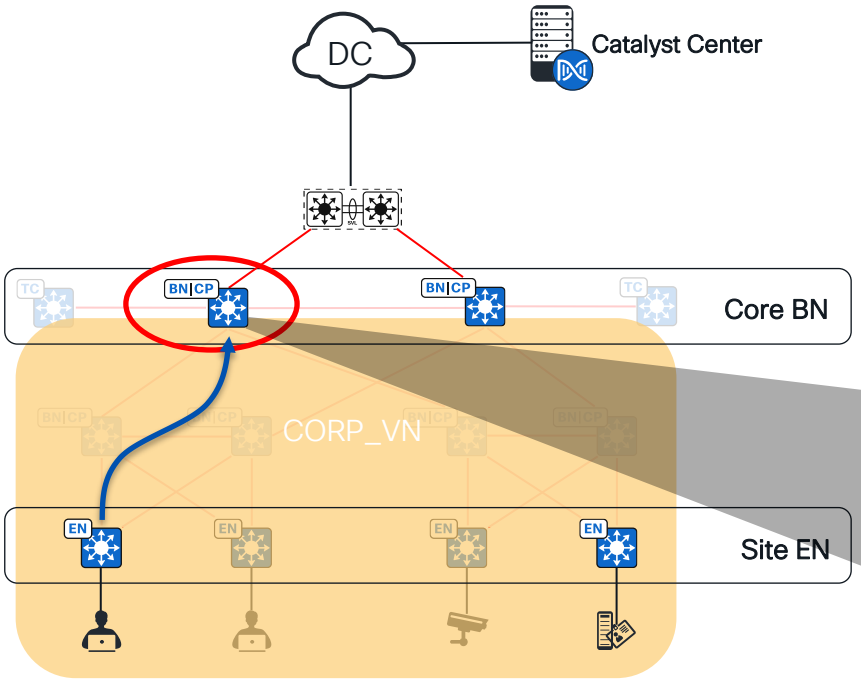
- Stateless inspection
- Protect North -> South traffic

```
S1-Edge-2#sh run | i enforcement
cts role-based enforcement
cts role-based enforcement vlan-list 101,300
```

```
S1-Edge-2#sh cts role-based permissions
IPv4 Role-based permissions default:
        Deny_IP_Log-00
IPv4 Role-based permissions from group 18:LAB_PC to group Unknown:
        Permit IP-00
IPv4 Role-based permissions from group 19:LAB_Cameras to group Unknown:
        Permit IP-00
IPv4 Role-based permissions from group 20:LAB_CardReaders to group Unknown:
        Permit IP-00
IPv4 Role-based permissions from group 22:LAB_Printer to group Unknown:
        Permit IP-00
IPv4 Role-based permissions from group 23:LAB_CatC to group 2:TrustSec_Devices:
        Permit IP-00
IPv4 Role-based permissions from group 24:LAB_ISE to group 2:TrustSec_Devices:
        Permit IP-00
```

Border Nodes (Micro-Seg)

Enforcement

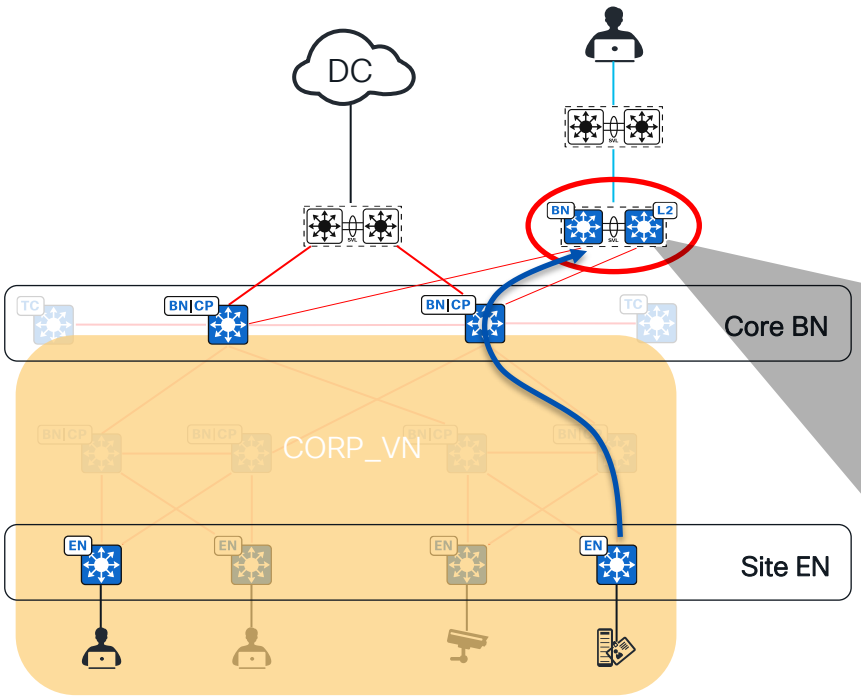


Border Nodes (L3 Handoff)

- Stateless inspection
- Protect South -> North traffic

```
DC-Border-1# sh run | i role-based
cts role-based enforcement vlan-list 3000-3002
```

Enforcement

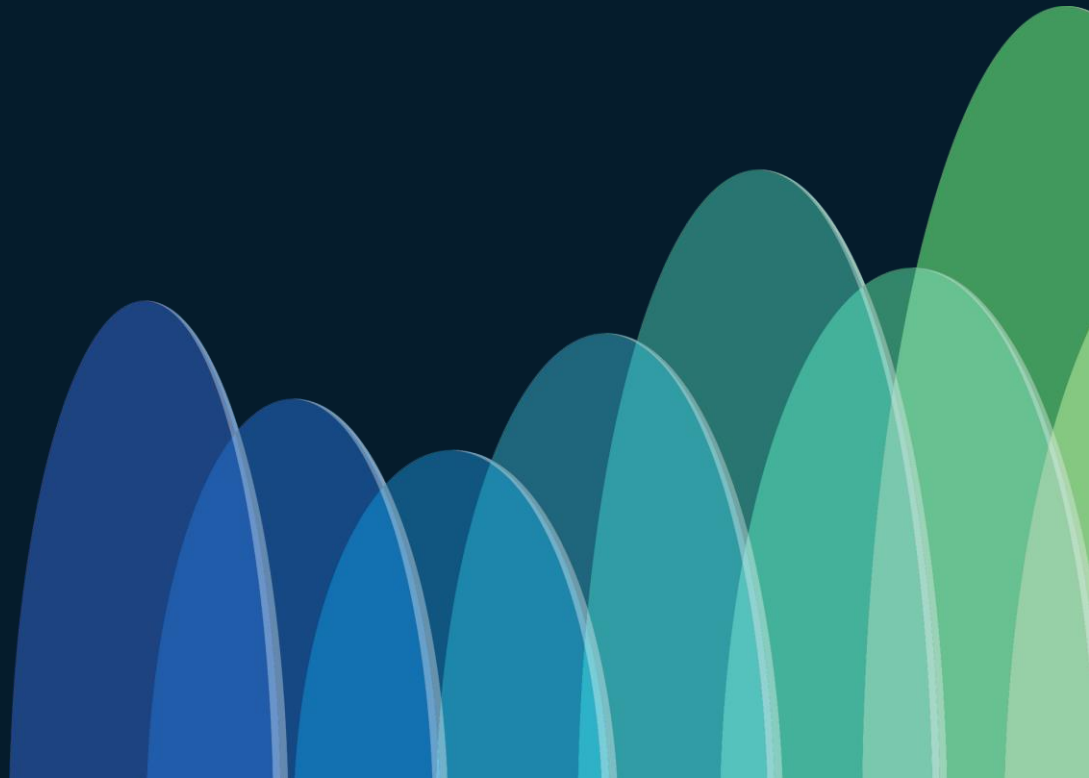


Border Nodes (L2 Handoff)

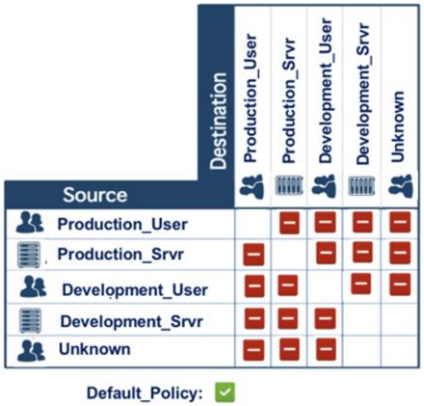
- Stateless inspection
- Protect South -> North traffic

```
DC-Border-3# sh run | i role-based
cts role-based enforcement vlan-list 101,300
```

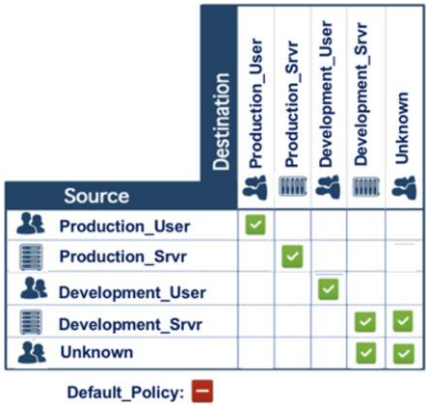
Trustsec Models



TrustSec Models



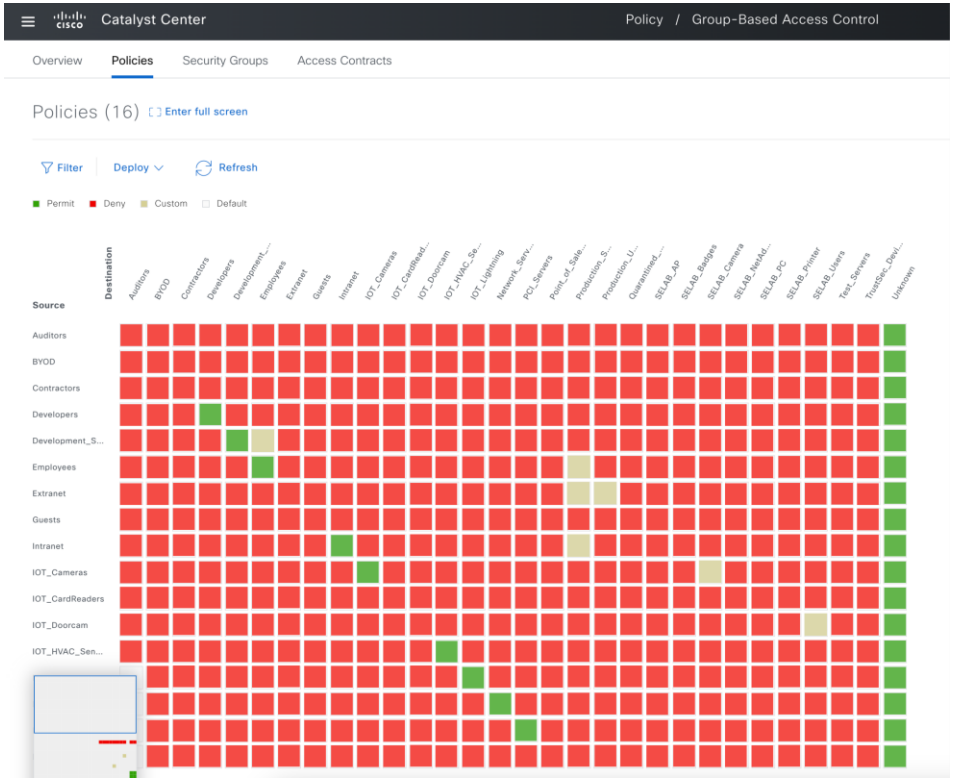
Deny-List



Allow-List

Failed design

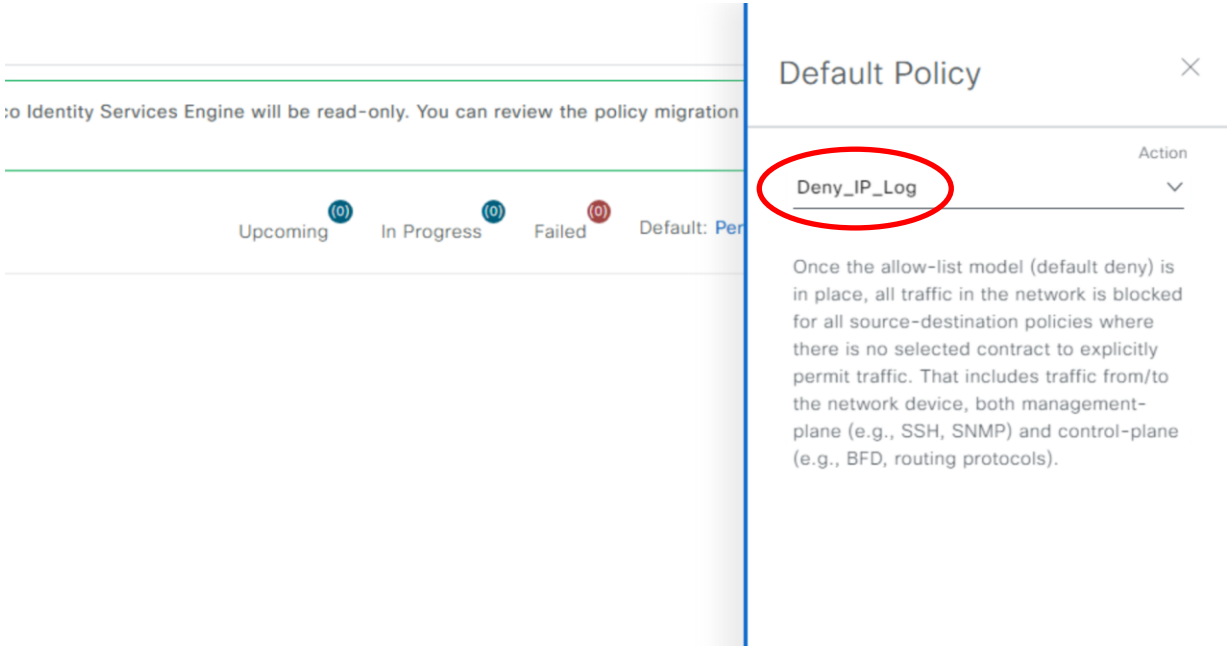
Seen this before ?



Logging

Logging

Turn logging on !



C9200-C9600

Enhanced SGACL Logging

Prior to IOS-XE 17.3

Any packet that matches an SGACL causes an informational logging message about the packet to be sent to the console. In releases prior to Cisco IOS-XE Amsterdam 17.3.1, SGACL logging was done as a CPU-intensive mechanism

IOS-XE 17.3

From Cisco IOS-XE Amsterdam 17.3.1 release, SGACL logging has been enhanced to use NetFlow hardware, which allows much larger logging rates.

SGACL Logging for 9500X, 9600X not supported

SGACL Logging Scale

Platform	Theoretical Scale (for 5 mins)	Measured Scale (for 5 mins)
Catalyst 9300, 9400, 9500	14948	16000
Catalyst 9500 High Performance and 9600	29023	32000
Catalyst 9200	5950	8000

Configuration

```
Switch(config)# ip access-list role-based acl18to21
Switch(config-rb-acl)# permit tcp src eq 57 log
Switch(config-rb-acl)# exit
Switch(config)# cts role-based enforcement
Switch(config)# cts role-based permissions from 18 to 21 acl18to21
```

Example SYSLOG by previous PUNT mechanism:

```
Switch#
Feb 28 12:48:17.236 IST: %IP-6-ACCESSLOGP:
list acl18to21 denied tcp 9.1.1.2 -> 5.1.1.2, 1 packet
```

Example SYSLOG by Enhanced mechanism:

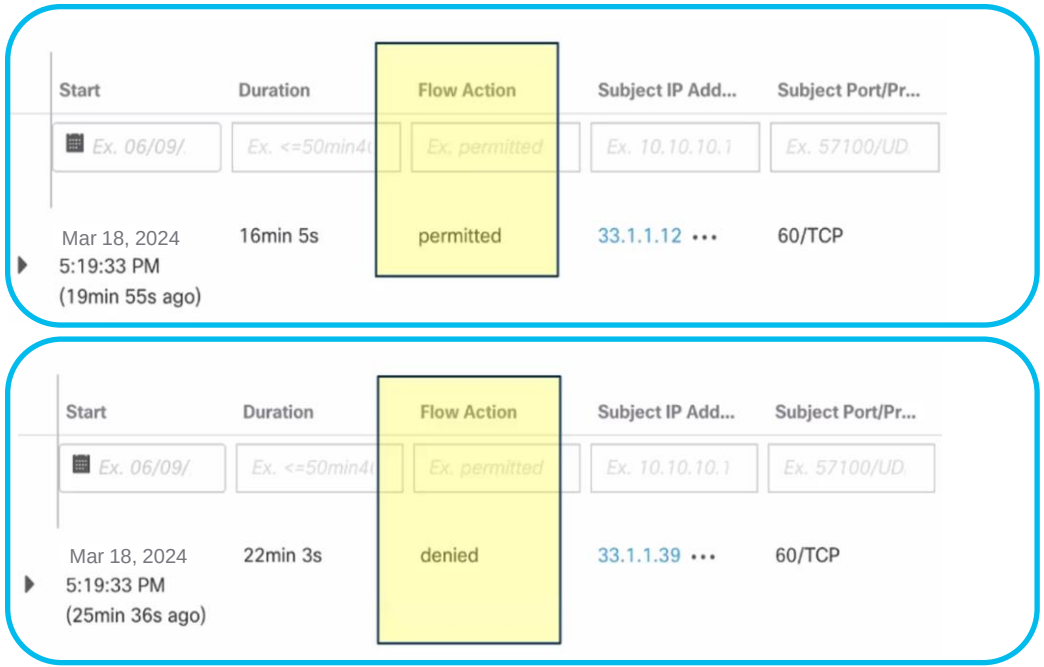
```
Switch#
Feb 28 12:25:13.135 IST: %RBM-6-SGACLHIT:
ingress_interface='HundredGigE1/0/27' sgacl_name='acl18to21' action='Permit'
protocol='tcp' src-vrf='default' src-ip='9.1.1.2' src-port='57' dest-
vrf='default' dest-ip='5.1.1.2' dest-port='101' sgt='18' dgt='21'
logging_interval_hits='3514841'
```

SGACL Enforcement Monitoring via NetFlow

IOS-XE 17.13 release supports export of firewallEvent (233) on Doppler ASIC platforms (92/93/94/95/9600).
SNA v7.4.2 has support for this field.

```
Flow record <record_name>
  match ipv6 version
  match ipv6 source address
  match ipv6 destination address
  match transport source-port
  match transport destination-port
  collect policy firewall event
!
Interface G1/0/1
  ipv6 flow monitor <monitor_name> output
```

firewallEvent (233) received by SNA:

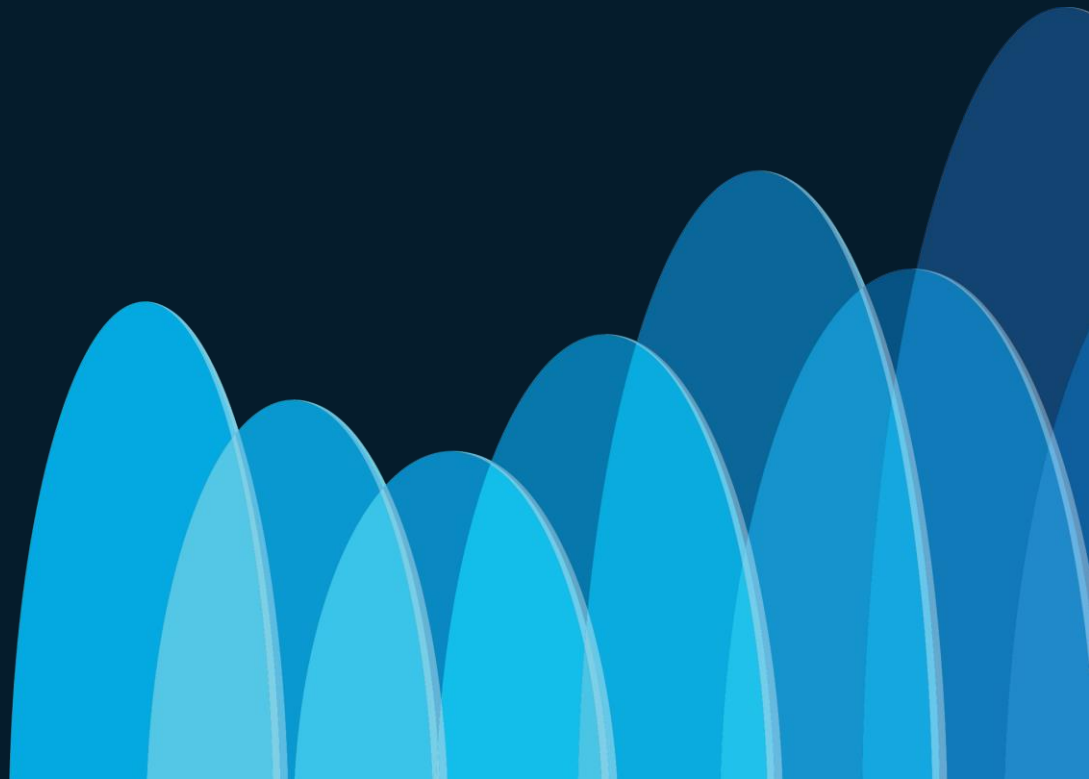


show flow monitor <monitor name> cache:
fw event: 1 (PERMIT) / 3 (DENY)

Agenda

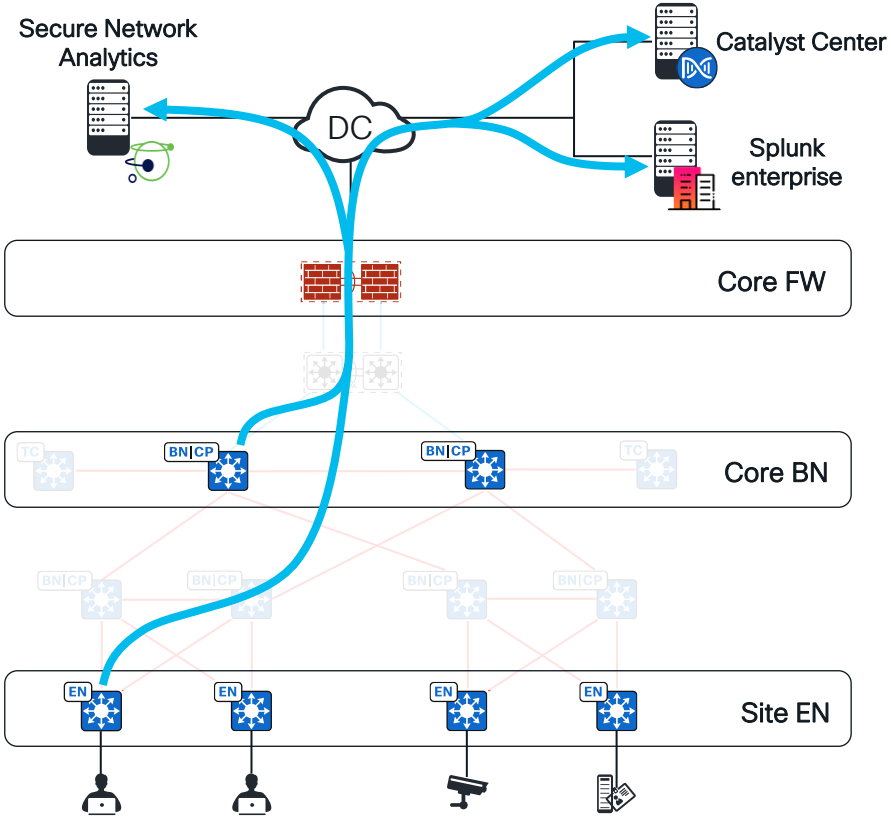
- Introduction
- Segmentation Strategy
- Observability Pipelines
- Deploy Allow-List Model
- Conclusions

Telemetry Broker



cisco Live!

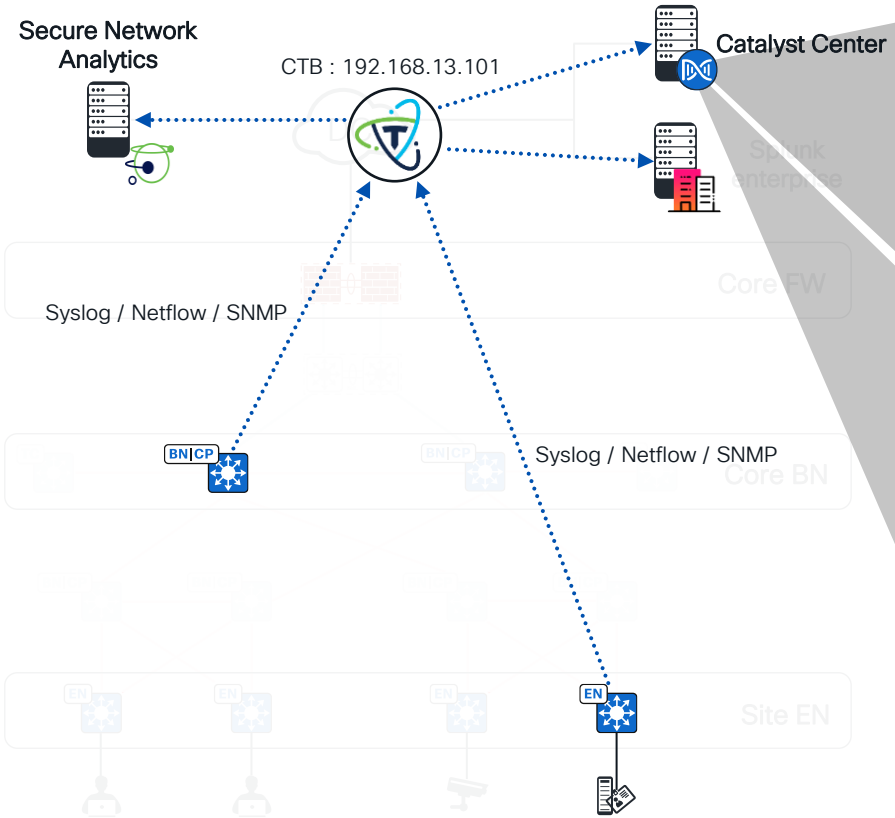
Telemetry Challenge

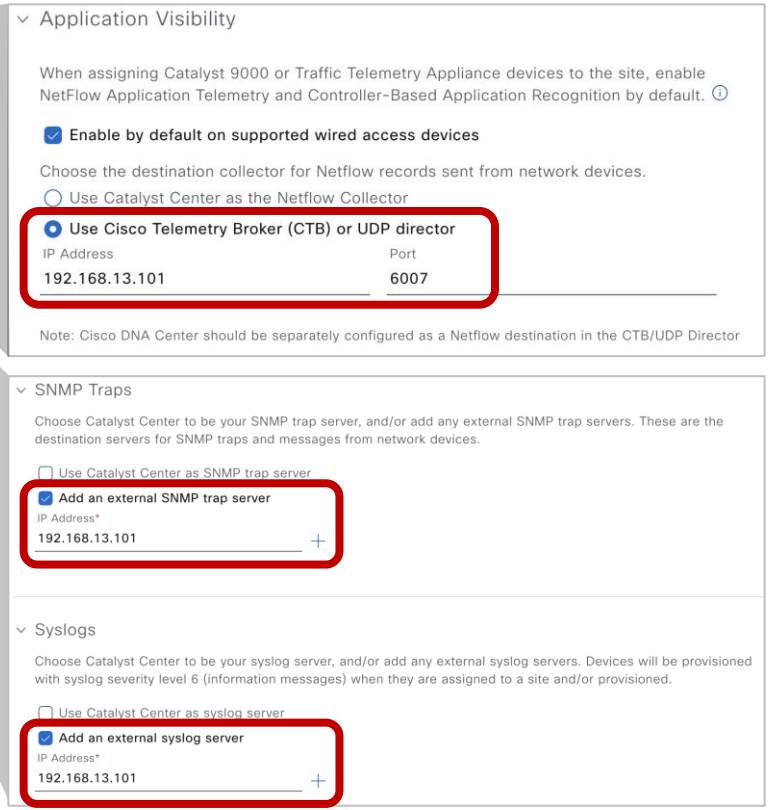


- TrustSec syslog sent to Splunk for analytics.
- System syslog sent to Catalyst Center for Assurance.
- Netflow sent to Catalyst Center, Splunk and SNA.

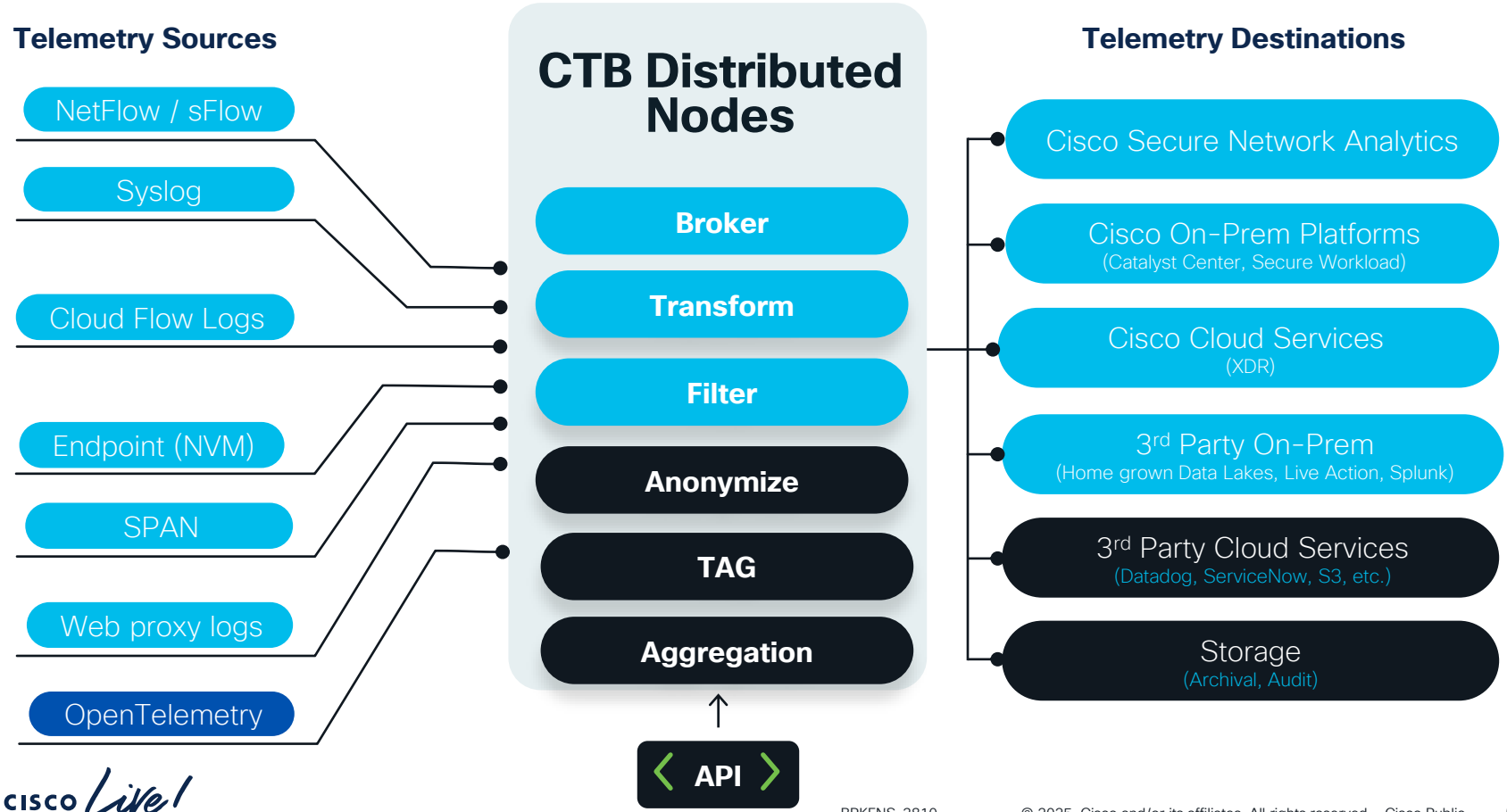
- Catalyst 9000 Series switches can only send netflow to two destinations
- Advanced telemetry such as AVC and ETA require compute resources

Telemetry Solution

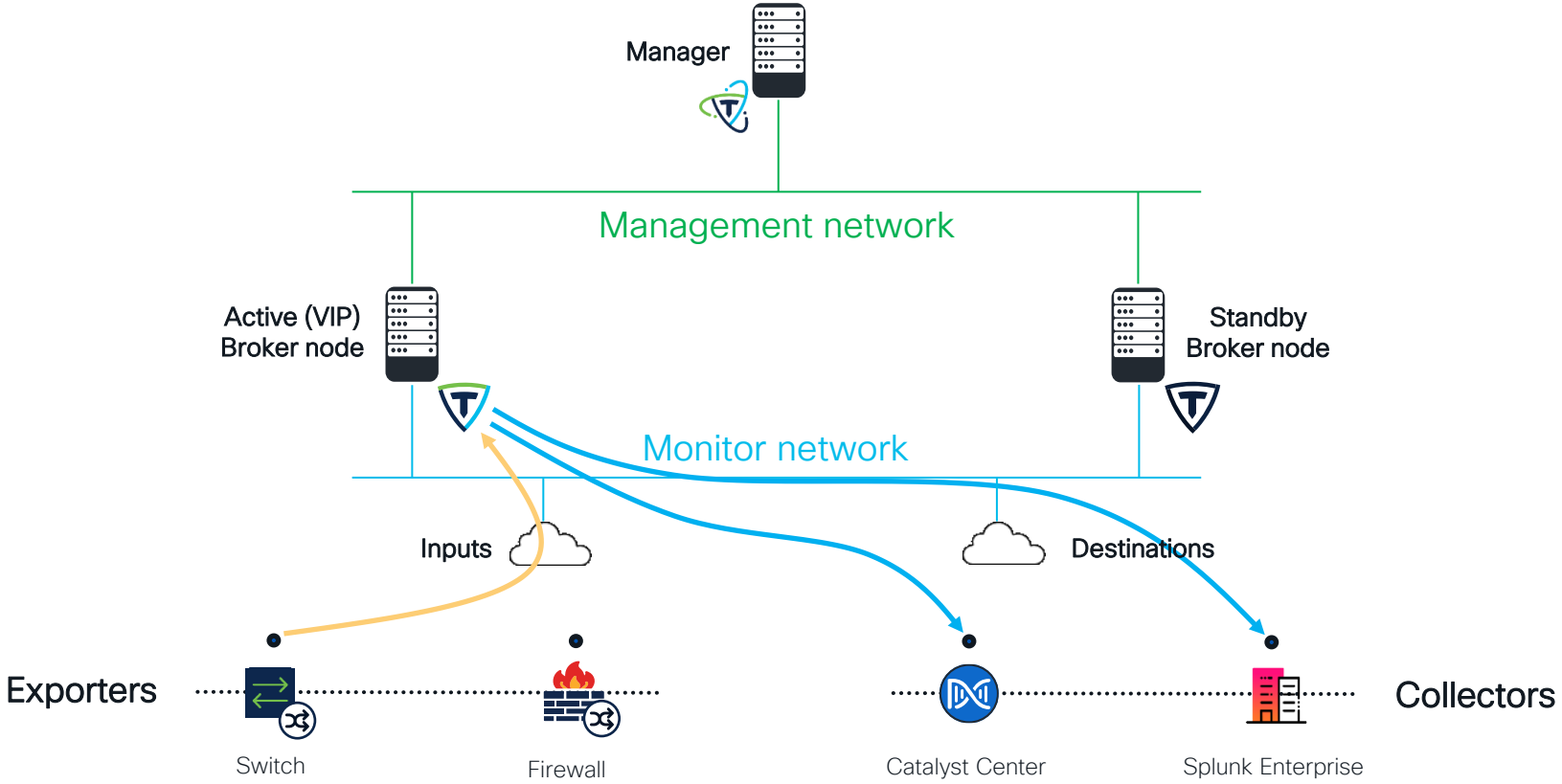


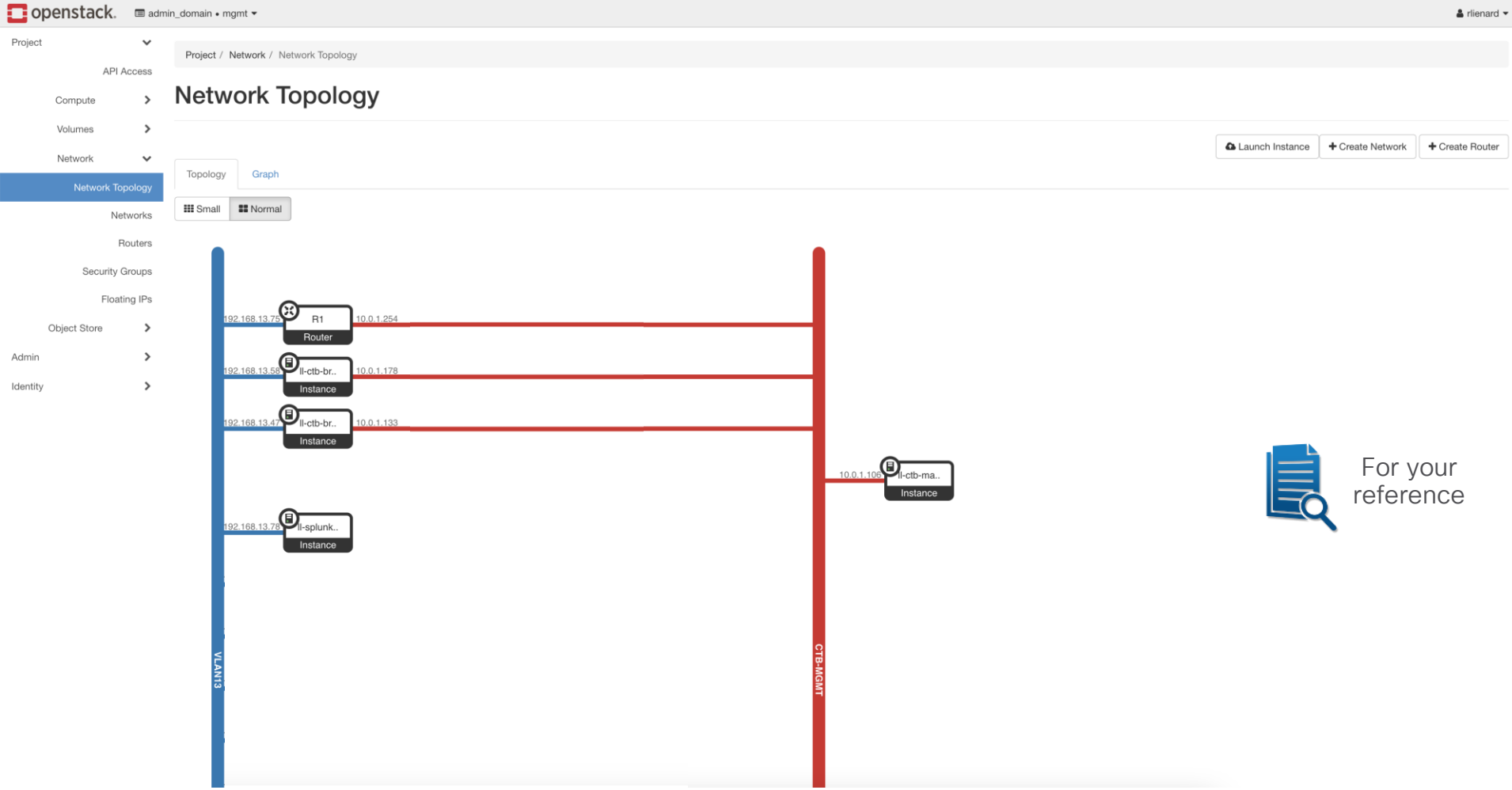


Cisco Telemetry Broker



Cisco Telemetry Broker





For your reference

Dashboard
Explorer
Settings

Dashboard

Average values are calculated for the last 30d

Inputs

Inputs	3
Received Last 24h	479 MB
Avg Received Daily	76.8 MB
No Destination	0

Destinations

Destinations	5
Sent Last 24h	942 MB
Avg Sent Daily	152 MB
Unreachable	0

Alerts

All | Unresolved (0)

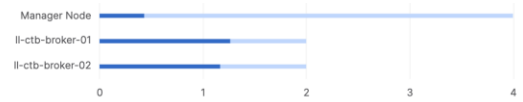
Most Recent on Top

There are no unresolved alerts.
To check the alerts configuration see Notification Settings.

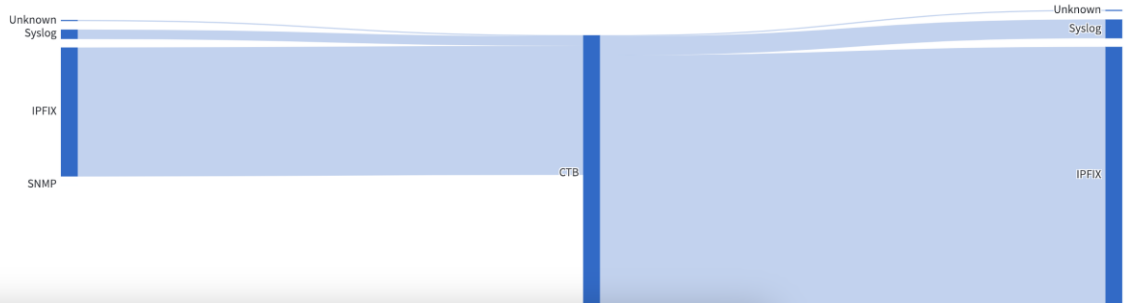
Broker Nodes

HA Cluster: selab

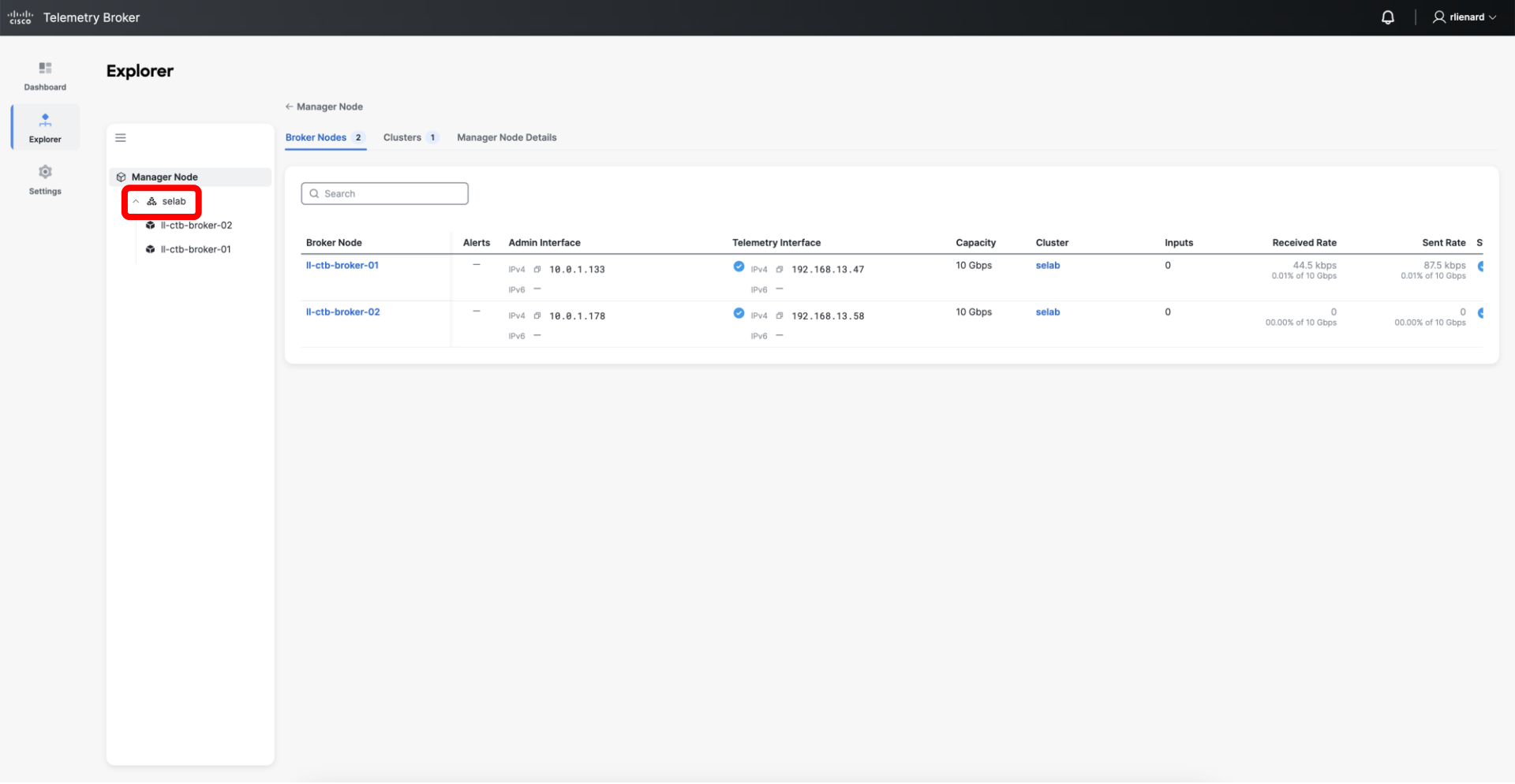
CPU

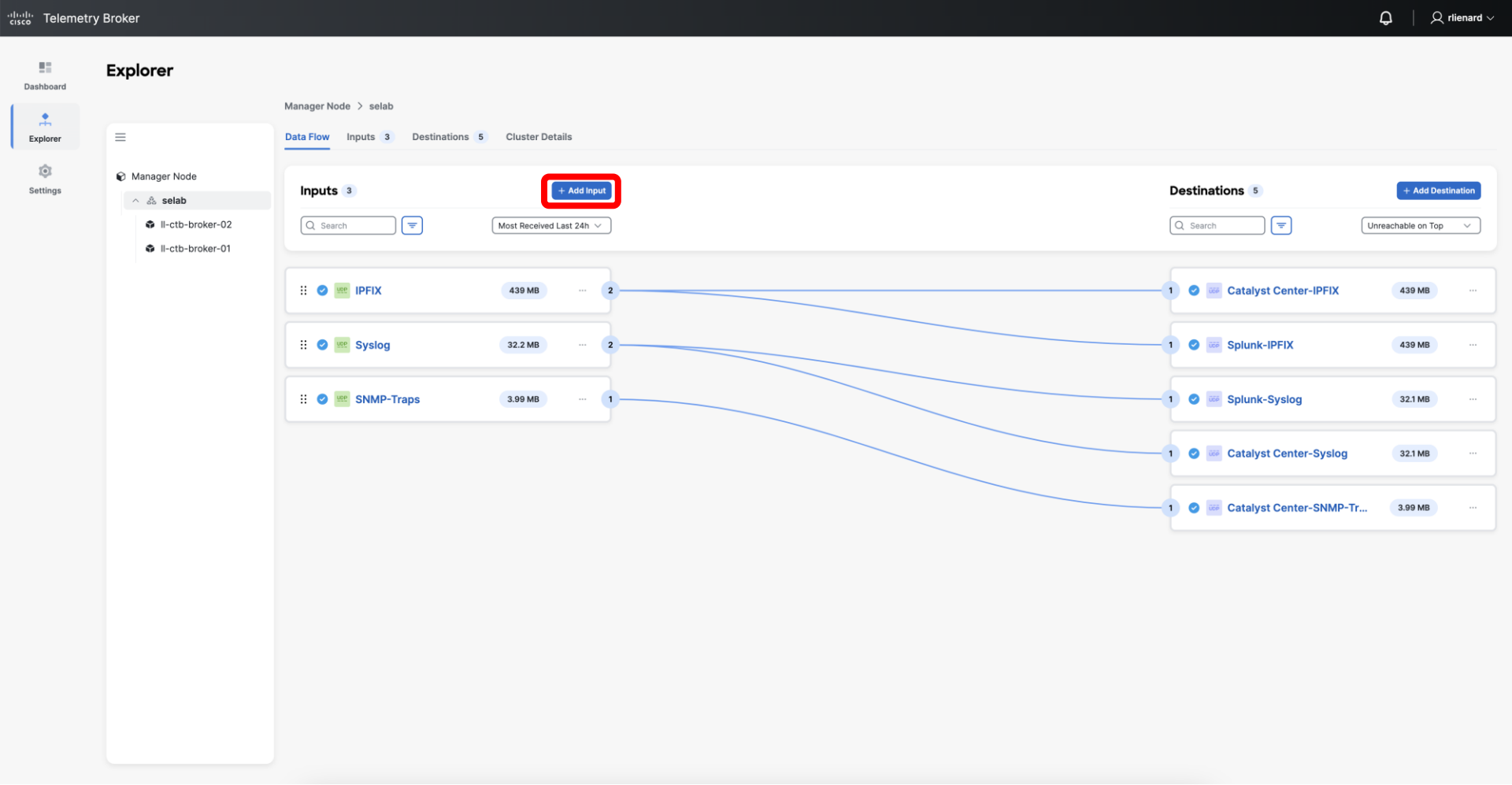


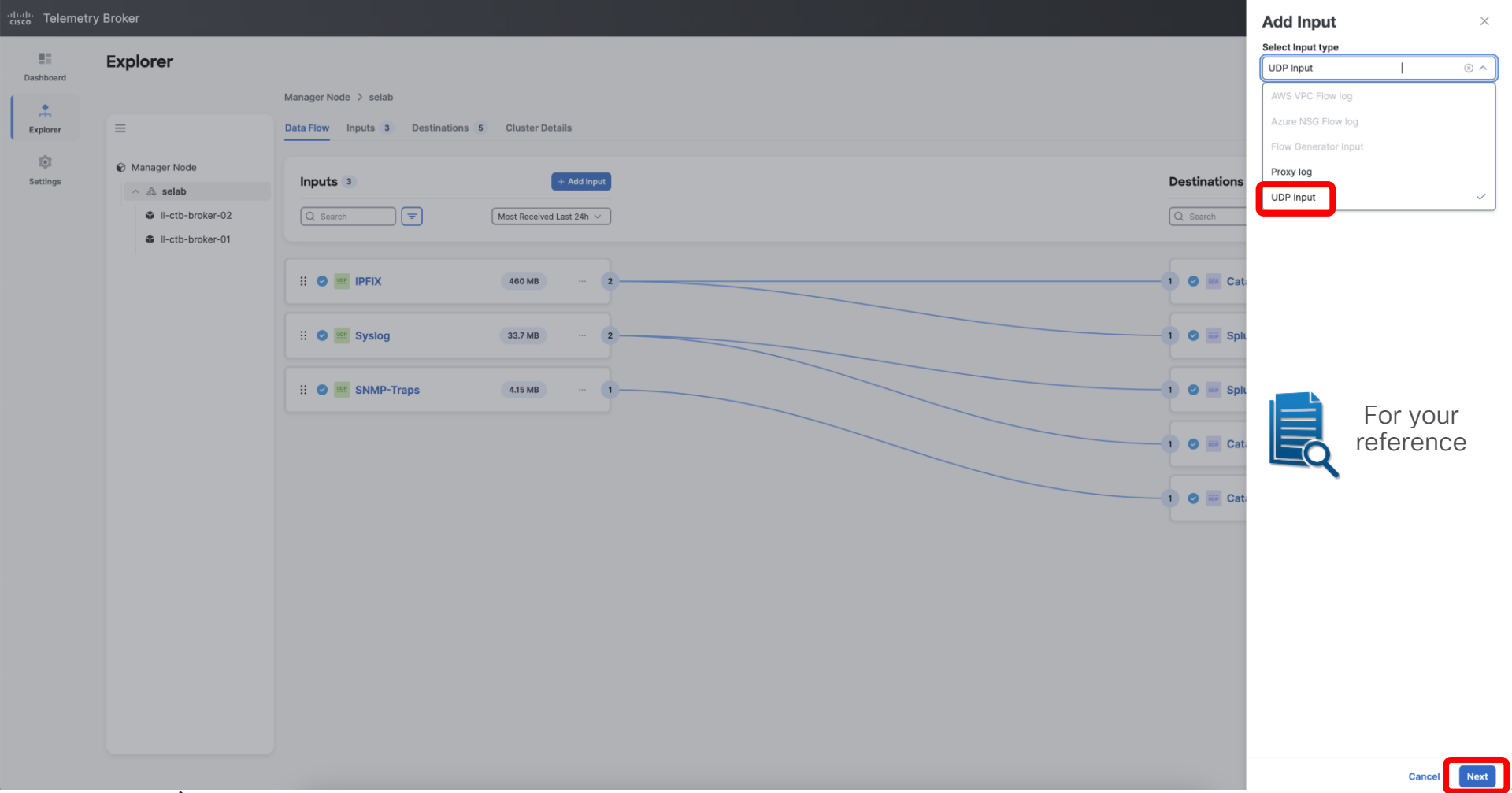
Telemetry Flows

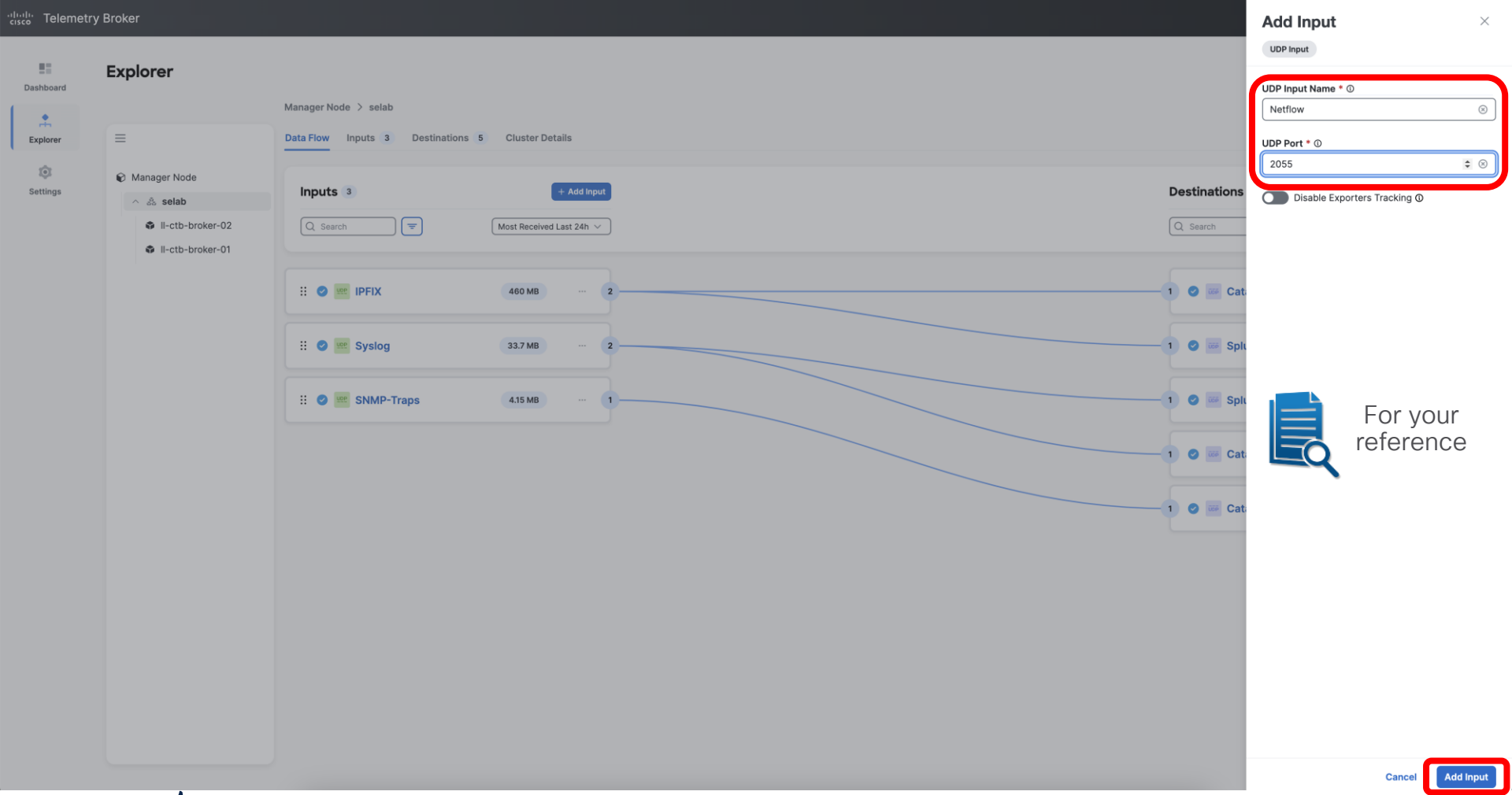


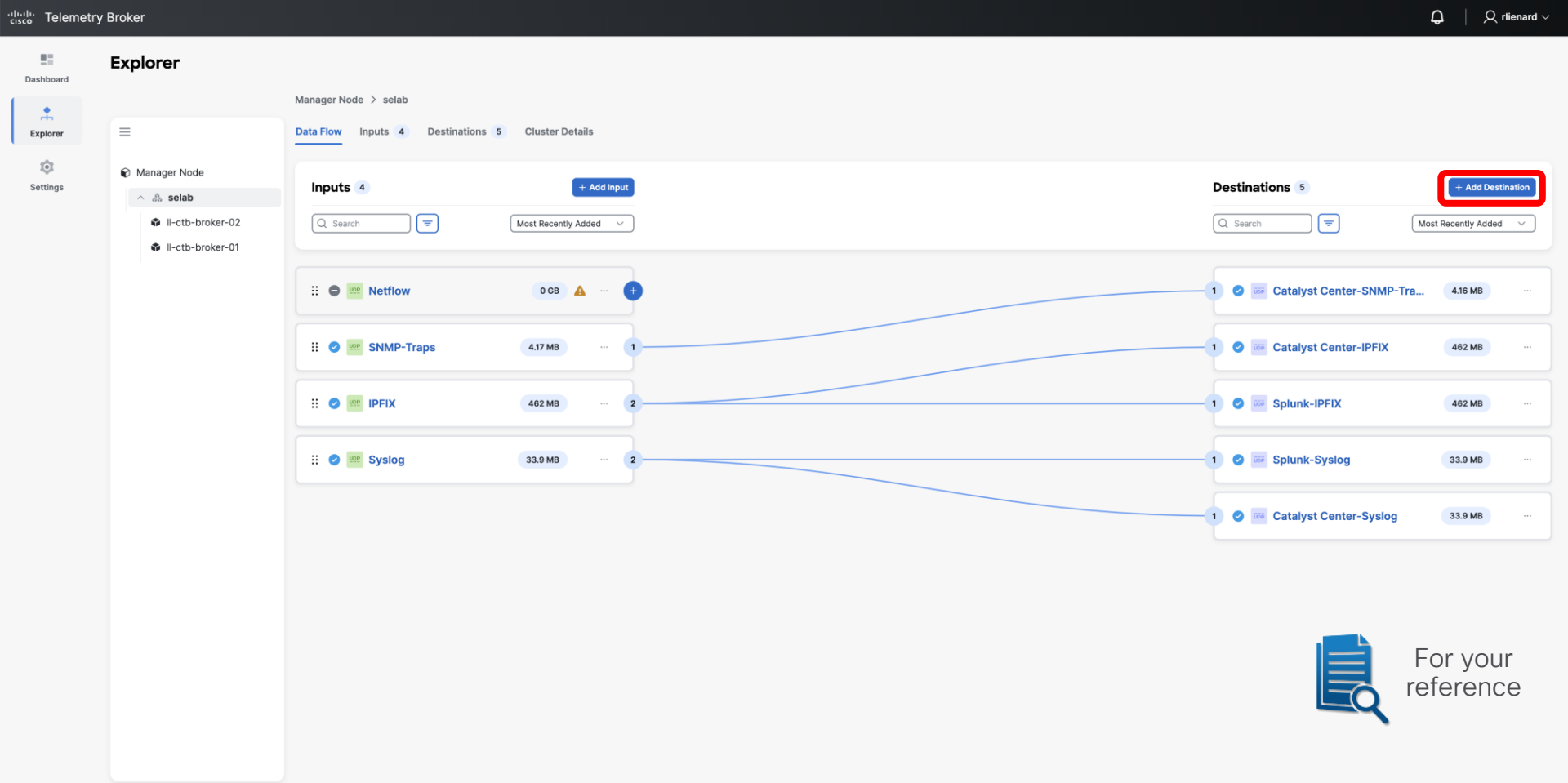
Licensing



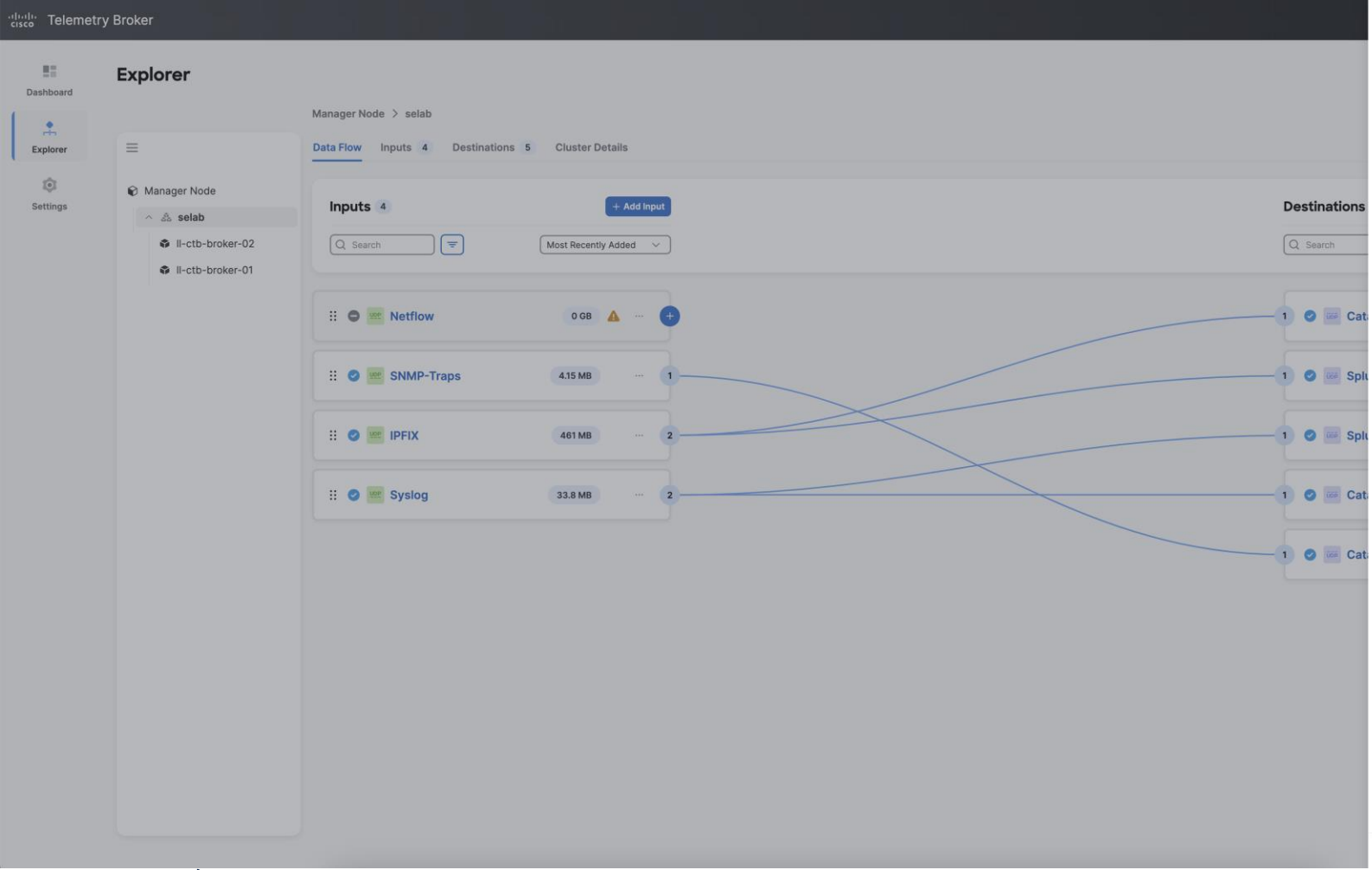


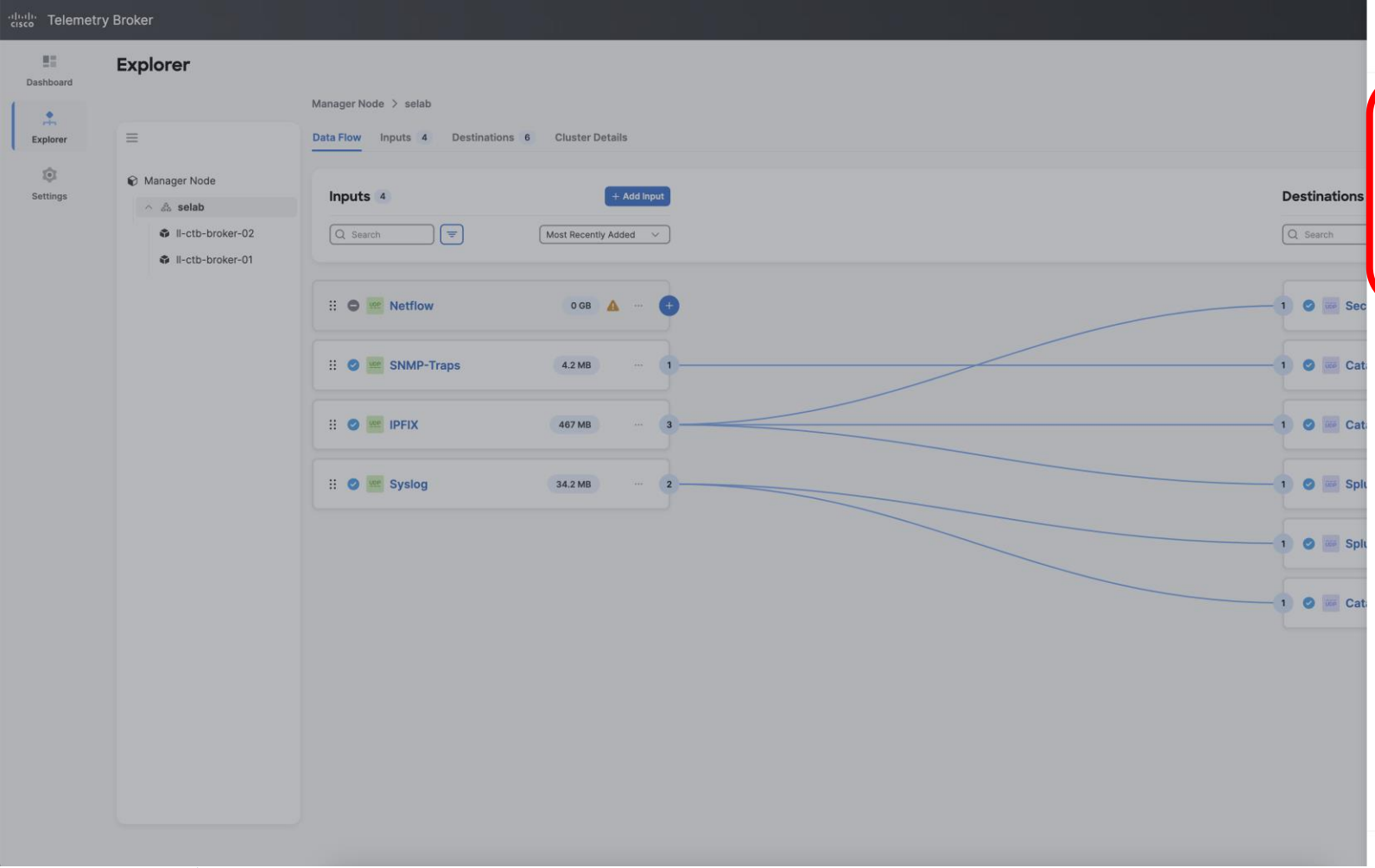




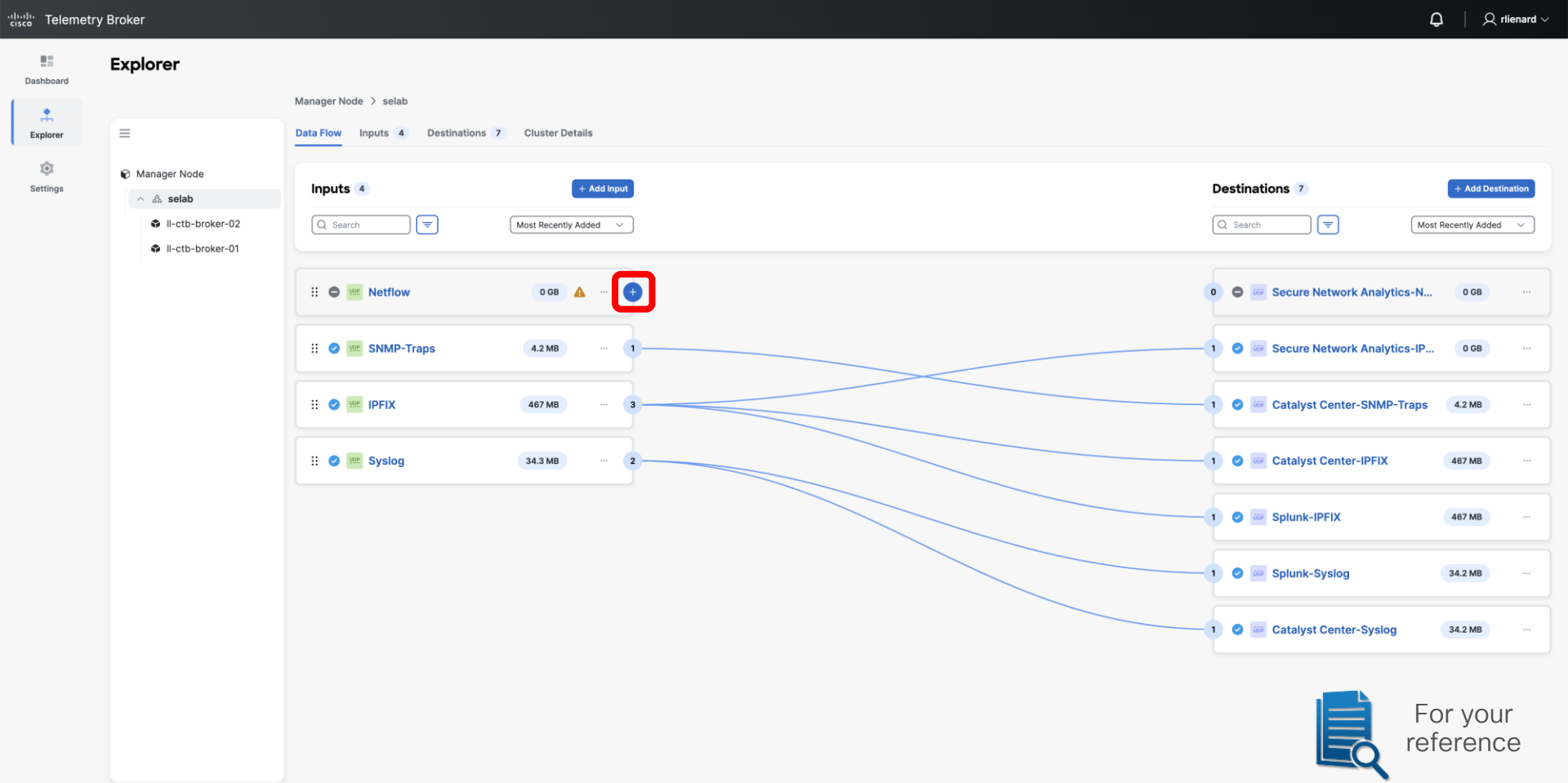


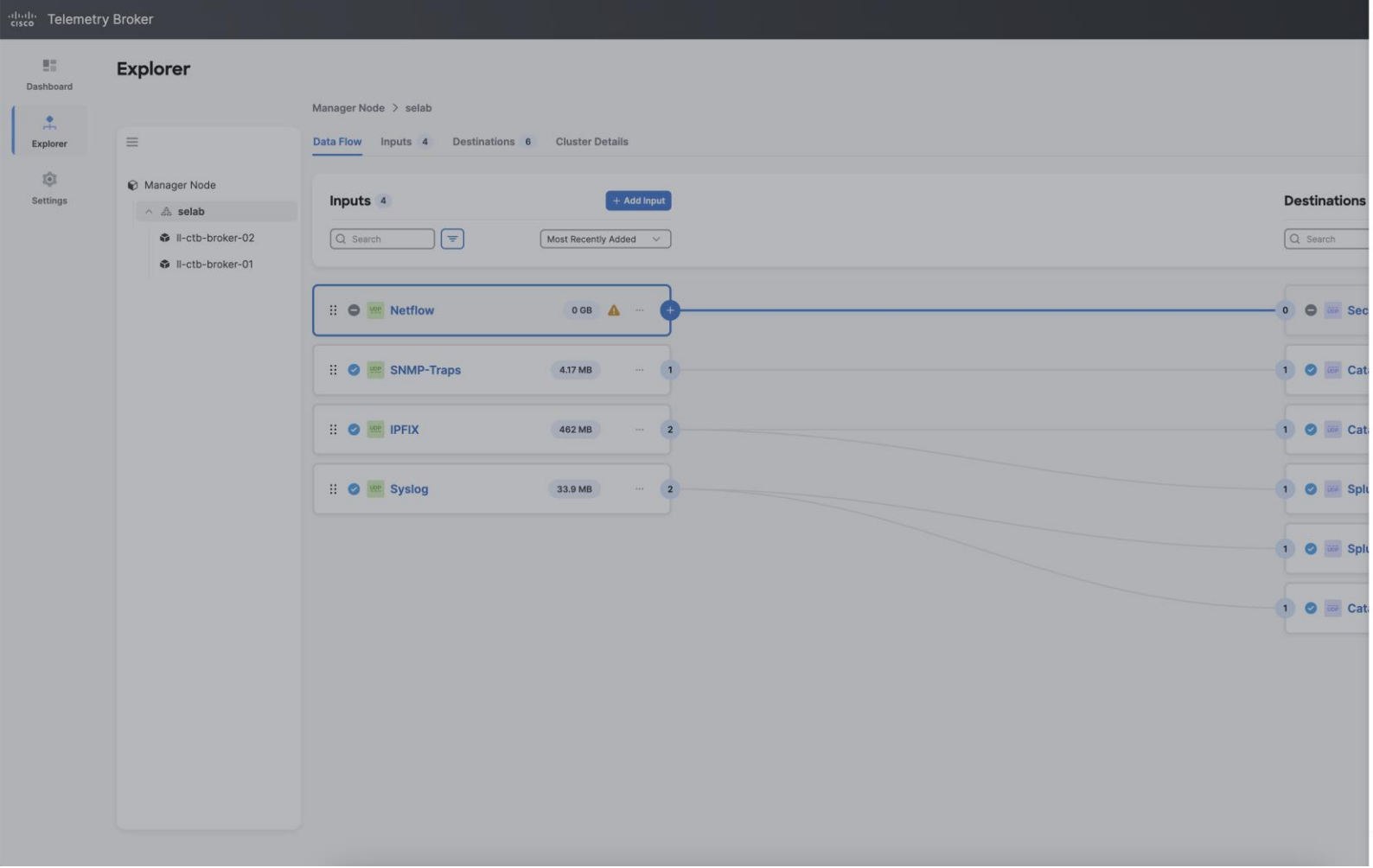
For your reference



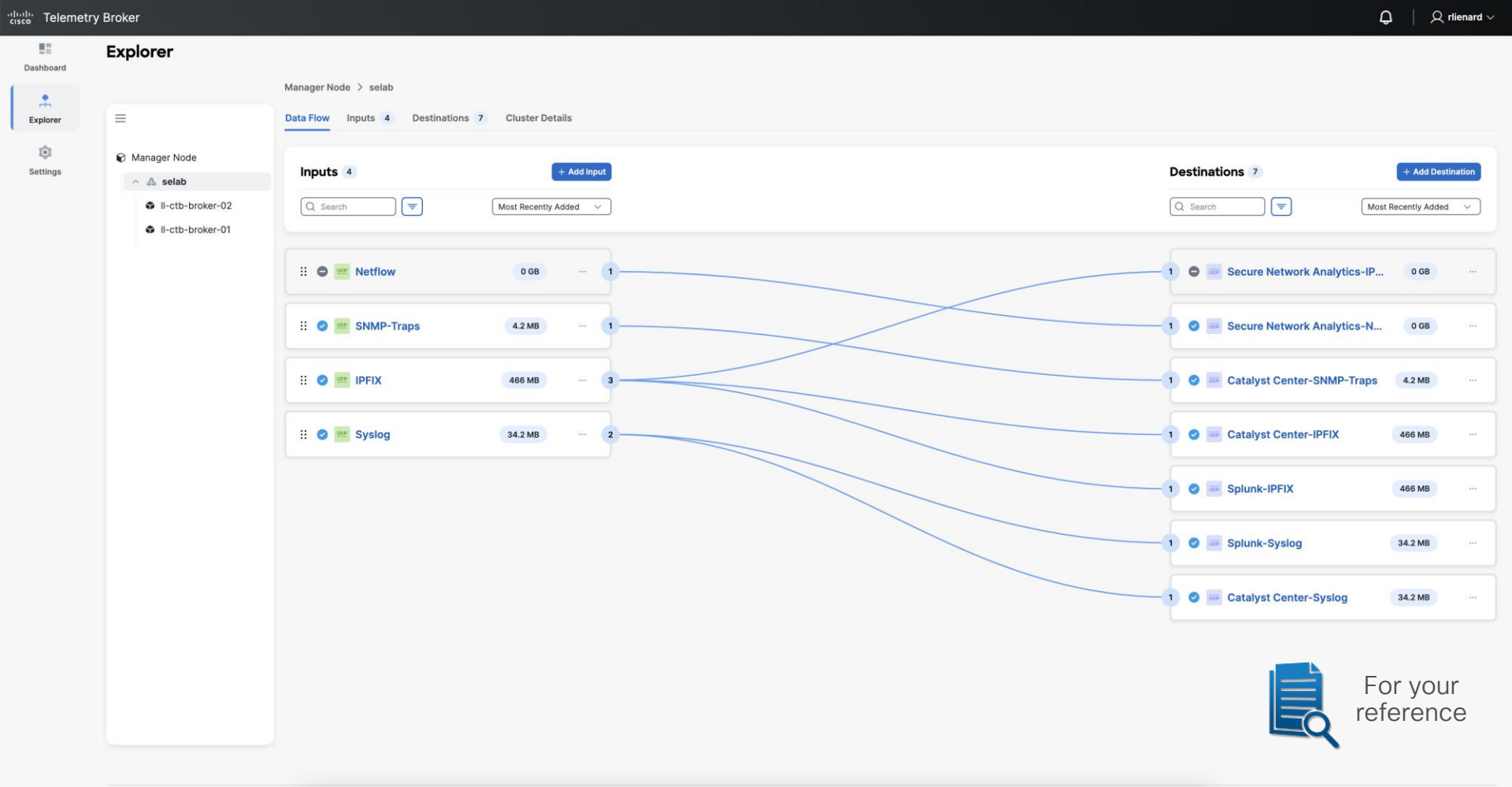


For your reference



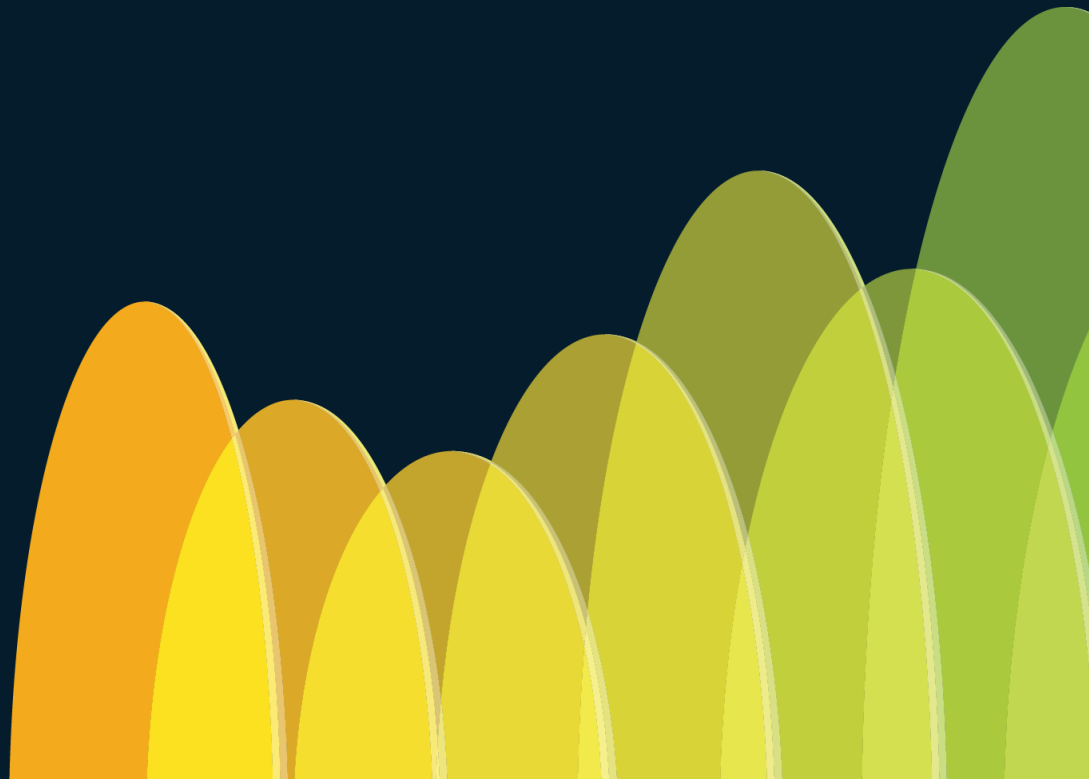


For your reference



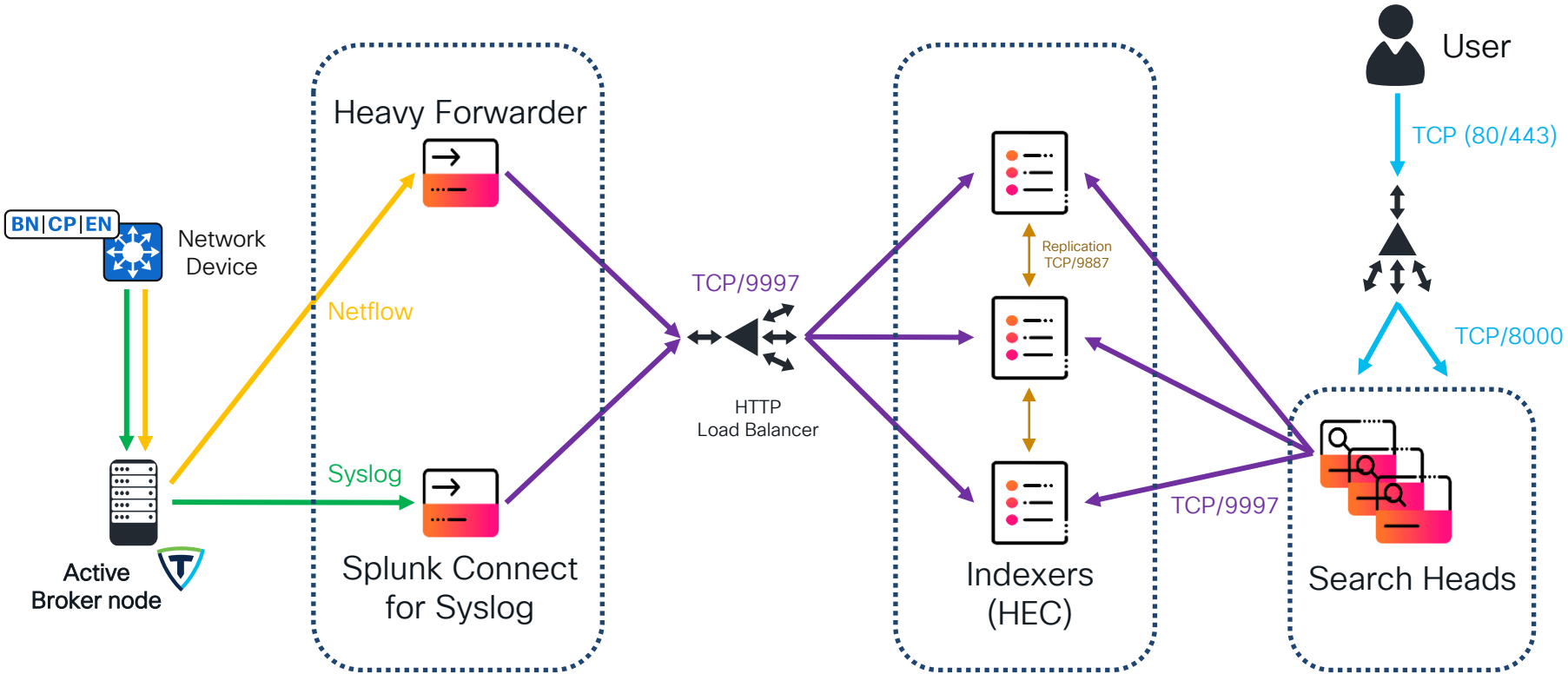
For your reference

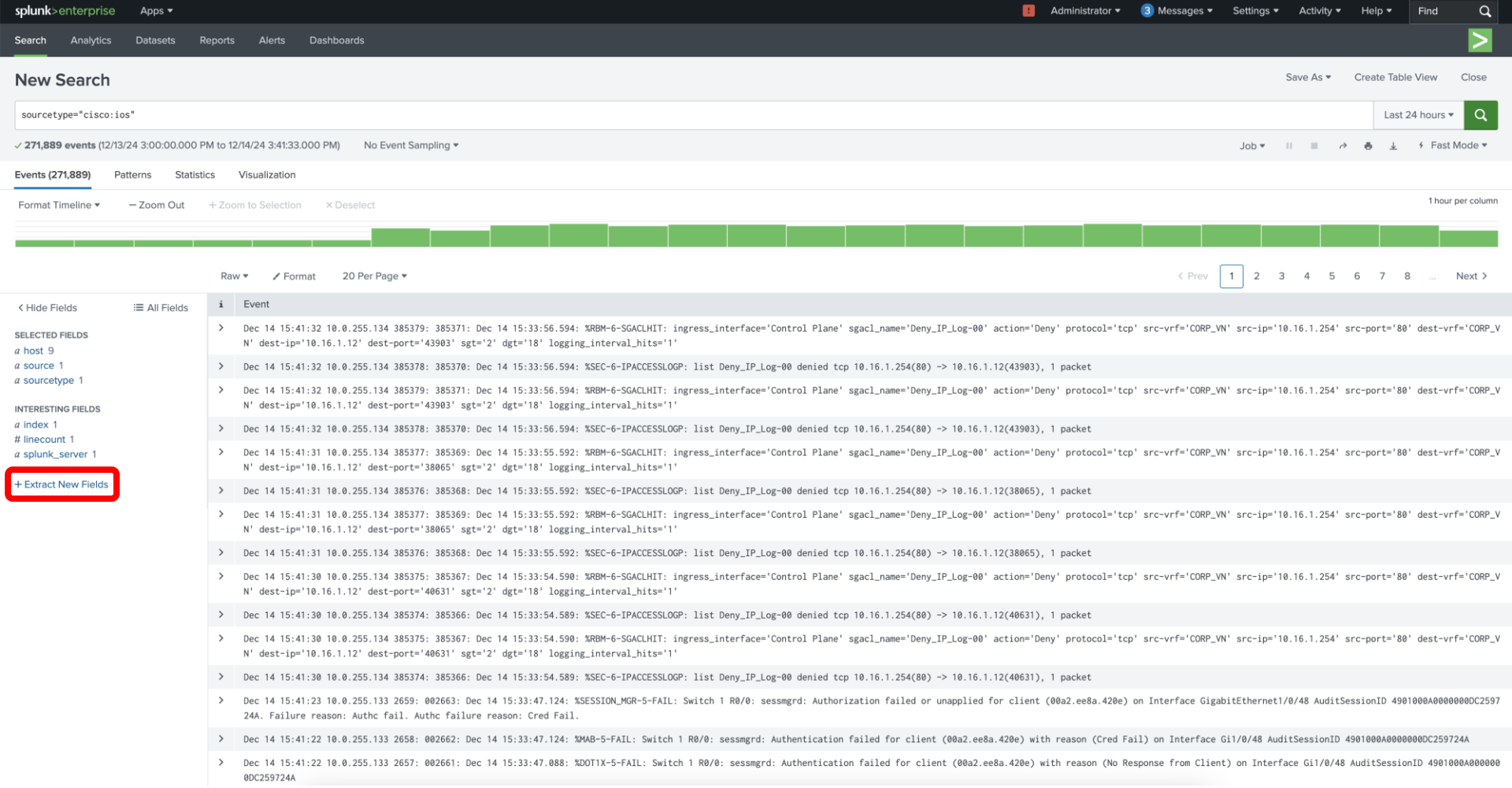
Splunk Enterprise



cisco Live!

Splunk Enterprise Architecture





Extract Fields — Select Sample — Select Method — Select Fields — Save — Next > — Existing fields >

Select Sample Event

Choose a source or source type, select a sample event, and click Next to go to the next step. The field extractor will use the event to extract fields. Learn more

I prefer to write the regular expression myself >

Source type
cisco:ios

Time Range
Last 90 days ▾

Events

✓ 1,000 events (9/15/24 12:00:00.000 AM to 12/14/24 3:56:18.000 PM)

20 per page ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

filter Apply Sample: 1,000 events ▾ All events ▾

_raw

Dec 14 15:54:20 10.0.255.128 267700: Dec 14 15:46:44.252: %RBM-6-SGACLHIT: ingress_interface='TenGigabitEthernet1/0/39' sgacl_name='Deny_IP_Log-00' action='Monitor' protocol='icmp' src-vrf='default' src-ip='10.0.254.18' src-port='5' dest-vrf='unknown' dest-ip='10.0.254.17' dest-port='1' sgt='0' dgt='2' logging_interval_hits='457'

Dec 14 15:54:18 10.0.255.134 386697: 386689: Dec 14 15:46:42.307: %RBM-6-SGACLHIT: ingress_interface='Control Plane' sgacl_name='Deny_IP_Log-00' action='Deny' protocol='tcp' src-vrf='CORP_VN' src-ip='10.16.1.254' src-port='80' dest-vrf='CORP_VN' dest-ip='10.16.1.15' dest-port='59397' sgt='2' dgt='4' logging_interval_hits='1'

Dec 14 15:54:18 10.0.255.134 386697: 386689: Dec 14 15:46:42.307: %RBM-6-SGACLHIT: ingress_interface='Control Plane' sgacl_name='Deny_IP_Log-00' action='Deny' protocol='tcp' src-vrf='CORP_VN' src-ip='10.16.1.254' src-port='80' dest-vrf='CORP_VN' dest-ip='10.16.1.15' dest-port='59397' sgt='2' dgt='4' logging_interval_hits='1'

Dec 14 15:54:17 10.0.255.134 386695: 386687: Dec 14 15:46:41.279: %RBM-6-SGACLHIT: ingress_interface='Control Plane' sgacl_name='Deny_IP_Log-00' action='Deny' protocol='tcp' src-vrf='CORP_VN' src-ip='10.16.1.254' src-port='80' dest-vrf='CORP_VN' dest-ip='10.16.1.15' dest-port='43703' sgt='2' dgt='4' logging_interval_hits='1'

Dec 14 15:54:17 10.0.255.134 386695: 386687: Dec 14 15:46:41.279: %RBM-6-SGACLHIT: ingress_interface='Control Plane' sgacl_name='Deny_IP_Log-00' action='Deny' protocol='tcp' src-vrf='CORP_VN' src-ip='10.16.1.254' src-port='80' dest-vrf='CORP_VN' dest-ip='10.16.1.15' dest-port='43703' sgt='2' dgt='4' logging_interval_hits='1'

Dec 14 15:54:16 10.0.255.134 386693: 386685: Dec 14 15:46:40.254: %RBM-6-SGACLHIT: ingress_interface='Control Plane' sgacl_name='Deny_IP_Log-00' action='Deny' protocol='tcp' src-vrf='CORP_VN' src-ip='10.16.1.254' src-port='80' dest-vrf='CORP_VN' dest-ip='10.16.1.15' dest-port='49945' sgt='2' dgt='4' logging_interval_hits='1'

Dec 14 15:54:16 10.0.255.134 386693: 386685: Dec 14 15:46:40.254: %RBM-6-SGACLHIT: ingress_interface='Control Plane' sgacl_name='Deny_IP_Log-00' action='Deny' protocol='tcp' src-vrf='CORP_VN' src-ip='10.16.1.254' src-port='80' dest-vrf='CORP_VN' dest-ip='10.16.1.15' dest-port='49945' sgt='2' dgt='4' logging_interval_hits='1'

Extract Fields — Select Sample — Select Method — Select Fields — Save — Next > — Existing fields >

Select Sample Event

Choose a source or source type, select a sample event, and click Next to go to the next step. The field extractor will use the event to extract fields. Learn more

I prefer to write the regular expression myself >

Source type
cisco:ios

Time Range
Last 90 days ▾

```
Dec 14 15:54:20 10.0.255.128 267700: Dec 14 15:46:44.252: %RBM-6-SGACLHIT: ingress_interface='TenGigabitEthernet1/0/39' sgacl_name='Deny_IP_Log-00' action='Monitor' protocol='icmp' src-vrf='default' src-ip='10.0.254.18' src-port='5' dest-vrf='unknown' dest-ip='10.0.254.17' dest-port='1' sgt='0' dgt='2' logging_interval_hits='457'
```

Events

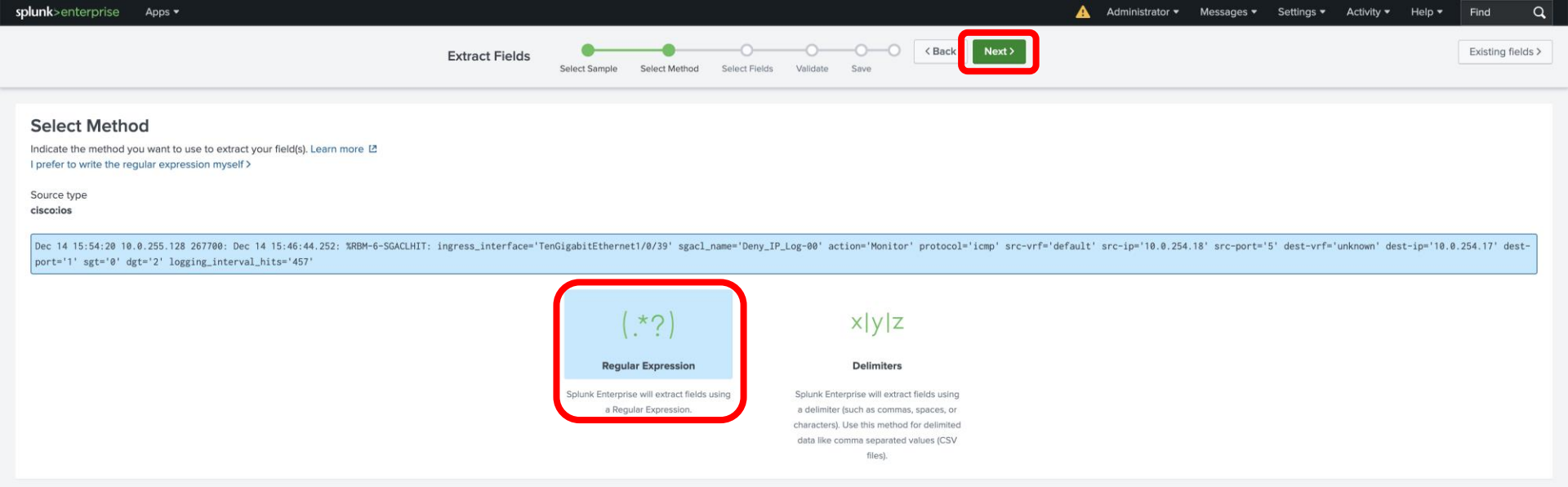
✓ 1,000 events (9/15/24 12:00:00.000 AM to 12/14/24 3:56:18.000 PM)

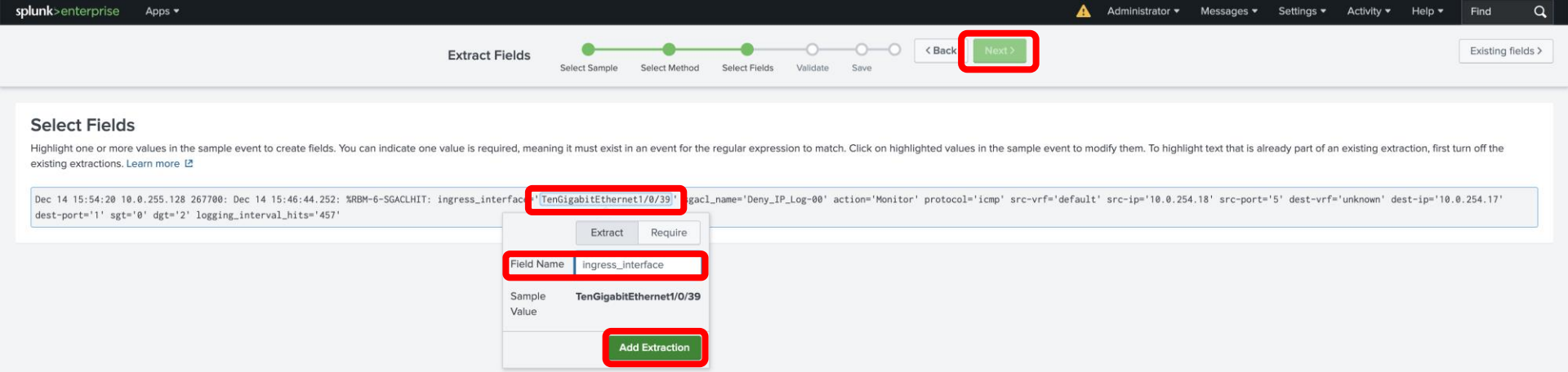
20 per page ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

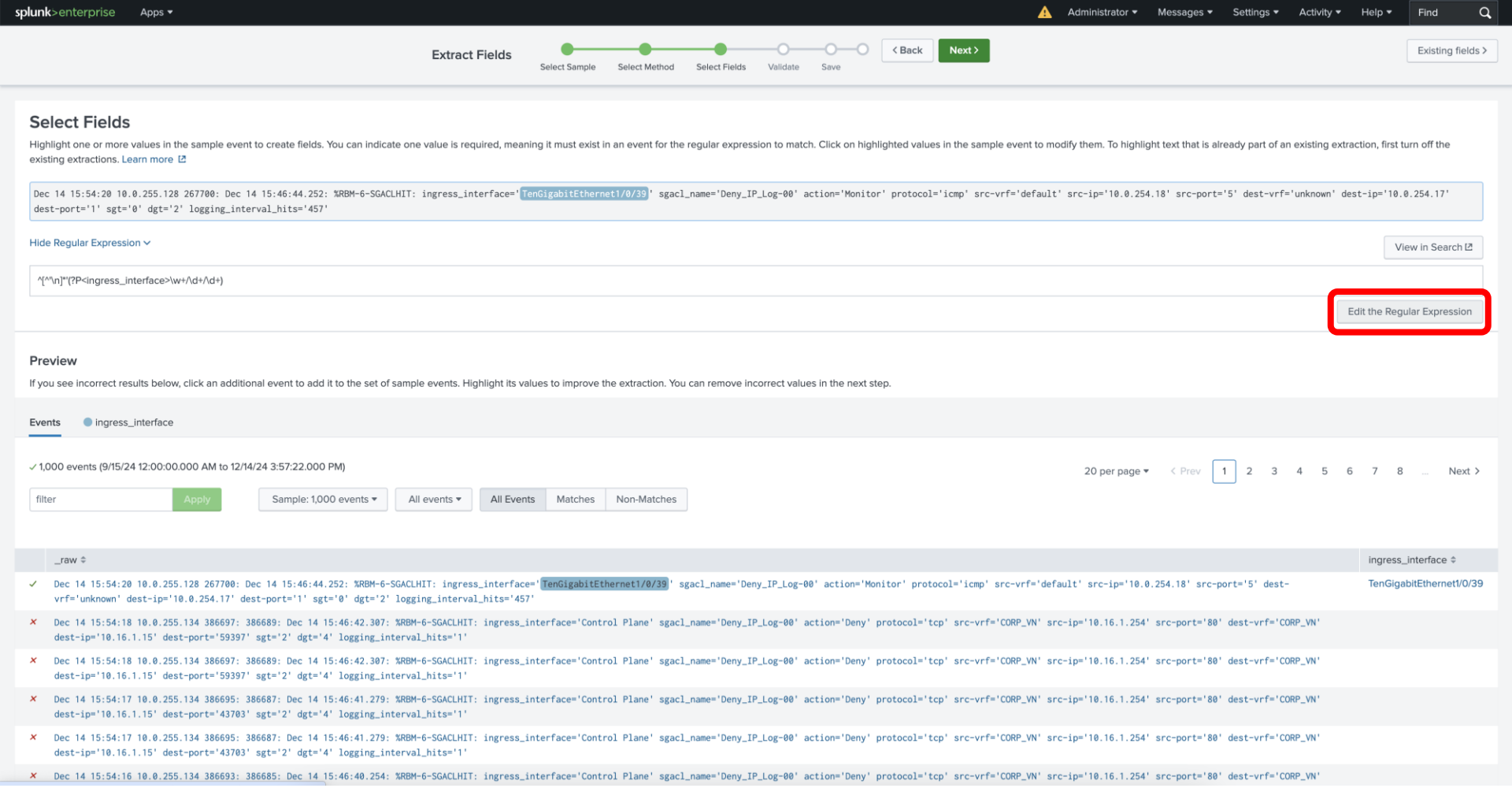
filter Apply Sample: 1,000 events ▾ All events ▾

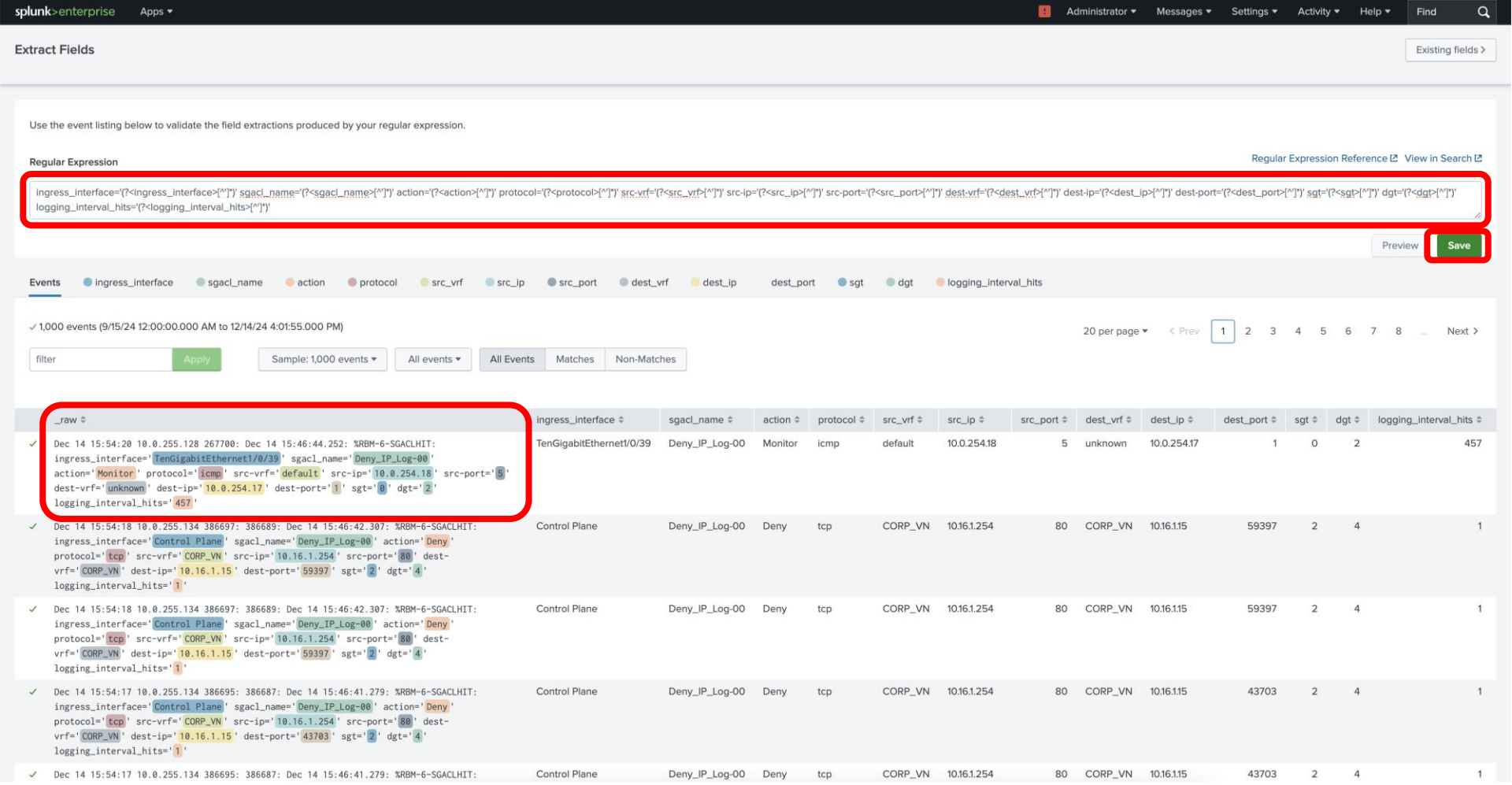
_raw

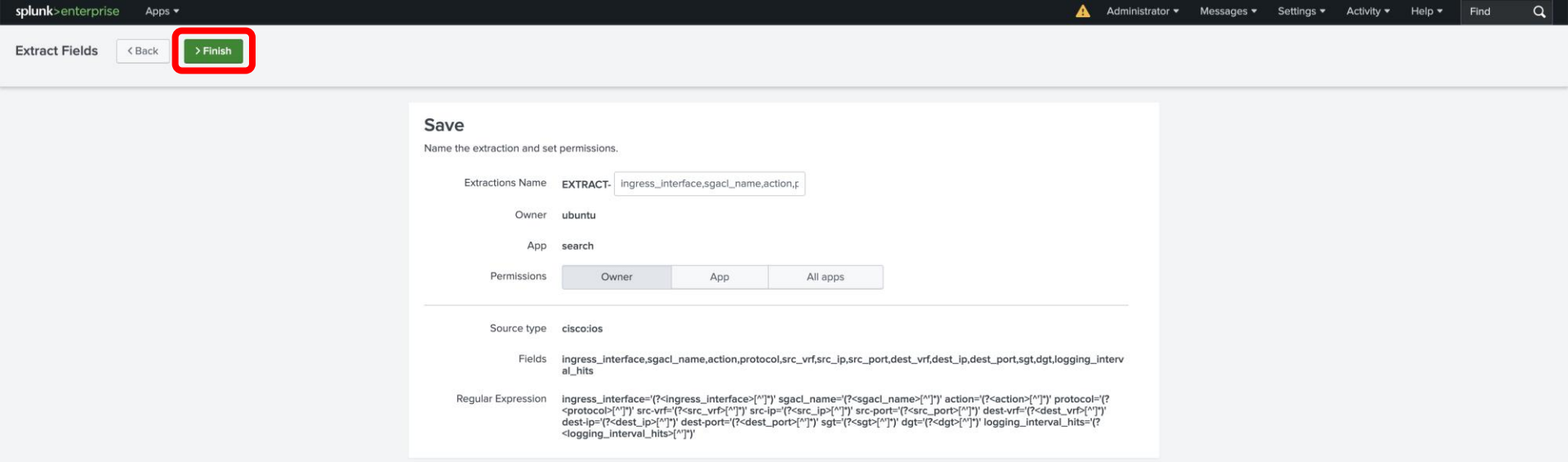
```
Dec 14 15:54:20 10.0.255.128 267700: Dec 14 15:46:44.252: %RBM-6-SGACLHIT: ingress_interface='TenGigabitEthernet1/0/39' sgacl_name='Deny_IP_Log-00' action='Monitor' protocol='icmp' src-vrf='default' src-ip='10.0.254.18' src-port='5' dest-vrf='unknown' dest-ip='10.0.254.17' dest-port='1' sgt='0' dgt='2' logging_interval_hits='457'
Dec 14 15:54:18 10.0.255.134 386697: 386689: Dec 14 15:46:42.307: %RBM-6-SGACLHIT: ingress_interface='Control Plane' sgacl_name='Deny_IP_Log-00' action='Deny' protocol='tcp' src-vrf='CORP_VN' src-ip='10.16.1.254' src-port='80' dest-vrf='CORP_VN' dest-ip='10.16.1.15' dest-port='59397' sgt='2' dgt='4' logging_interval_hits='1'
Dec 14 15:54:18 10.0.255.134 386697: 386689: Dec 14 15:46:42.307: %RBM-6-SGACLHIT: ingress_interface='Control Plane' sgacl_name='Deny_IP_Log-00' action='Deny' protocol='tcp' src-vrf='CORP_VN' src-ip='10.16.1.254' src-port='80' dest-vrf='CORP_VN' dest-ip='10.16.1.15' dest-port='59397' sgt='2' dgt='4' logging_interval_hits='1'
Dec 14 15:54:17 10.0.255.134 386695: 386687: Dec 14 15:46:41.279: %RBM-6-SGACLHIT: ingress_interface='Control Plane' sgacl_name='Deny_IP_Log-00' action='Deny' protocol='tcp' src-vrf='CORP_VN' src-ip='10.16.1.254' src-port='80' dest-vrf='CORP_VN' dest-ip='10.16.1.15' dest-port='43703' sgt='2' dgt='4' logging_interval_hits='1'
Dec 14 15:54:17 10.0.255.134 386695: 386687: Dec 14 15:46:41.279: %RBM-6-SGACLHIT: ingress_interface='Control Plane' sgacl_name='Deny_IP_Log-00' action='Deny' protocol='tcp' src-vrf='CORP_VN' src-ip='10.16.1.254' src-port='80' dest-vrf='CORP_VN' dest-ip='10.16.1.15' dest-port='43703' sgt='2' dgt='4' logging_interval_hits='1'
Dec 14 15:54:16 10.0.255.134 386693: 386685: Dec 14 15:46:40.254: %RBM-6-SGACLHIT: ingress_interface='Control Plane' sgacl_name='Deny_IP_Log-00' action='Deny' protocol='tcp' src-vrf='CORP_VN' src-ip='10.16.1.254' src-port='80' dest-vrf='CORP_VN' dest-ip='10.16.1.15' dest-port='49945' sgt='2' dgt='4' logging_interval_hits='1'
Dec 14 15:54:16 10.0.255.134 386693: 386685: Dec 14 15:46:40.254: %RBM-6-SGACLHIT: ingress_interface='Control Plane' sgacl_name='Deny_IP_Log-00' action='Deny' protocol='tcp' src-vrf='CORP_VN' src-ip='10.16.1.254' src-port='80' dest-vrf='CORP_VN' dest-ip='10.16.1.15' dest-port='49945' sgt='2' dgt='4' logging_interval_hits='1'
```

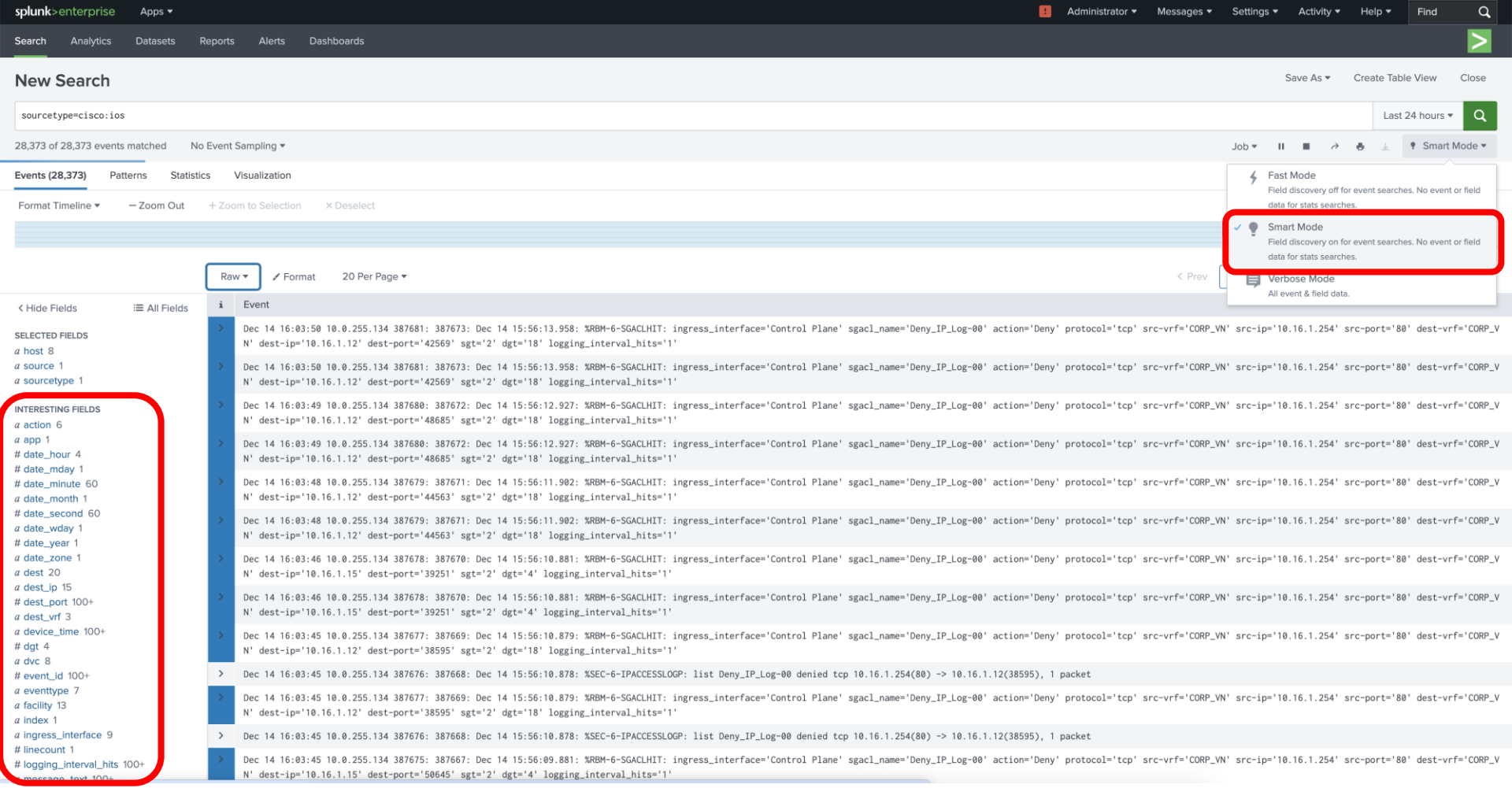


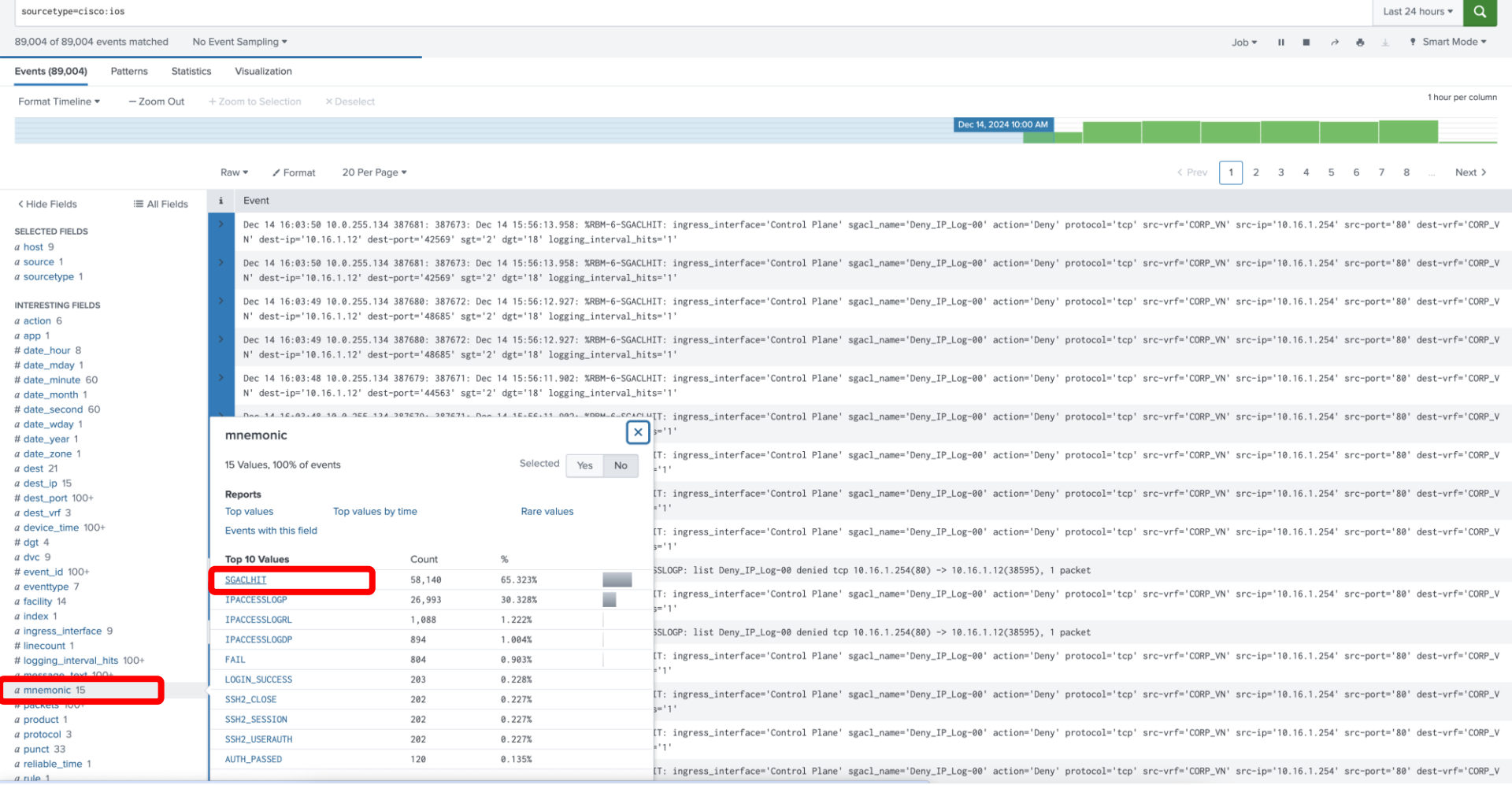


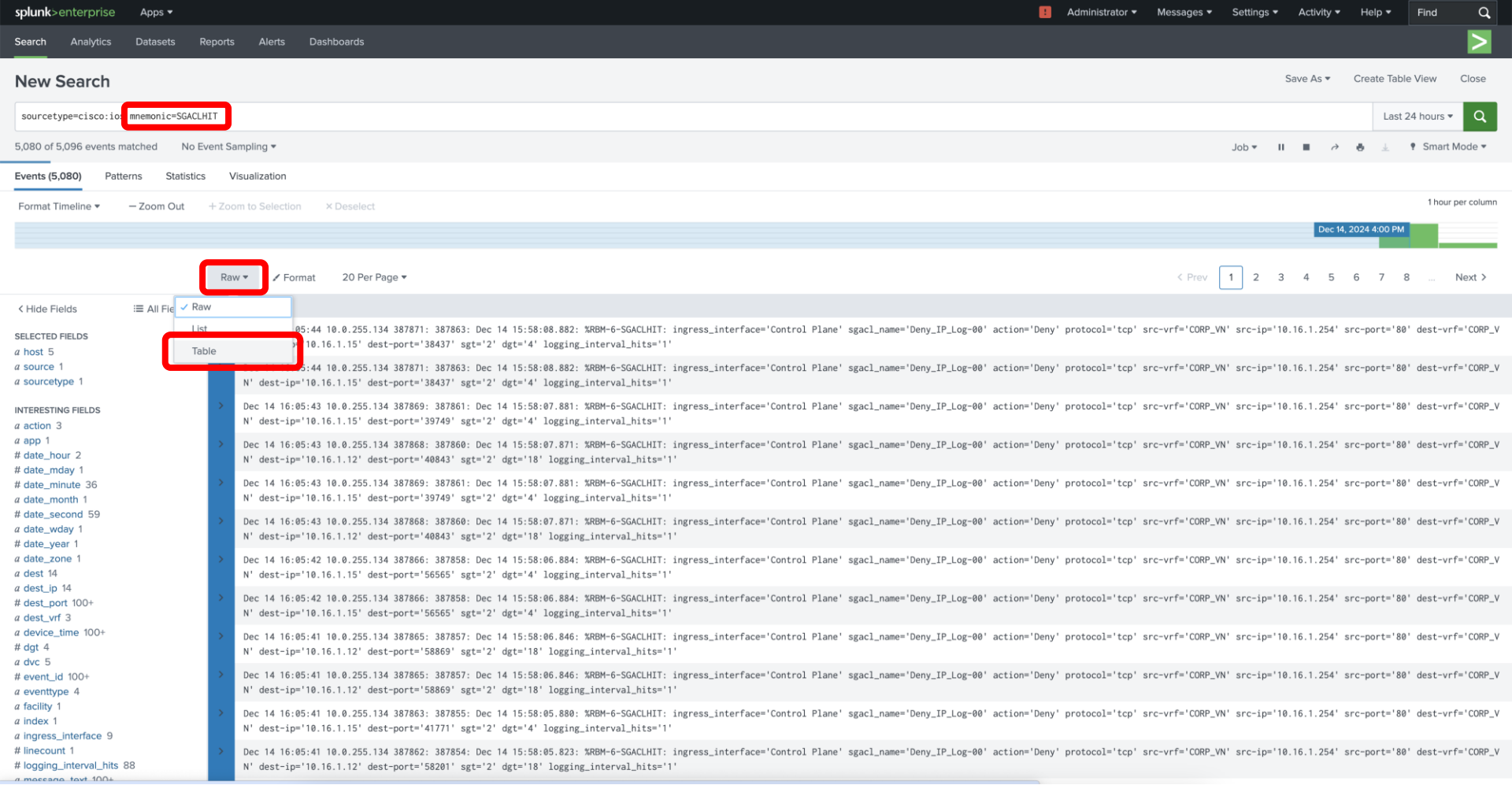


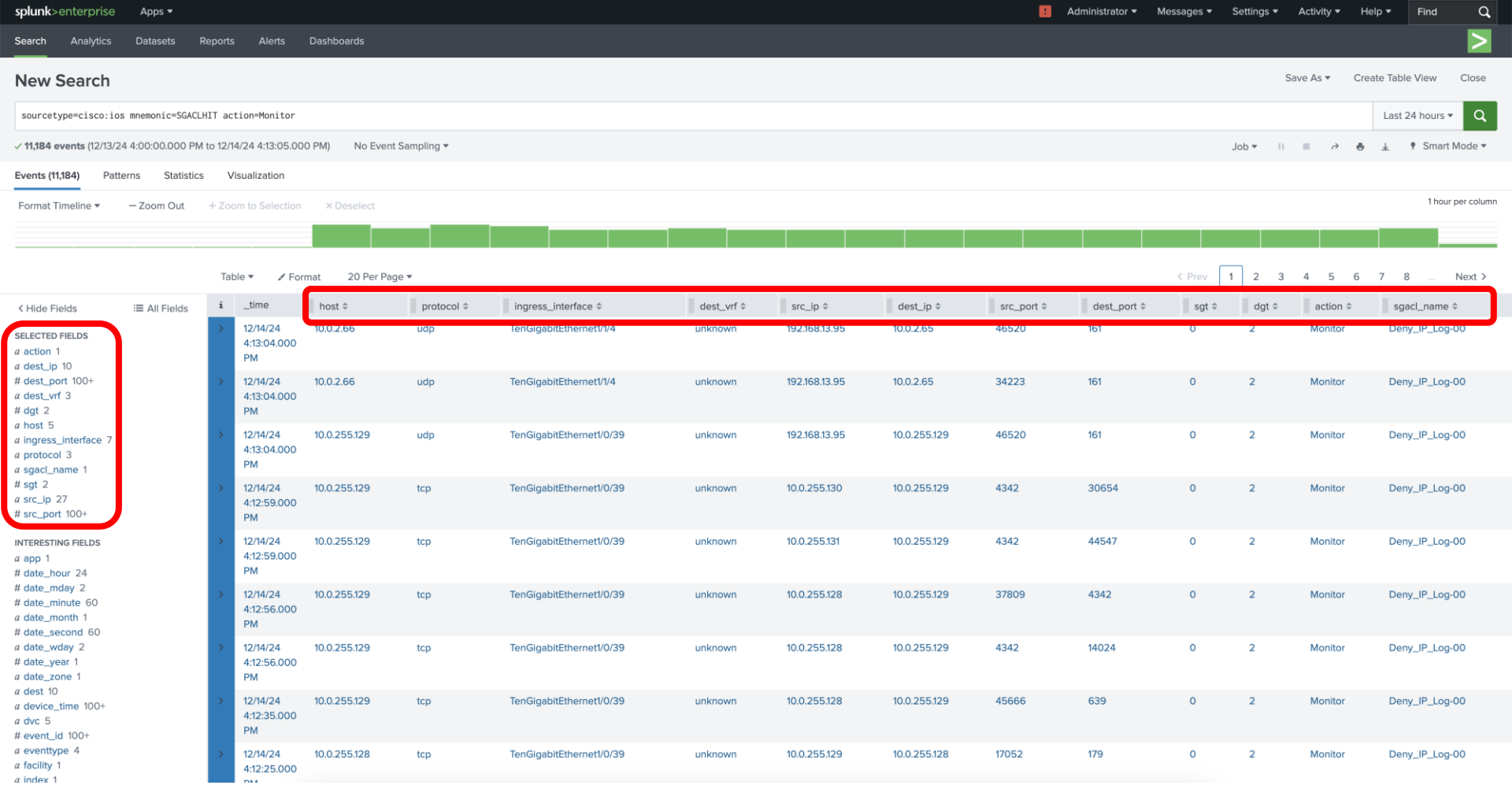












Agenda

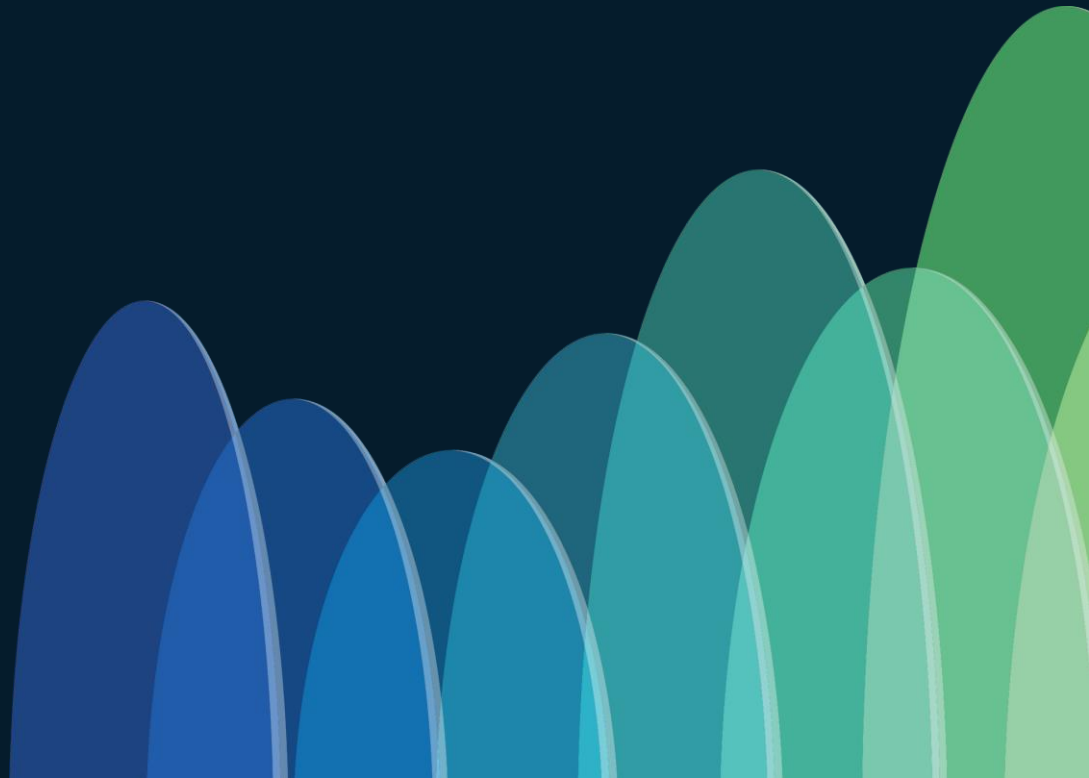
- Introduction
- Segmentation Strategy
- Observability Pipelines
- Deploy Allow-List Model
- Conclusions

Warning

Before applying the Allow-List model

- Disable enforcement on ALL fabric facing interfaces.

Prepare the Matrix



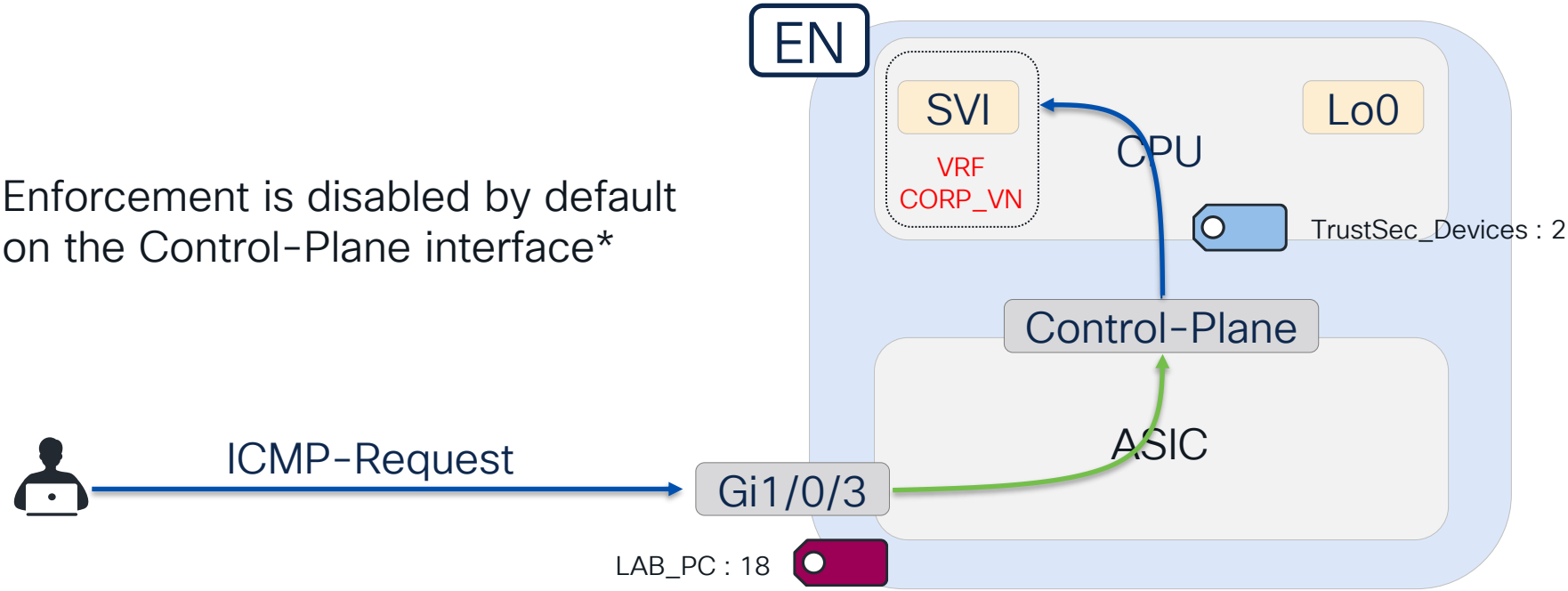
cisco Live!

Traffic to Anycast Gateway

cisco Live!

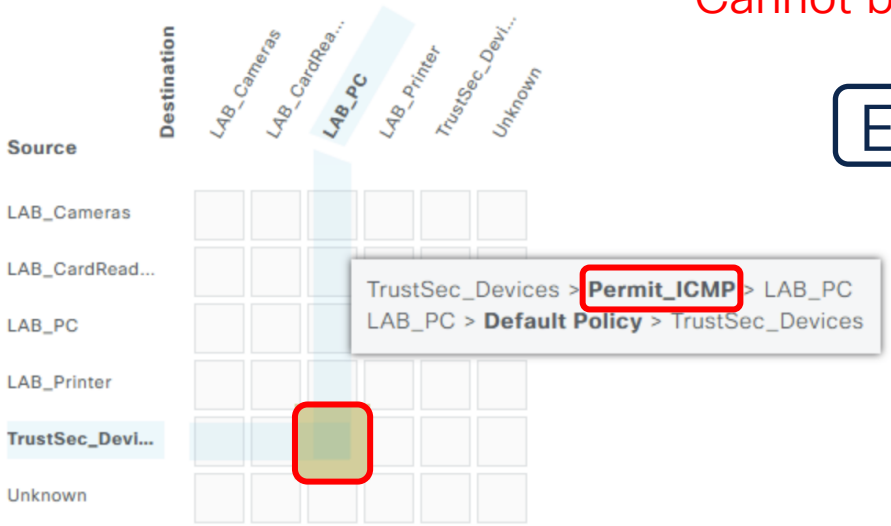
Traffic to Anycast Gateway

Enforcement is disabled by default on the Control-Plane interface*



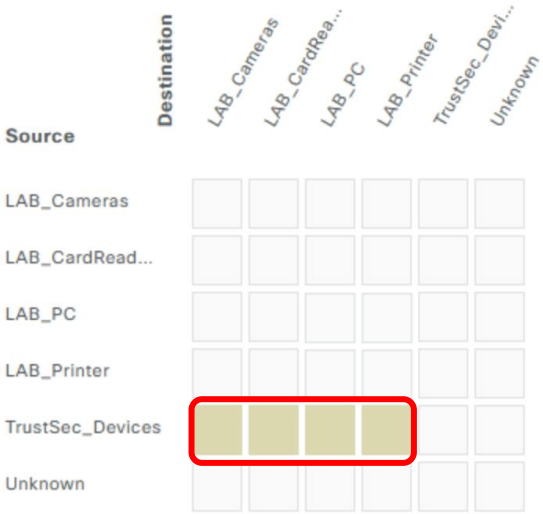
Traffic to Anycast Gateway

Cannot be used to protect the CPU from DoS !



Returning traffic is enforced

Traffic to Anycast Gateway



Repeat for other overlay SGTs

EN

SVI

VRF
CORP_VN

Lo0

CPU

TrustSec_Devices : 2

Control-Plane

ASIC

VLAN Enforcement

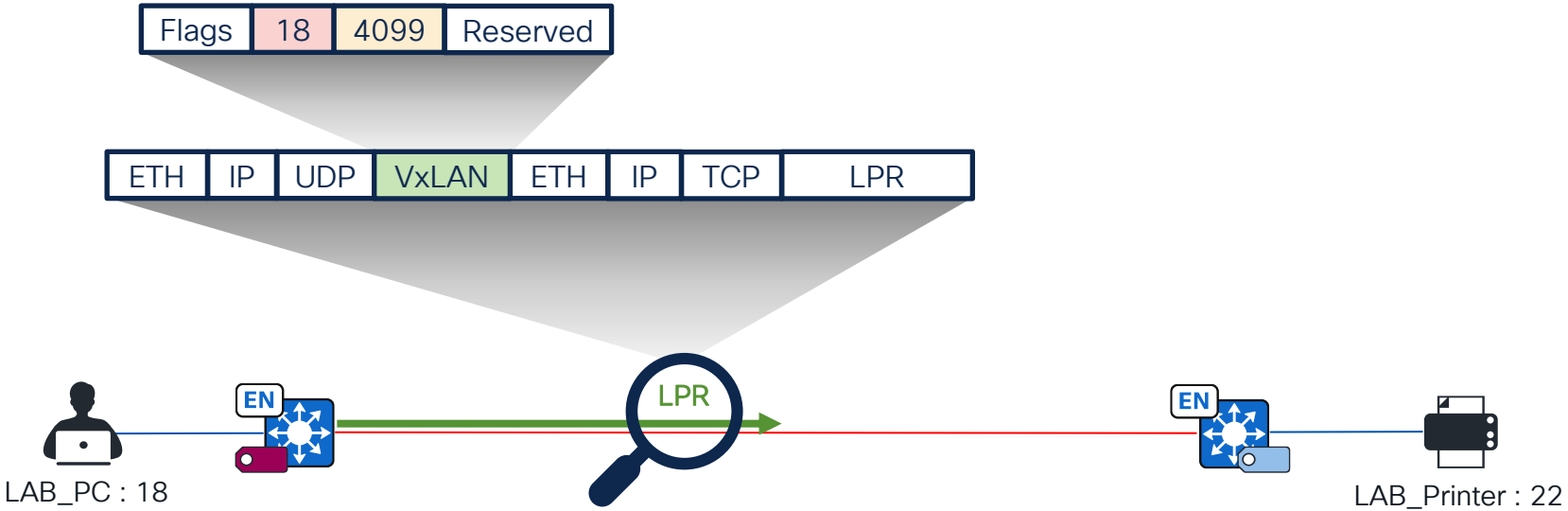
Gi1/0/x

SGT : xx

ICMP-Reply

East-West Traffic

East-West Traffic



East-West Traffic

Access Contract

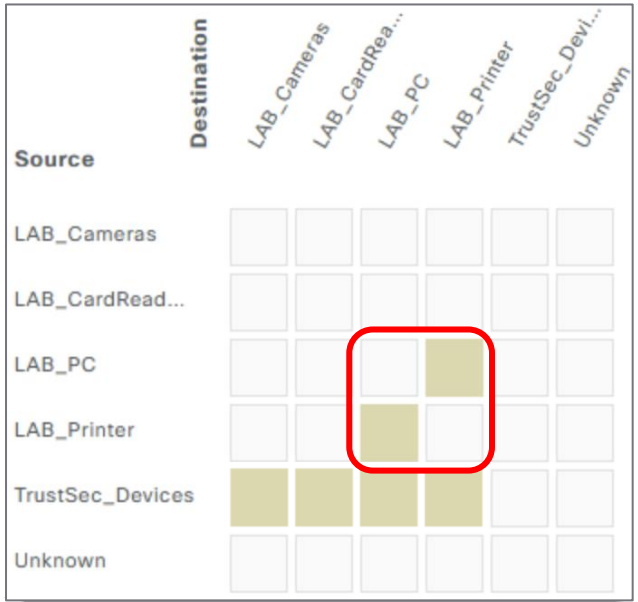
Name*: Permit_LPR_ICMP

Description:

CONTRACT CONTENT (3)

#	Action*	Application*	Transport Protocol	Source / Destination	Port	Logging	Action
1	Permit	Advanced	TCP	Destination	515		
				Source	ANY		
2	Permit	Advanced	TCP	Destination	ANY		
				Source	515		
3	Permit	Advanced	ICMP	–	–		

Default Action: Deny — Logging



East-West Traffic

East-West Traffic

```
S1-Edge-2#sh cts role-based counters from 18 to 22
Role-based IPv4 counters
From    To      SW-Denied  HW-Denied  SW-Permitt  HW-Permitt  SW-Monitor  HW-Monitor
18      22      0          0          0           2           0           0
```

East-West Traffic

Tips & Tricks

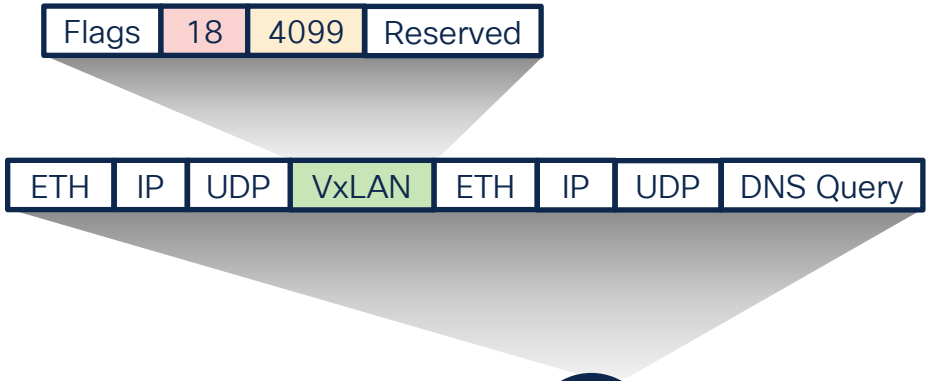
- Start by creating all obvious contracts
- Apply Permit_IP_Log where traffic needs monitoring
- Leave the rest to default

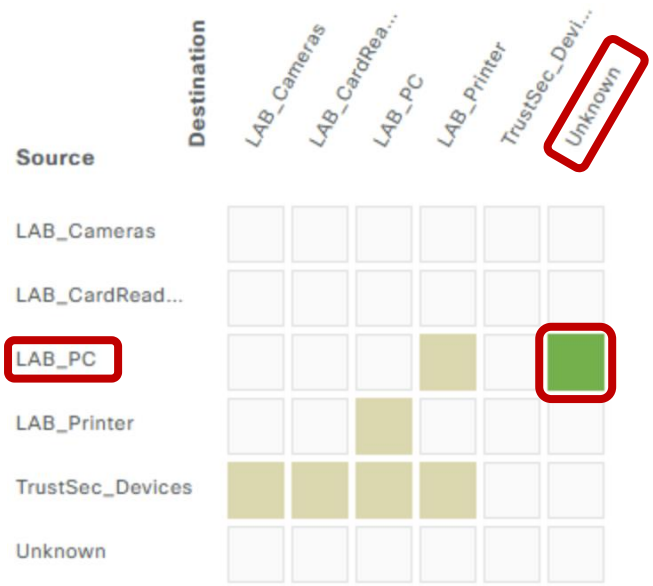
South->North Traffic with BN Enforcement

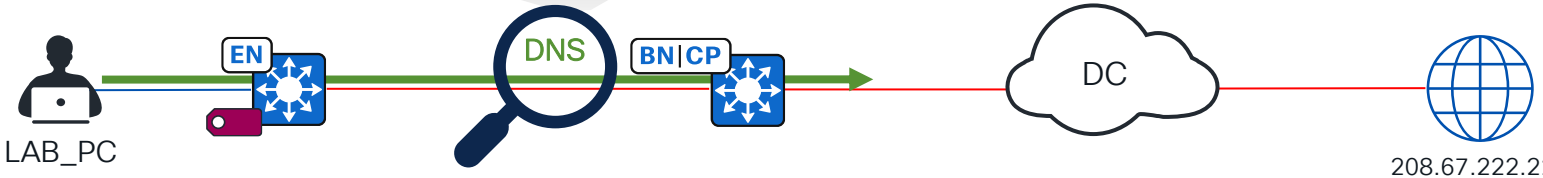
cisco Live!

South->North Traffic w/ BN Enforcement

Traffic to Unknown should be allowed to cross the Border.



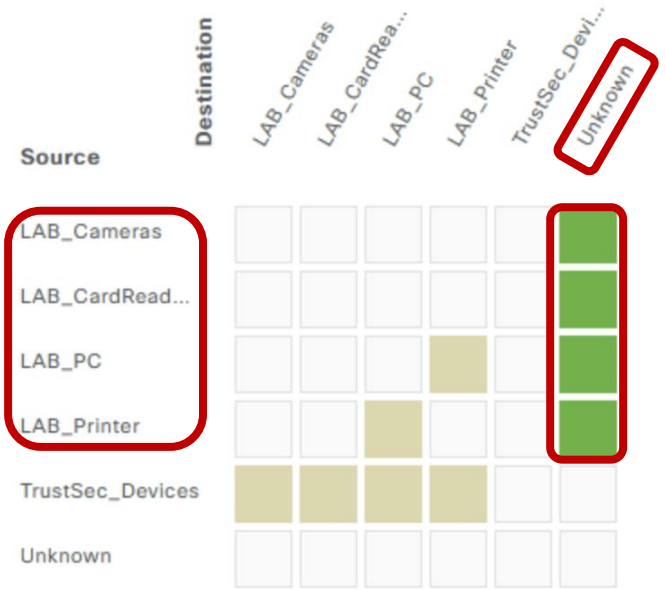


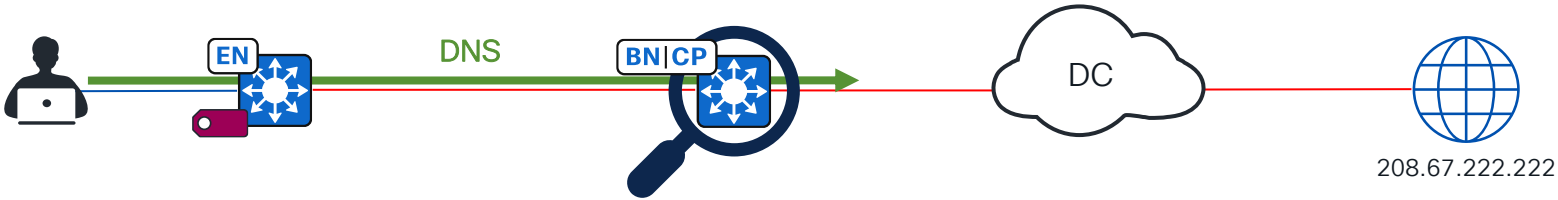


Unclassified destination

South->North Traffic w/ BN Enforcement

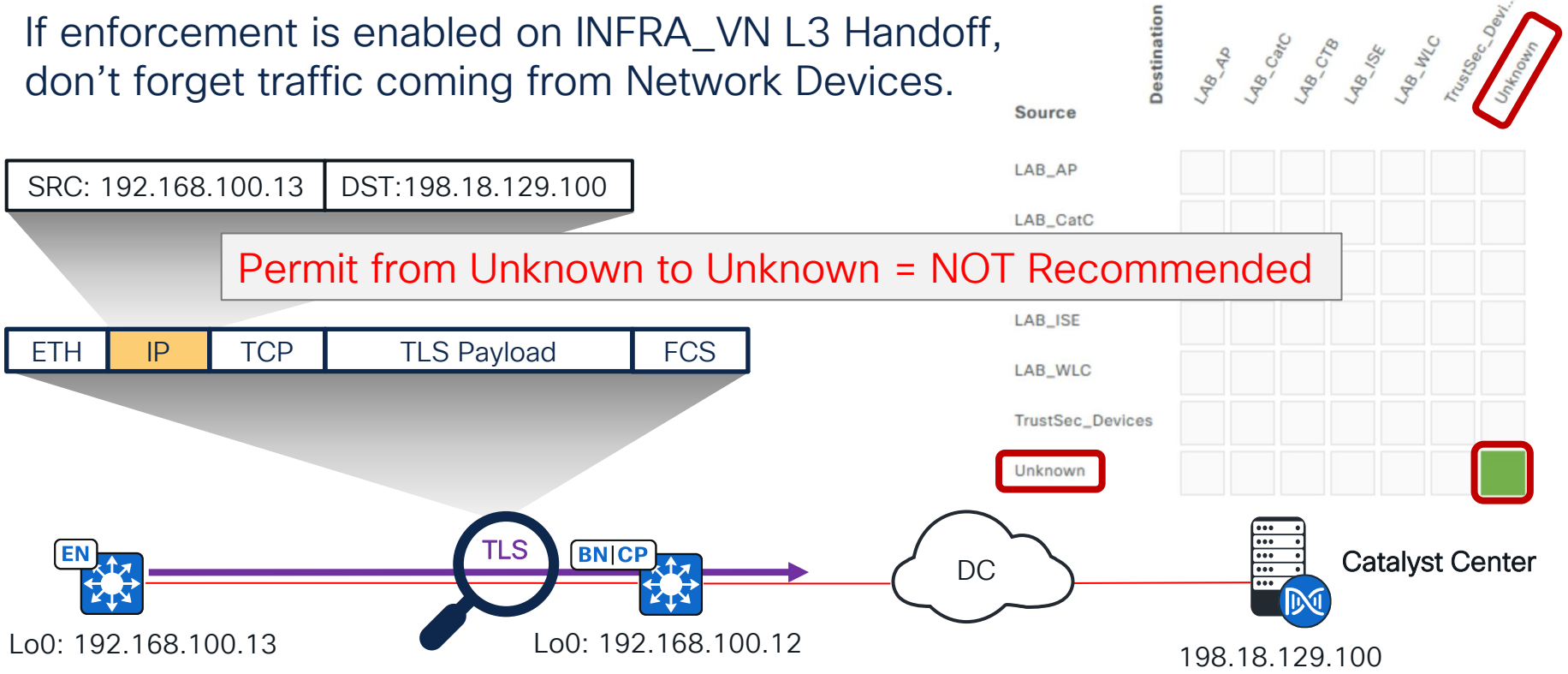
Repeat for any SGTs that need to go out.





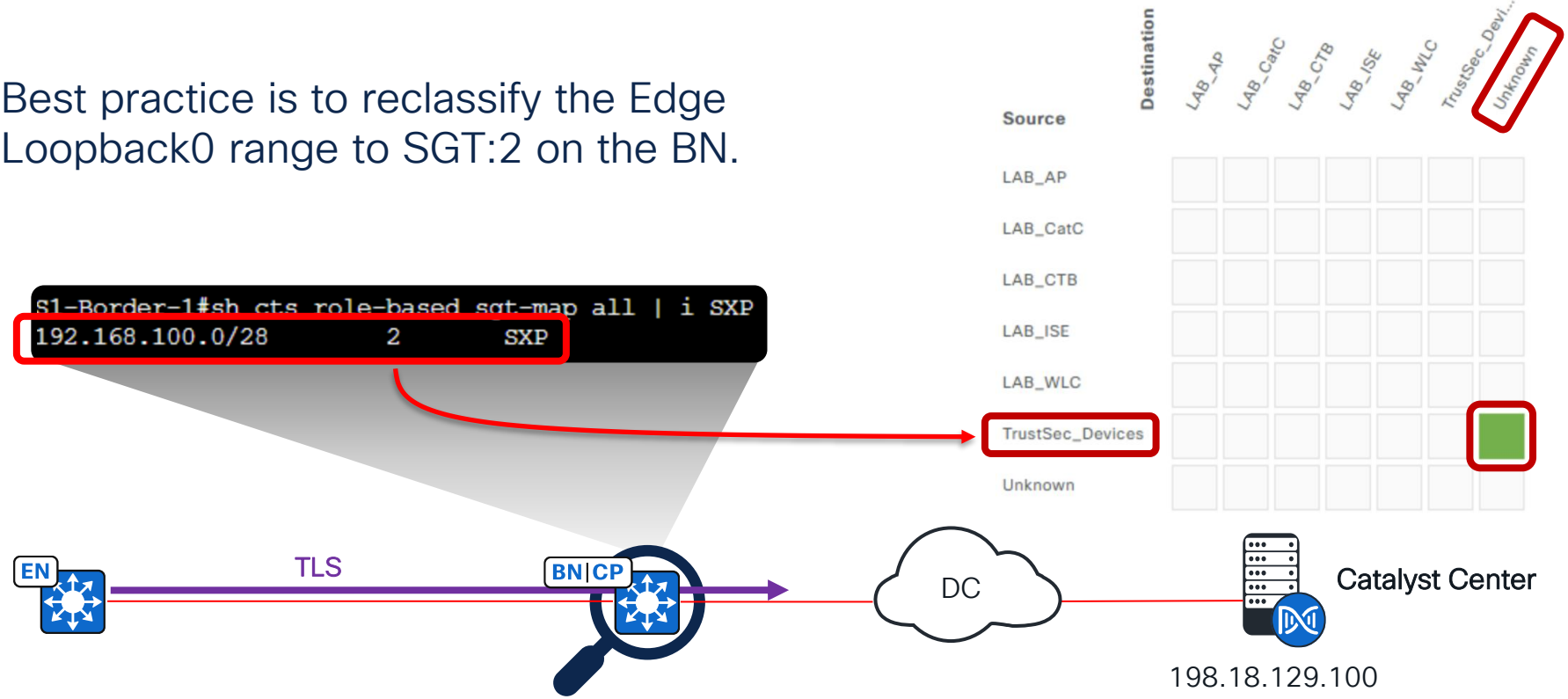
South->North Traffic w/ BN Enforcement

If enforcement is enabled on INFRA_VN L3 Handoff, don't forget traffic coming from Network Devices.



South->North Traffic w/ BN Enforcement

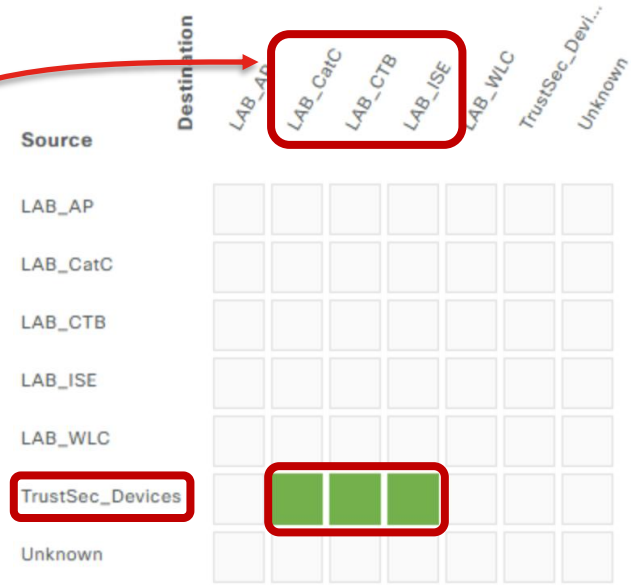
Best practice is to reclassify the Edge Loopback0 range to SGT:2 on the BN.

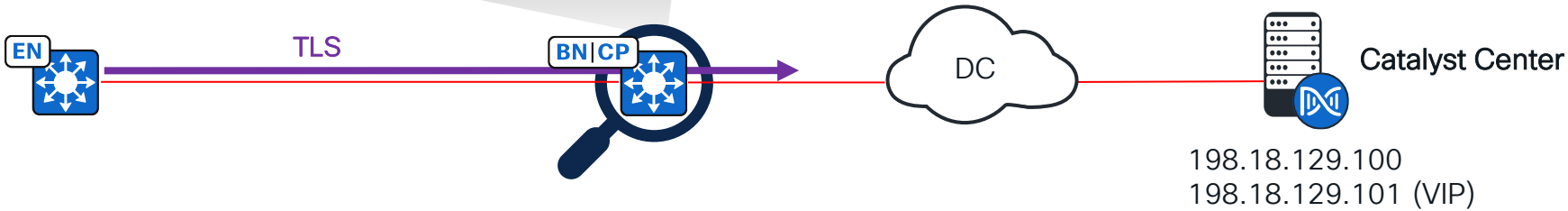


South->North Traffic w/ BN Enforcement

CC, ISE and CTB can also be classified to remove Unknown from the equation.

```
S1-Border-1#sh cts role-based sgt-map all | i SXP
192.168.100.0/28        2       SXP
198.18.129.100          23      SXP
198.18.129.101          23      SXP
198.18.133.27           24      SXP
198.18.133.46           25      SXP
Total number of SXP      bindings = 5
```





South->North Traffic w/ BN Enforcement

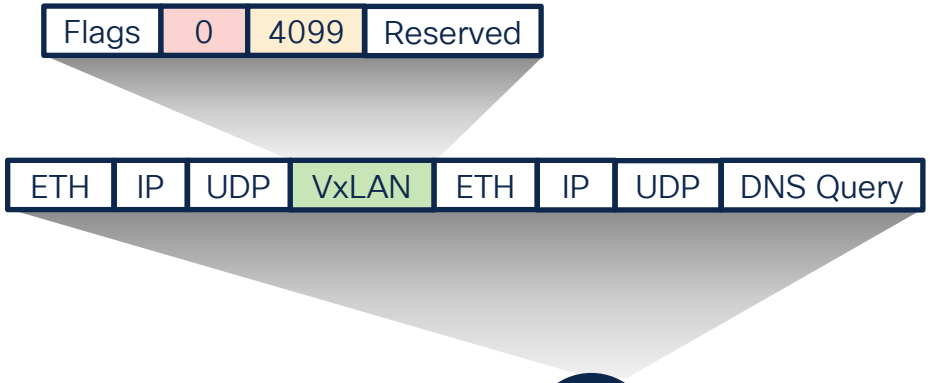
Tips & Tricks

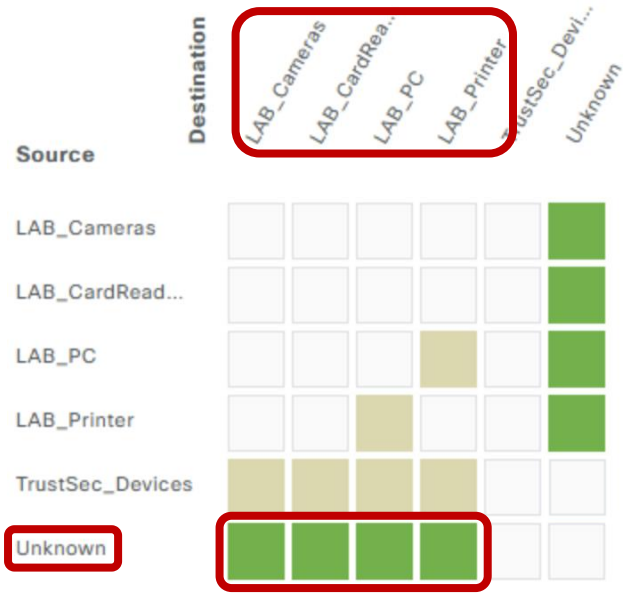
- Use BN enforcement only if required.
- Allow traffic to Unknown for Overlay traffic.
- Block/monitor traffic from Unknown to Unknown.

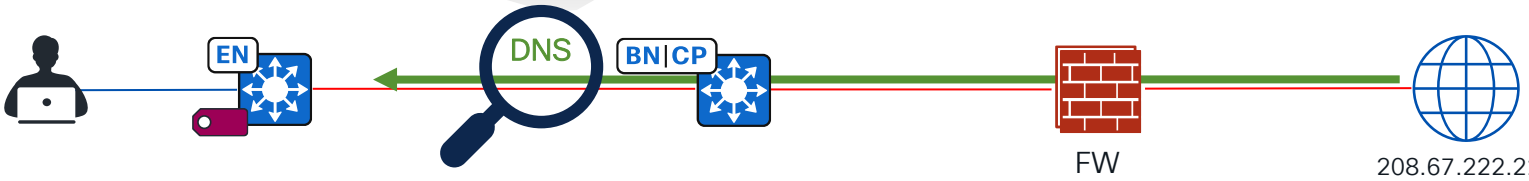
North->South Traffic

North->South Traffic

Returning traffic is enforced on Edges and should be explicitly allowed.

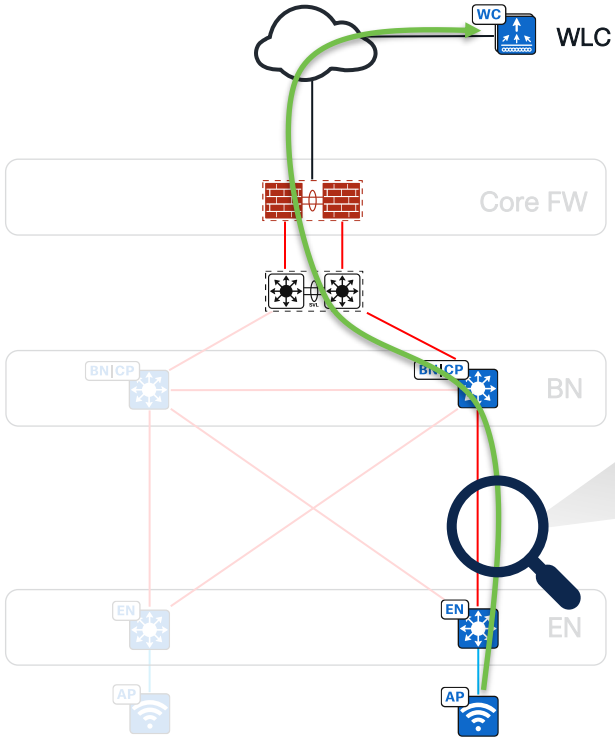






INFRA_VN Traps

Fabric Enabled Wireless – AP to WLC



In most situations*, CAPWAP traffic from Fabric AP to WLC is not VxLAN encapsulated.

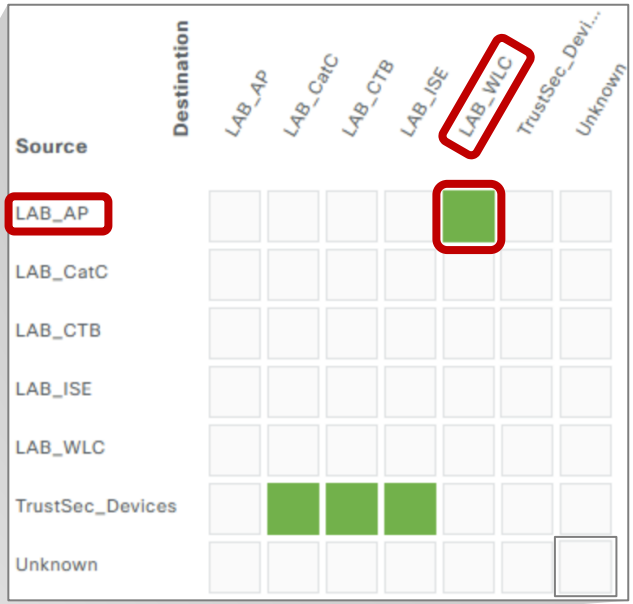
Any classification on ENs for Fabric AP traffic is not propagated.

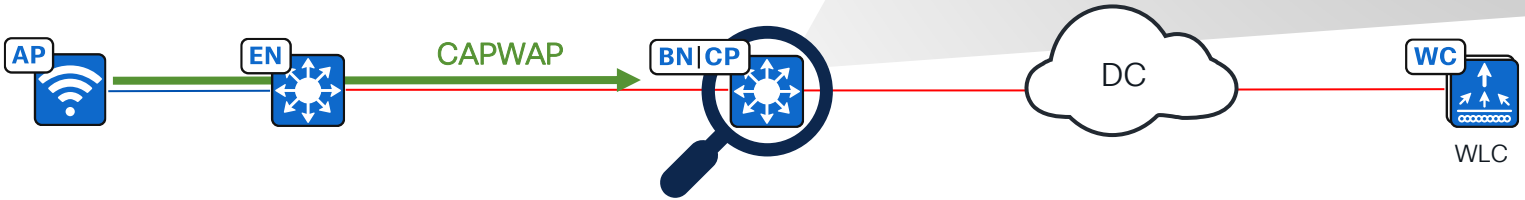
*When using External Borders and 0.0.0.0/0 is present in underlay

Fabric Enabled Wireless – AP to WLC

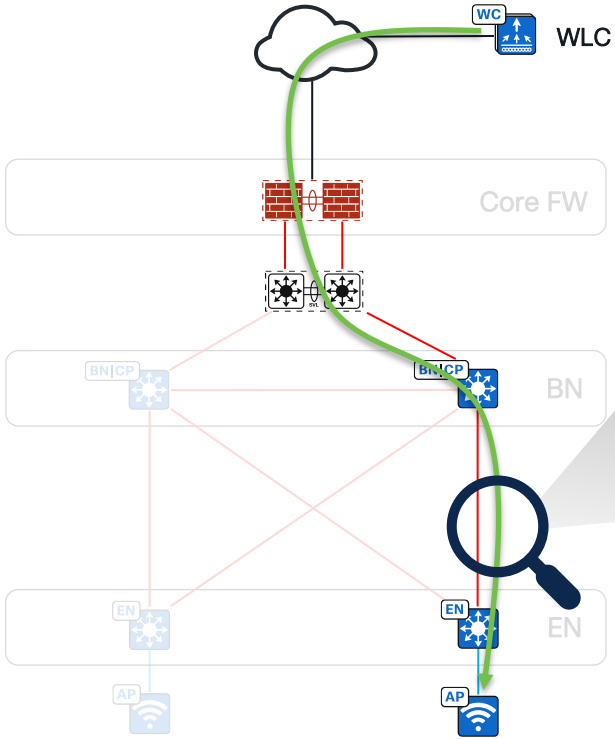
If Enforcement is enabled on INFRA_VN L3 Handoff:

Best practice is to reclassify Fabric AP range & External WLC on BN to avoid allowing traffic from unknown to unknown.





Fabric Enabled Wireless – WLC to AP



Capwap returning from WLC to Fabric AP is VxLAN encapsulated.

ETH	IP	UDP	VxLAN	ETH	IP	UDP	CAPWAP	FCS

Any re-classification on BN will be propagated.

Fabric Enabled Wireless – WLC to AP

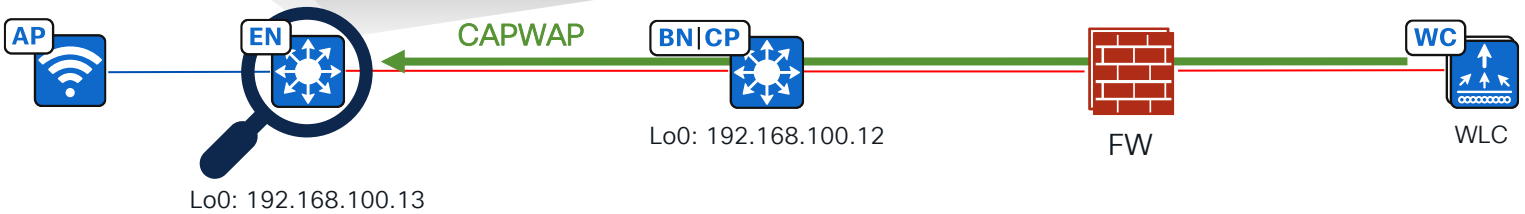
To enforce returning traffic:

- Enforcement needs to be enabled on Fabric AP VLAN.
- ENs need to download the policies, so classification needs to be done on interfaces facing Fabric APs.

```
S1-Edge-1#sh run int gi1/0/5 | s cts
cts manual
 policy static sgt 21
 no propagate sgt
```

```
S1-Edge-1#sh cts role-based permissions from 26 to 21
IPv4 Role-based permissions from group 26:LAB_WLC to group 21:LAB_AP:
        Permit IP-00
```

Source \ Destination	LAB_AP	LAB_CatC	LAB_CTB	LAB_ISE	LAB_WLC	TrustSec_Devi...	Unknown
LAB_AP					■		
LAB_CatC							
LAB_CTB							
LAB_ISE							
LAB_WLC	■						
TrustSec_Devices		■	■	■			
Unknown							



Fabric Enabled Wireless

Tips & Tricks

- Enforcement on Fabric AP and SB/PEN mgmt VLANs is disabled since Catalyst Center 2.3.7.6

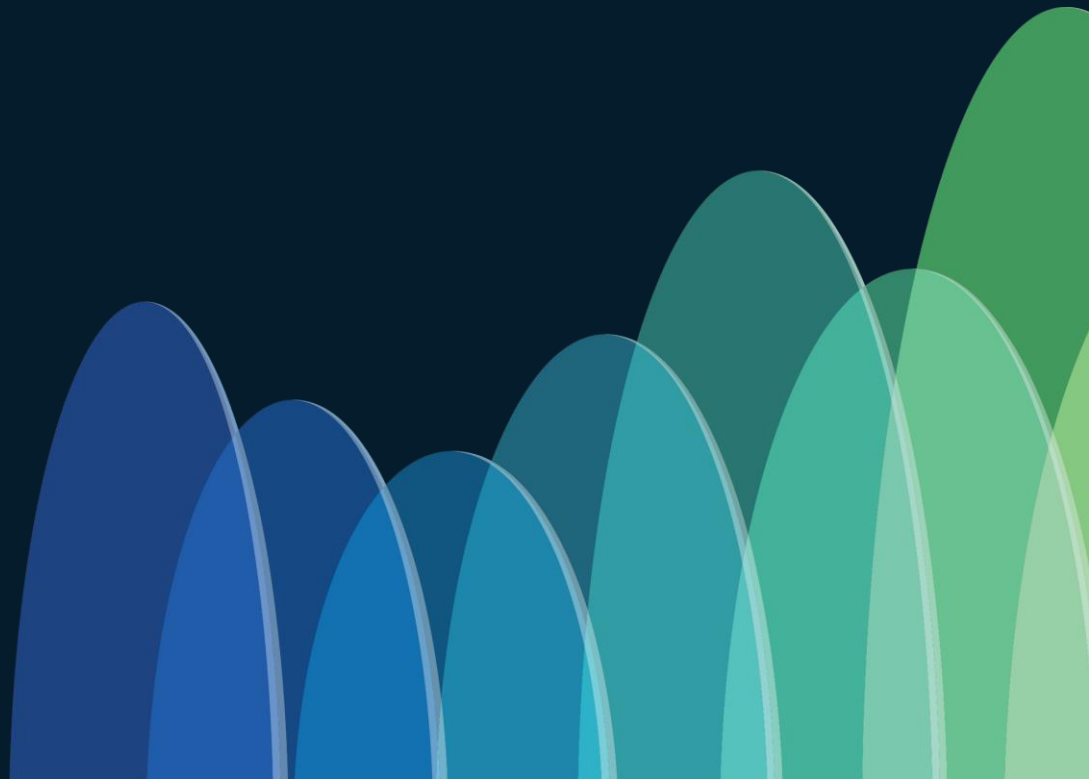
Excluded Traffic

Excluded Traffic

Enforcement is by-passed by default since 17.1.1 on :

- B roadcast traffic (ARP, DHCP etc)
- U nknown unicast traffic
- M ulticast traffic (ISIS Hello, OSPF Hello etc)

Apply the new model



Overview | Policies | Security Groups | Access Contracts

Policies (20) Enter full screen

Upcoming (0) In Progress (0) Failed (0) Default: Permit IP Create Policies

Filter Deploy Refresh View: Default View

Permit Deny Custom Default

Overview | Policies | Security Groups | Access Contracts

Policies (20) Enter full screen

Upcoming (0) In Progress (0) Failed (0) Default: P

Filter | Deploy | Refresh

Permit Deny Custom Default

Expand Minimap

Default Policy

Action

Deny_IP_Log

Once the allow-list model (default deny) is in place, all traffic in the network is blocked for all source-destination policies where there is no selected contract to explicitly permit traffic. That includes traffic from/to the network device, both management-plane (e.g., SSH, SNMP) and control-plane (e.g., BFD, routing protocols).

Cancel | Save Now

Overview | Policies | Security Groups | Access Contracts

Policies (20)

Enter full screen

Upcoming (0) | In Progress (0) | Failed (0) | Default: Deny_IP_Log | Create Policies

Filter | Deploy | Refresh | View: Default View

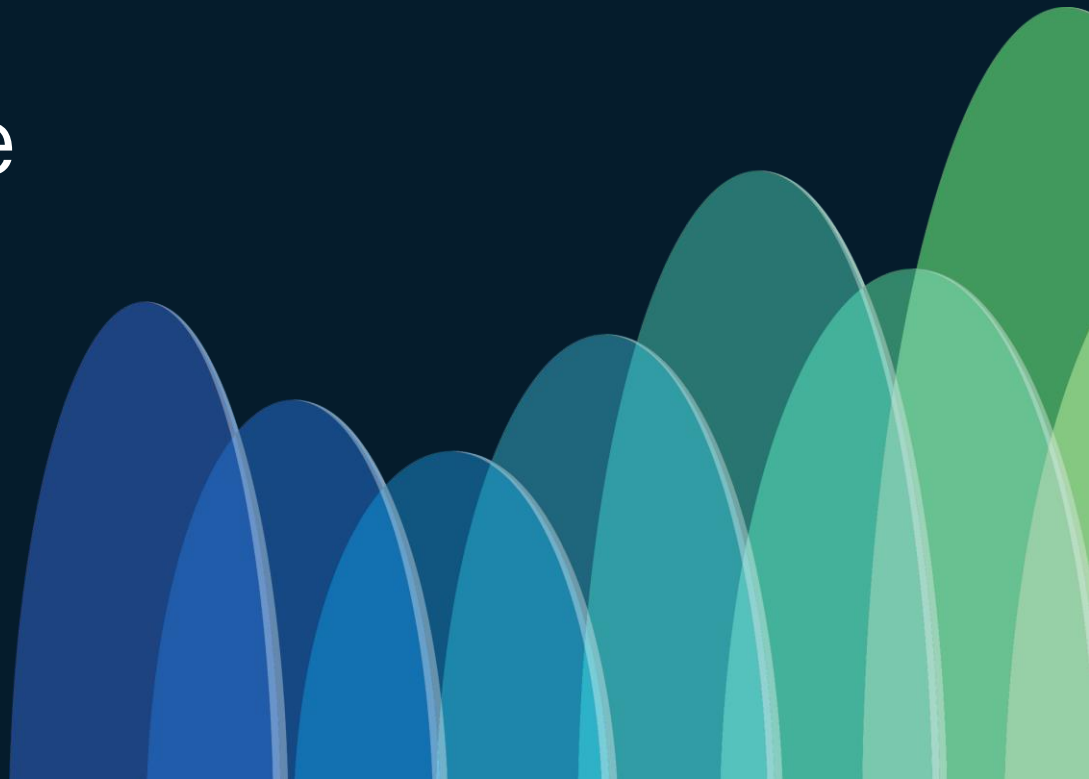
Deploy Now
Schedule Deploy

Permit

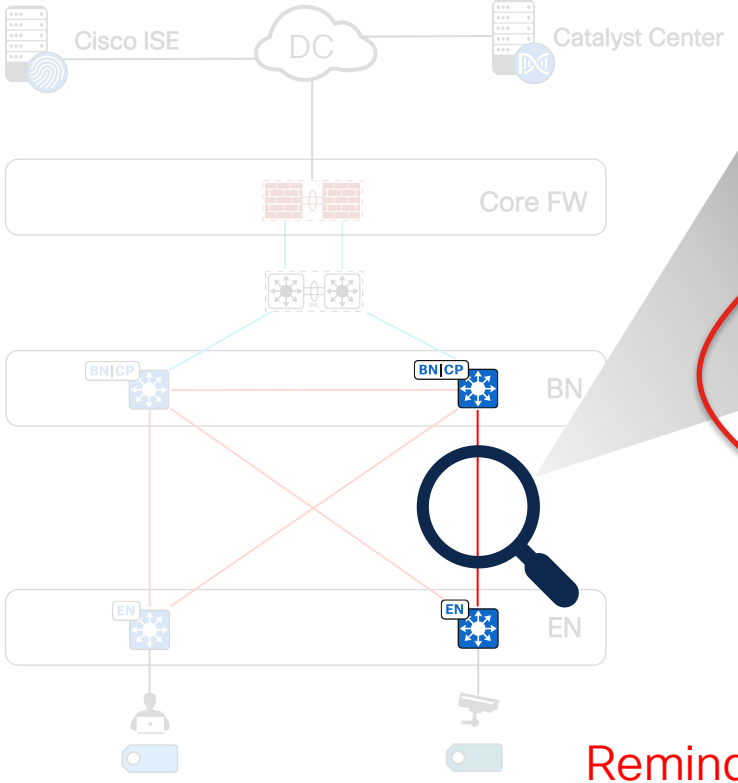
Expand Minimap

Success
Deploy status: DONE

Forgot to disable enforcement on Fabric Links ?



Underlay – Enforcement on Fabric Links

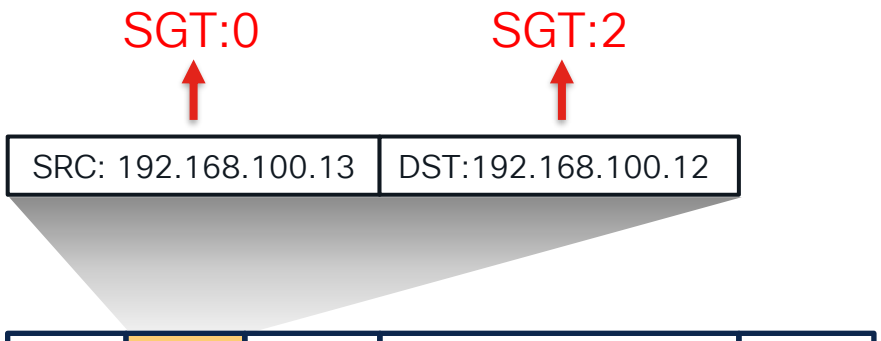


Source	Destination	Protocol	Length	Info
192.168.100.169	192.168.100.130	DHCP	426	DHCP Request - Transaction ID 0x508
192.168.100.130	192.168.100.169	DHCP	409	DHCP ACK - Transaction ID 0x5081ec
192.168.100.14	198.18.129.101	TLSv1.2	598	Application Data
192.168.100.14	192.168.100.12	LISP	308	Msg: 52, Registration for Unknown LC 53, Registration for [4099] 192.168.10
192.168.100.14	198.18.133.27	RADIUS	431	Access-Request id=124
192.168.100.14	198.18.133.27	RADIUS	431	Access-Request id=125
198.18.129.101	192.168.100.14	TCP	66	25103 \xe2\x86\x92 59995 [ACK] Seq Win=126 Len=0 TSval=1437943959 T

```
▶Frame 19: 192 bytes on wire (1536 bits), 192 bytes captured (1536 bits)
▶Ethernet II, Src: RealtekU_0f:5b:9b (52:54:00:0f:5b:9b), Dst: RealtekU_1d:d5:40 (52:54:00:1d:d5:40)
▶Internet Protocol Version 4, Src: 192.168.100.12, Dst: 192.168.100.14
▶Transmission Control Protocol, Src Port: 4342, Dst Port: 27637, Seq: 1, Ack: 255, Len: 138
▶Locator/ID Separation Protocol (Reliable Transport), Msg: 78, Registration ACK for [8188] 192.168.100.170/32
```

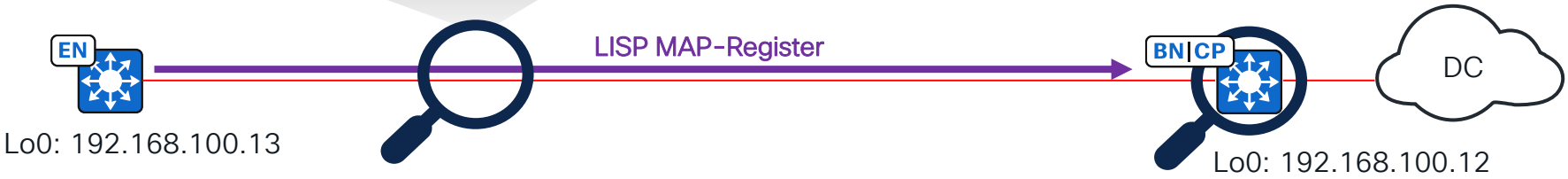
Reminder : CTS Propagation is disabled in the Underlay

Underlay – Enforcement on Fabric Links



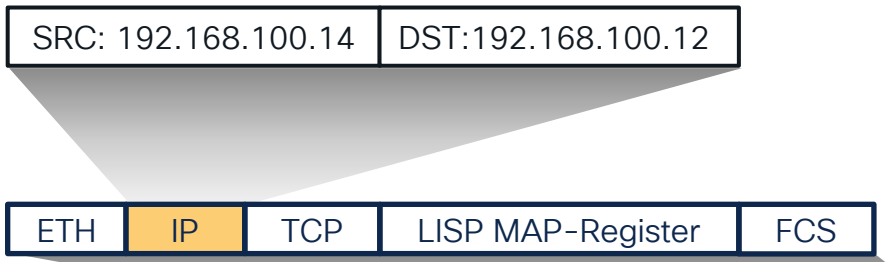
Expectation:

There is no enforcement on ingress traffic, right ?



Underlay – Enforcement on Fabric Links

In reality, the LISP MAP-Register gets dropped before reaching CPU !

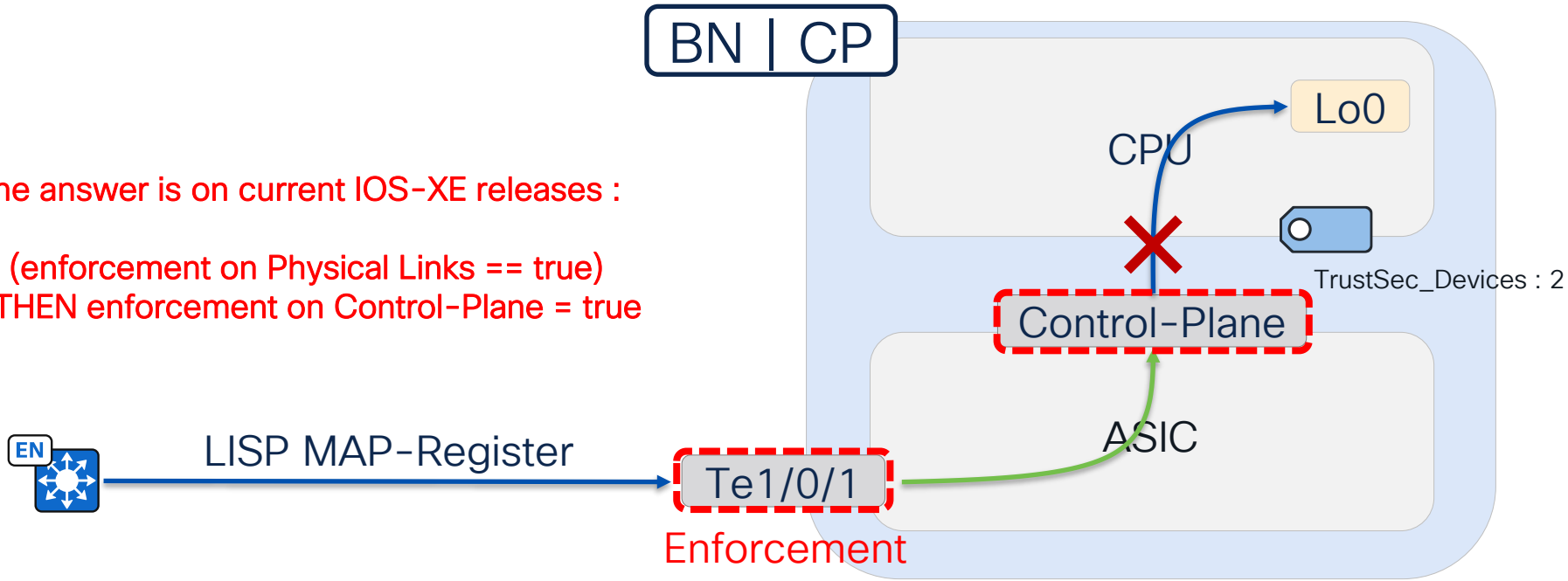



```
S1-Border-2#sh cts role-based counters
Role-based IPv4 counters
From    To      SW-Denied  HW-Denied  S
*       *       0          0          0
0       0       0          0          0
0       2       5          0          1
```

Underlay – Enforcement on Fabric Links

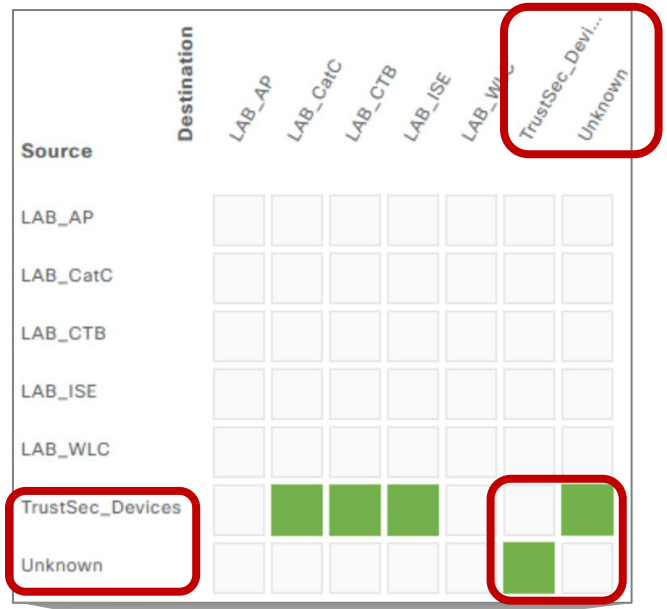
The answer is on current IOS-XE releases :

IF (enforcement on Physical Links == true)
THEN enforcement on Control-Plane = true

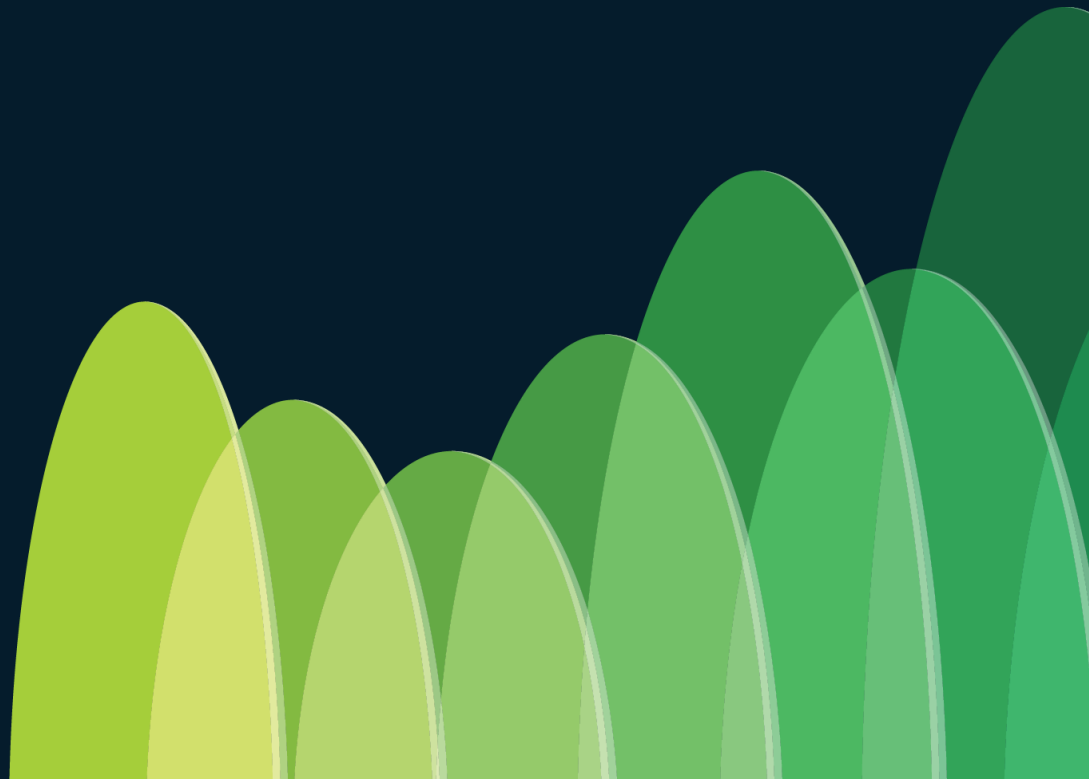


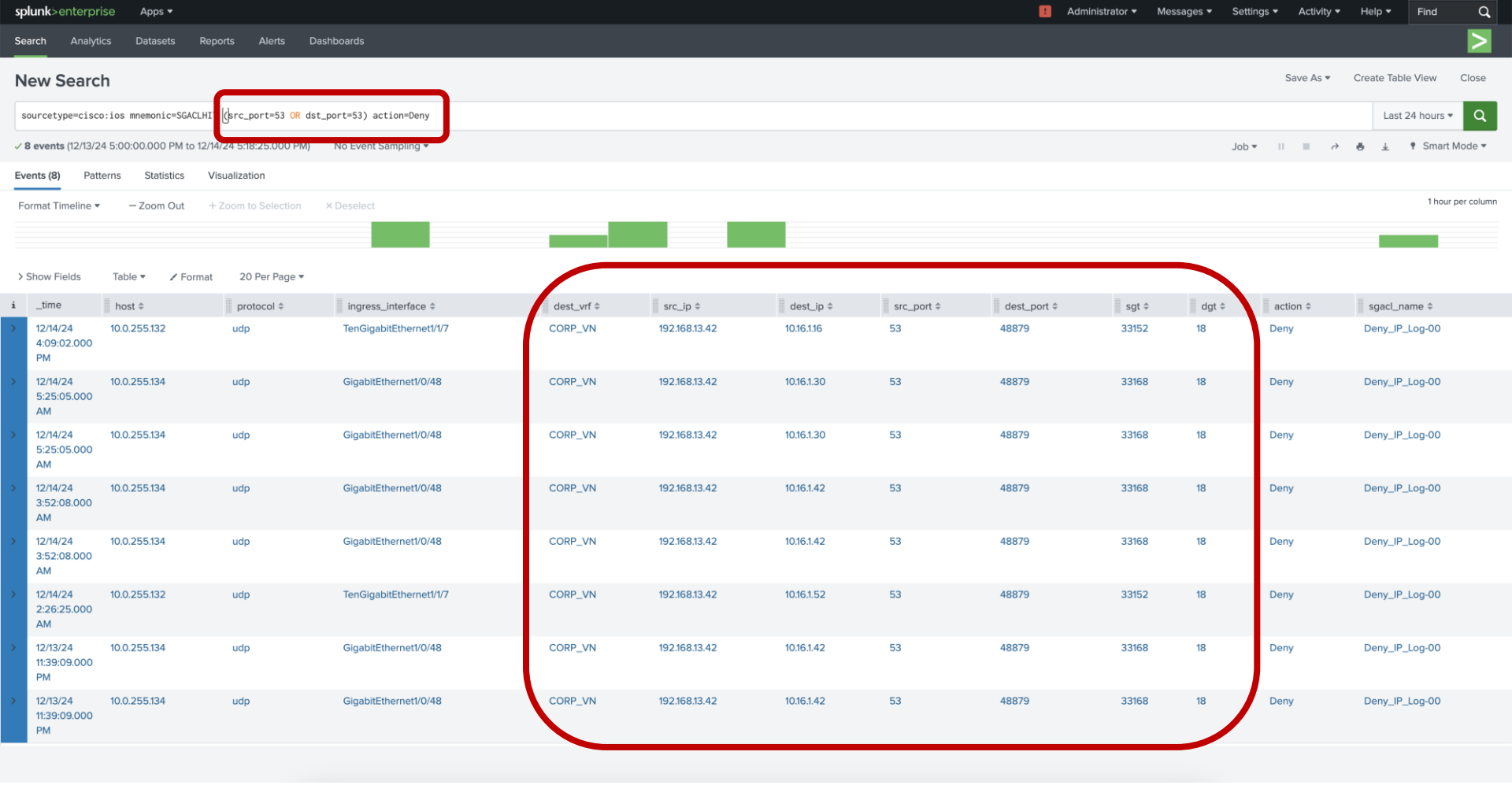
Underlay – Enforcement on Fabric Links

To avoid breaking the underlay (Control-Plane & Data-Plane), both ingress & egress traffic should be allowed.



Monitor & Adapt





Agenda

- Introduction
- Segmentation Strategy
- Observability Pipelines
- Deploy Allow-List Model
- Conclusions

Wrap up time

- Classify all Endpoints (keep Unknown outside of the fabric)
- Choose wisely where enforcement is done (Edge & Firewall)
- Build your logging infrastructure to keep track of drops
- Prepare your TrustSec Matrix
- Verify that enforcement is disabled on Fabric Links
- Change the default contract to Deny_IP_Log
- Monitor and adapt your SGACLs

Webex App

Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.

Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

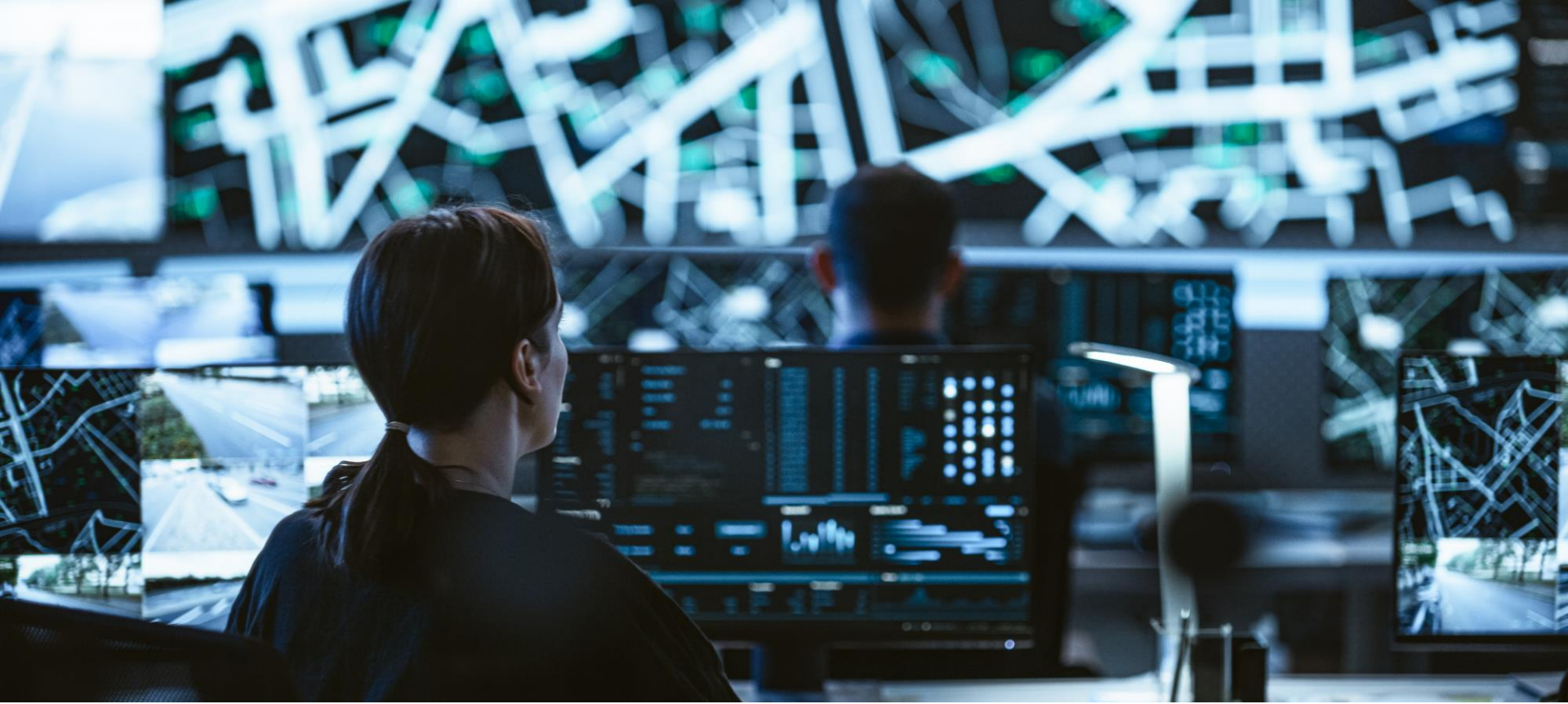
All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

Content Catalog

Continue your education

- Start implementing Zero Trust in your network tomorrow by talking to us today. Meet our engineers (MTE) or plan a meeting with your local SE.
- Full Segmentation Strategy Guide here.
- Zero Trust is also about continuous Endpoints trust evaluation, learn more about AI Endpoint Analytics here.
- Take our Labs on SD-Access : LABENS-2480, LABENS-2410, LTRENS-2509

Contact me at: rlienard@cisco.com



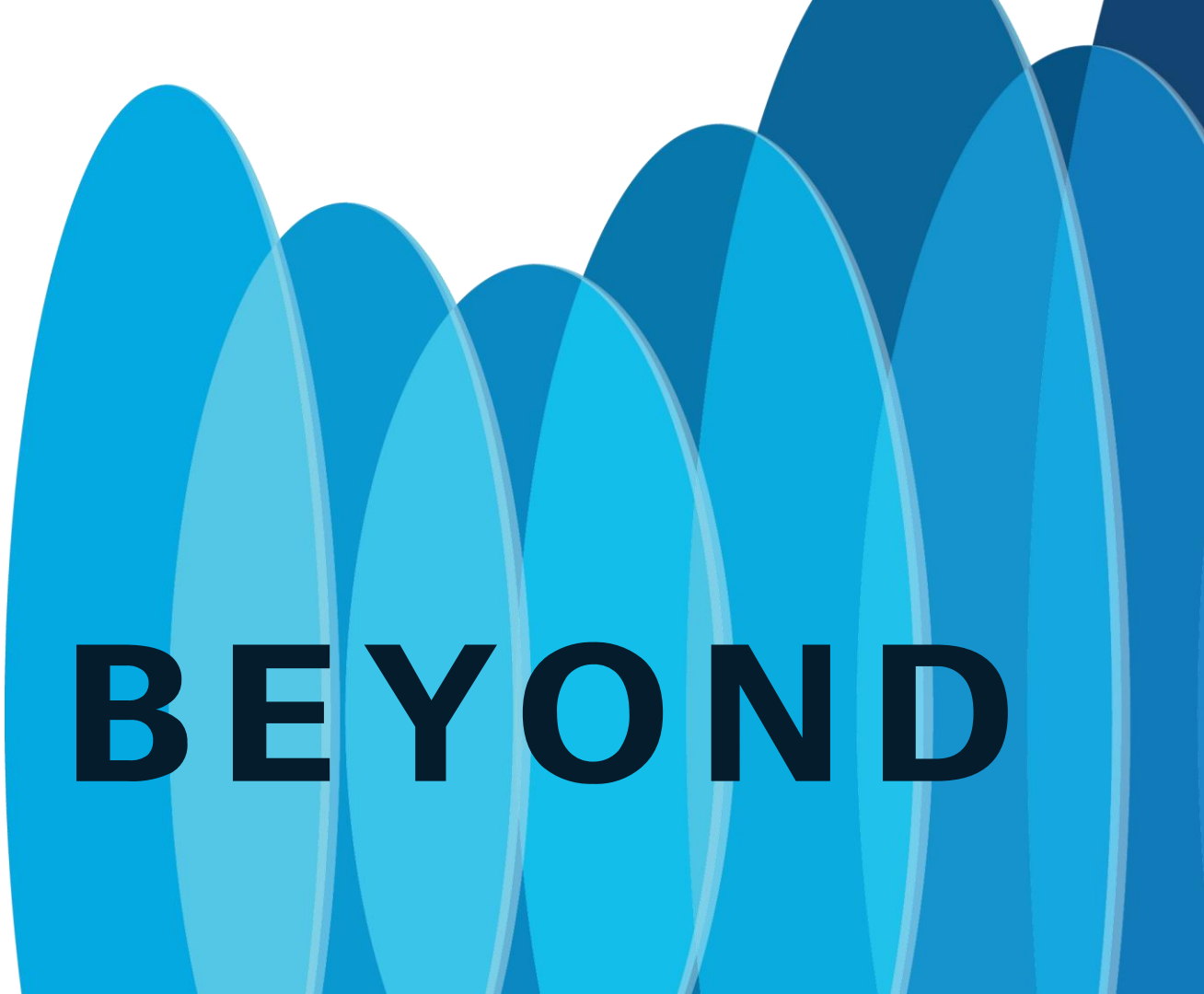
“ *With a **proper plan***, Zero Trust using SD-Access is a no-brainer ”

Next Actions

- Plan A
  - First step
    - Implement it in your lab
    - Validate your configs
  - Second step
    - Apply in production
- Plan B
  - Talk about it to your local SE
  - Get local support


cisco
Thank you
cisco Live!

cisco Live!



GO BEYOND