



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

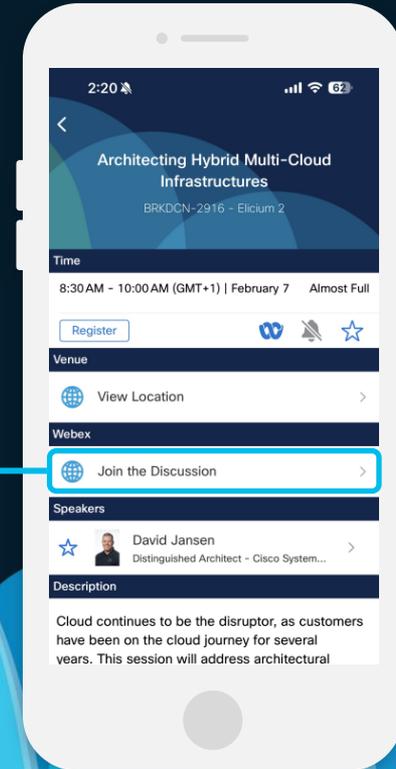
Questions?

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”

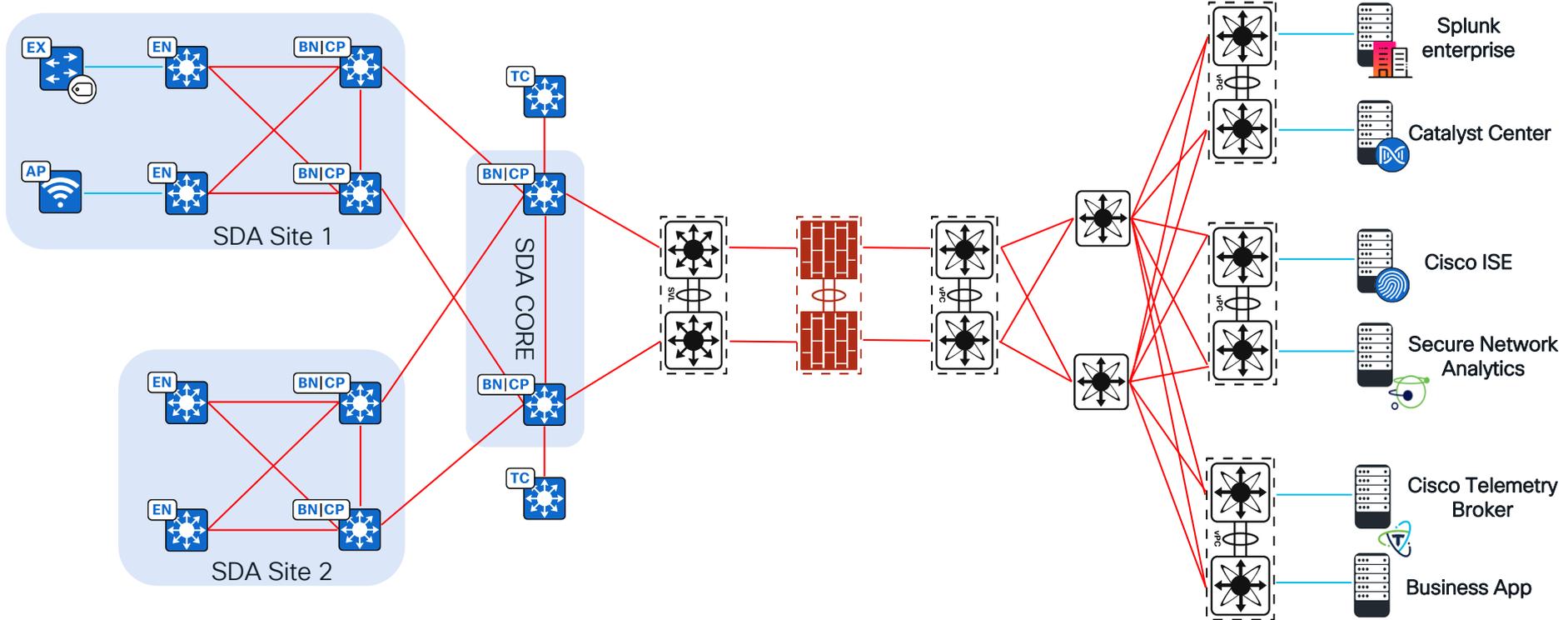


For your
reference

Reference Architecture



For your reference





“ Zero Trust assumes that threats are already inside ”

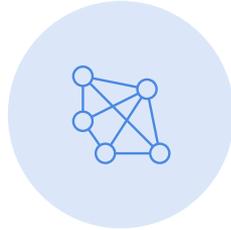
Agenda

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

Classification



Classification

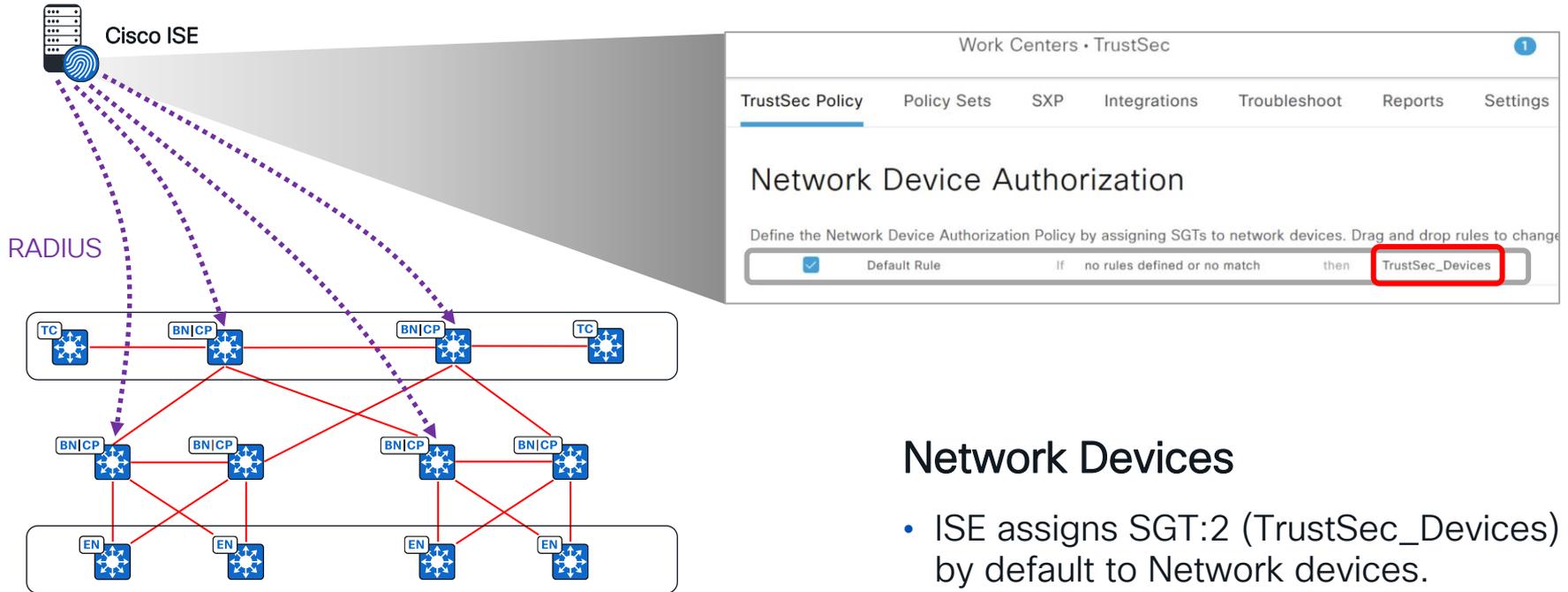


UNDERLAY



OVERLAY

Classification – Network Devices



Network Devices

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

Classification



UNDERLAY

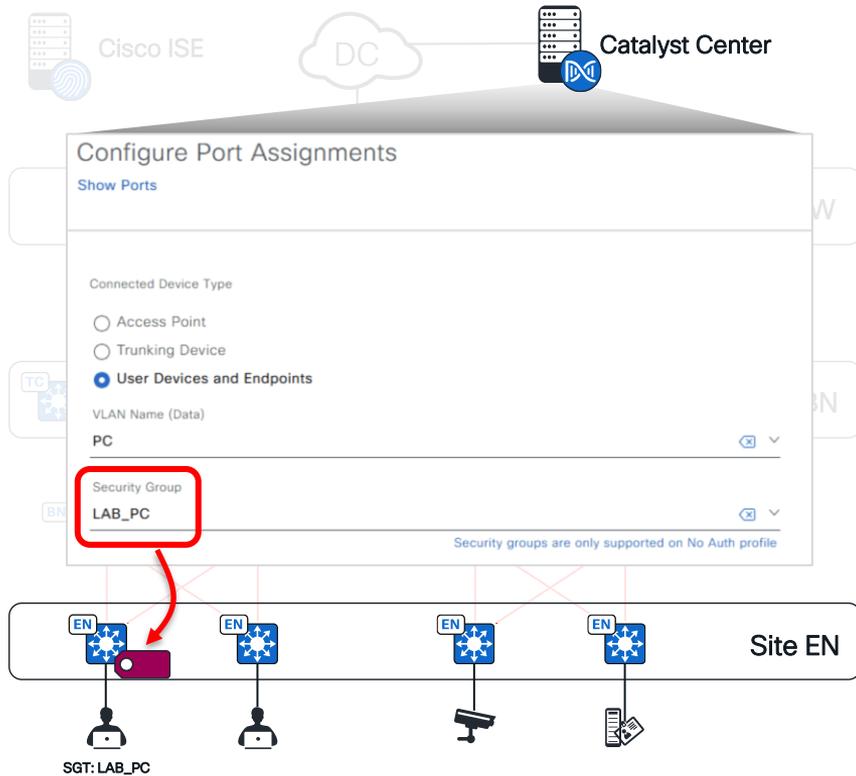


OVERLAY

Edge Nodes



Classification – Internal Endpoints



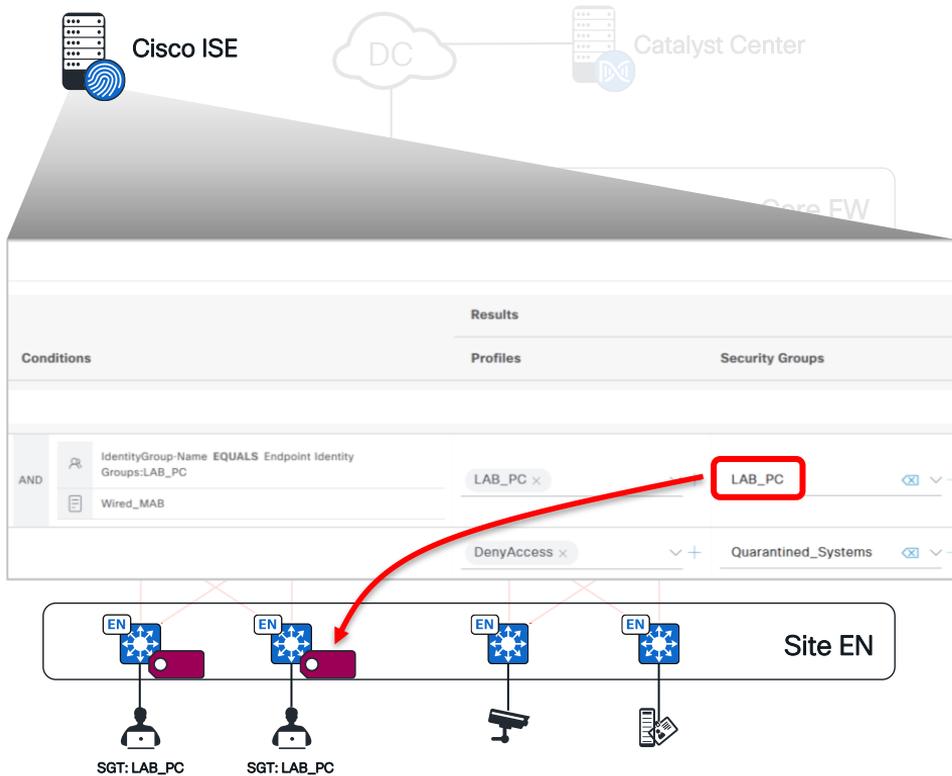
Edge Nodes

- 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



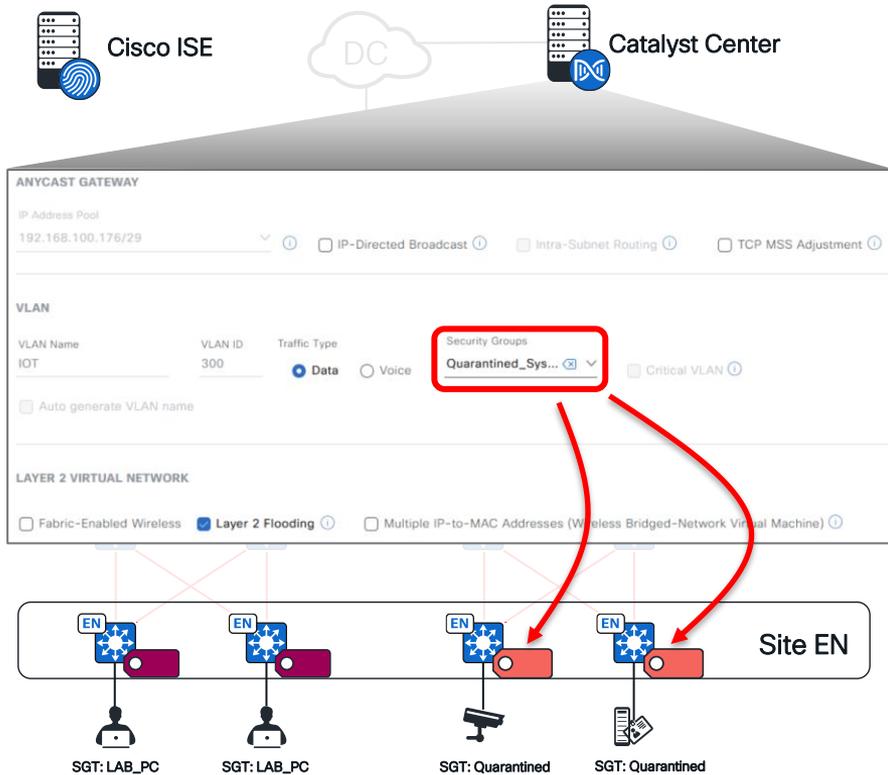
Edge Nodes

- 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

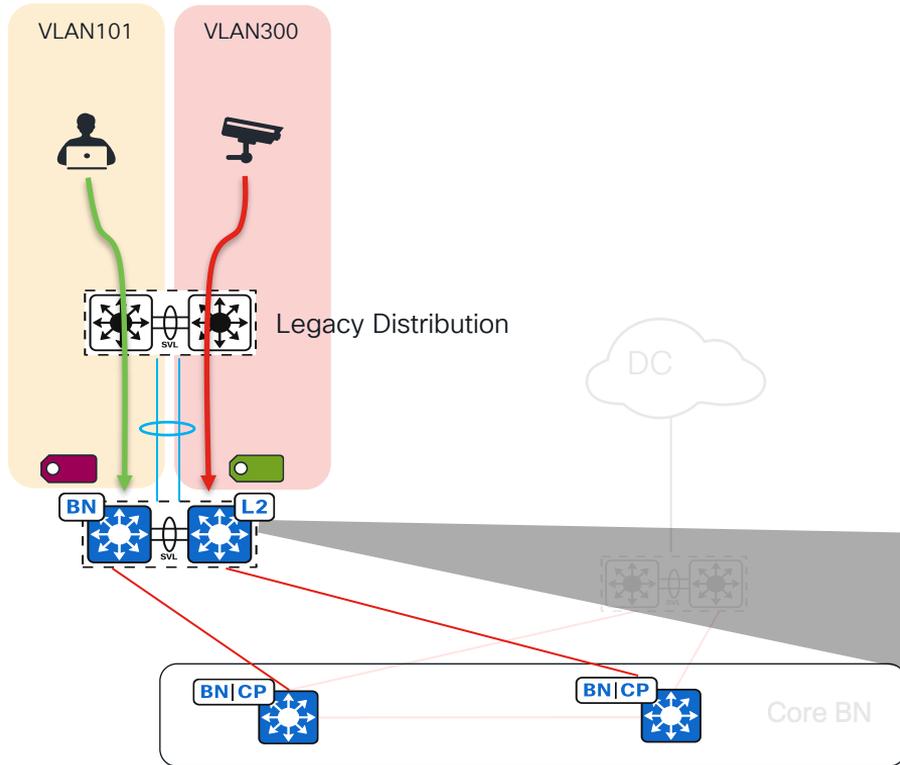
Recommendation

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

Border Nodes



Classification – External Endpoints (L2 Handoff)



Border Nodes

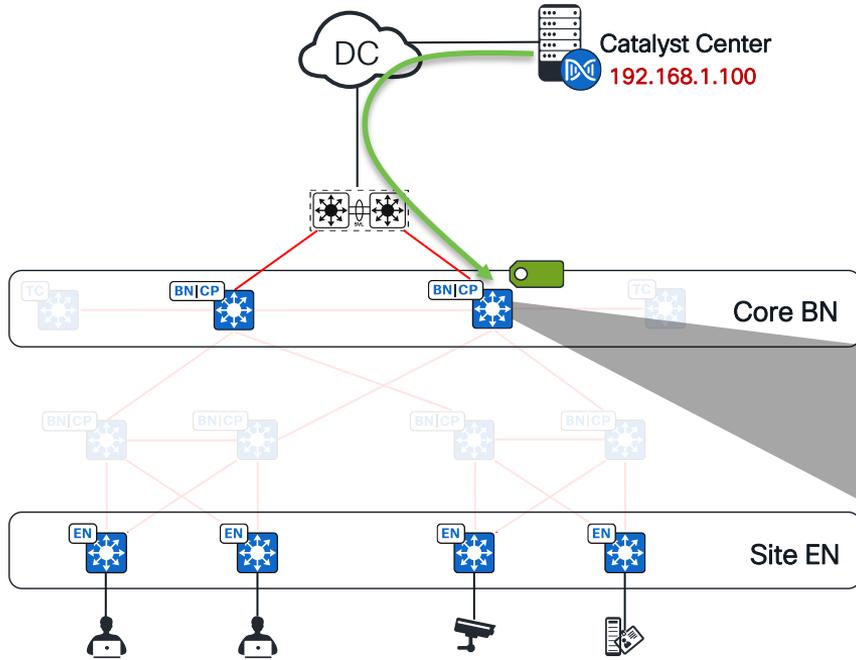
- Static VLAN to SGT Mapping

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)

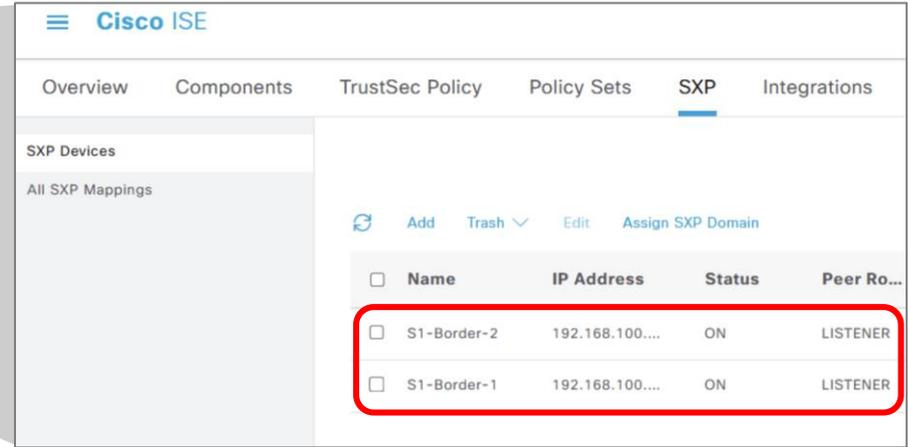
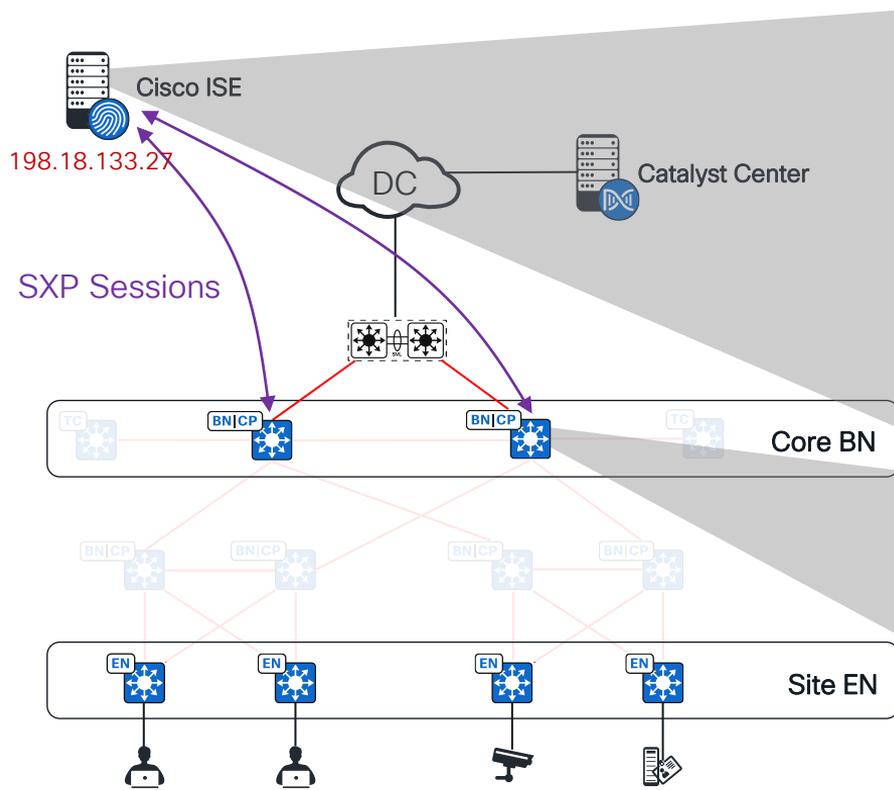


Border Nodes

- 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

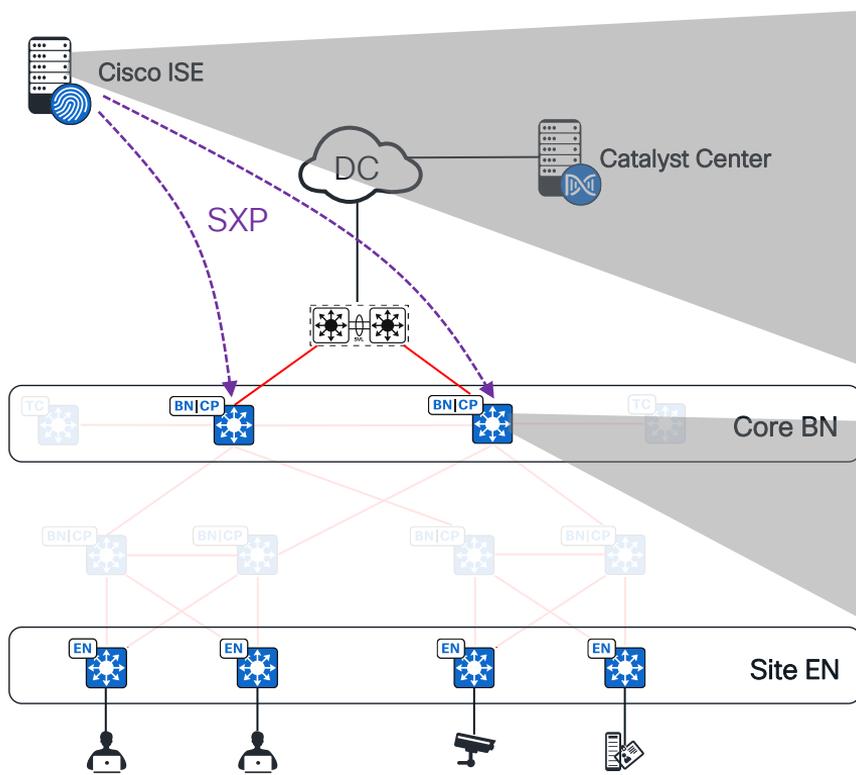


```
DC-Border-2#sh run | i sxp
cts sxp enable
cts sxp default password 7 13211913085D56796A
cts sxp connection peer 198.18.133.27 source 192.168.100.11
password default mode local listener hold-time 0 0
```

Border Nodes

- Dynamic (SXP)

Classification – External Endpoints



Cisco ISE

Overview **Components** TrustSec Policy Policy Sets SXP Integration

Security Groups

IP SGT Static Mapping

Security Group ACLs

Network Devices

Trustsec Servers >

IP address/Host	SGT
<input type="checkbox"/> 192.168.100.0/28	TrustSec_Devices (2/0002)
<input type="checkbox"/> 198.18.129.100	LAB_CatC (23/0017)
<input type="checkbox"/> 198.18.129.101	LAB_CatC (23/0017)

```
DC-Border-2#sh cts role-based sgt-map all | i SXP
```

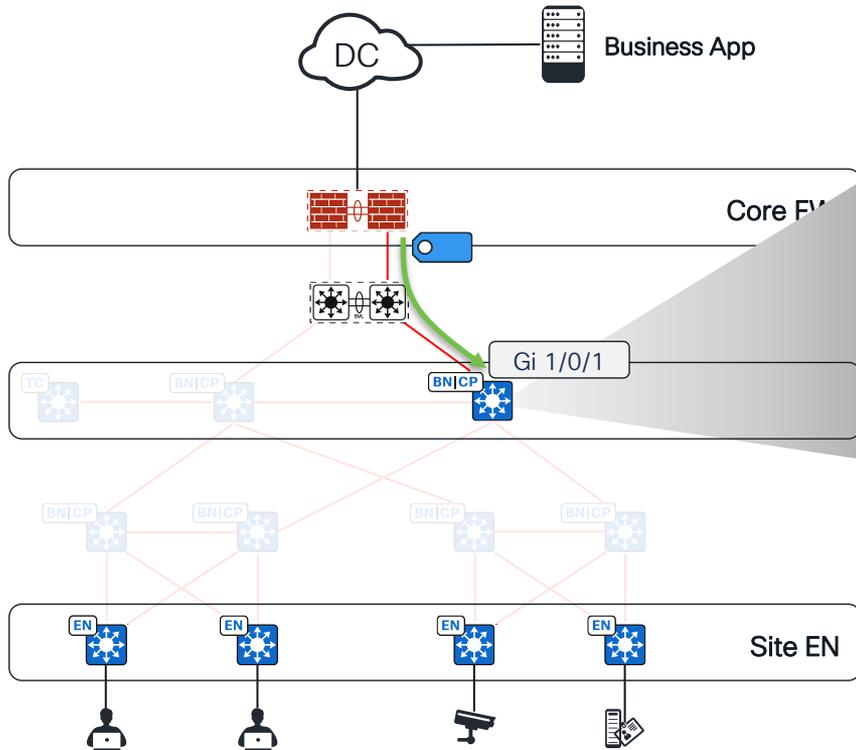
192.168.100.0/28	2	SXP
198.18.129.100	23	SXP
198.18.129.101	23	SXP
198.18.133.27	24	SXP
198.18.133.46	25	SXP

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)
```

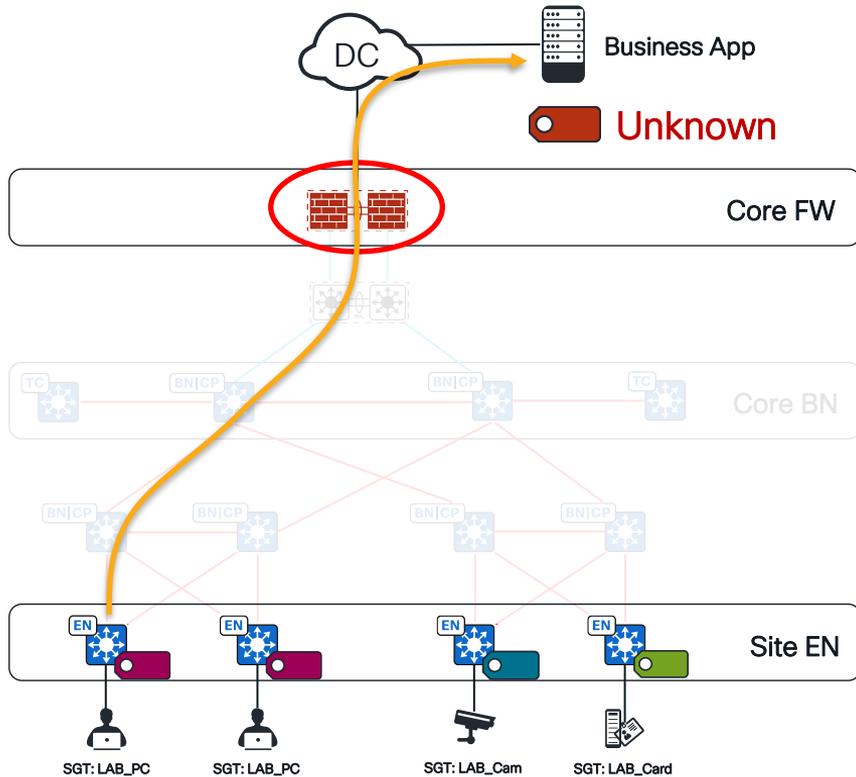
Trusted Classification

- 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



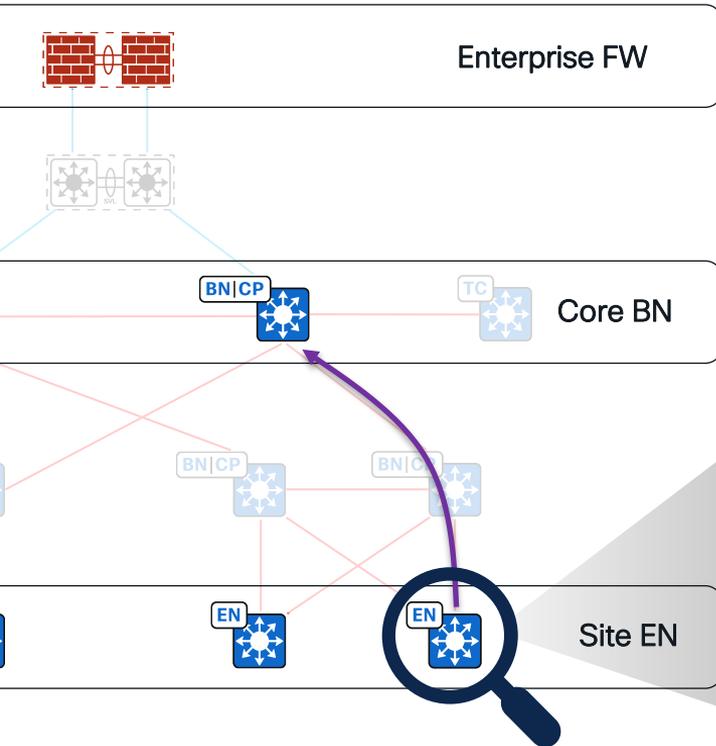
Rules of thumbs

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

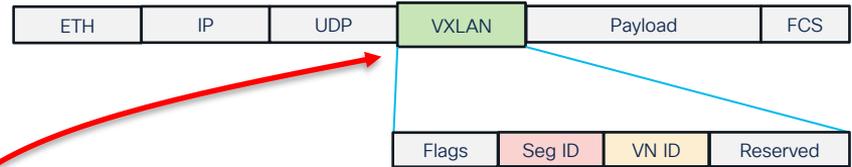
Propagation



Propagation - Dataplane

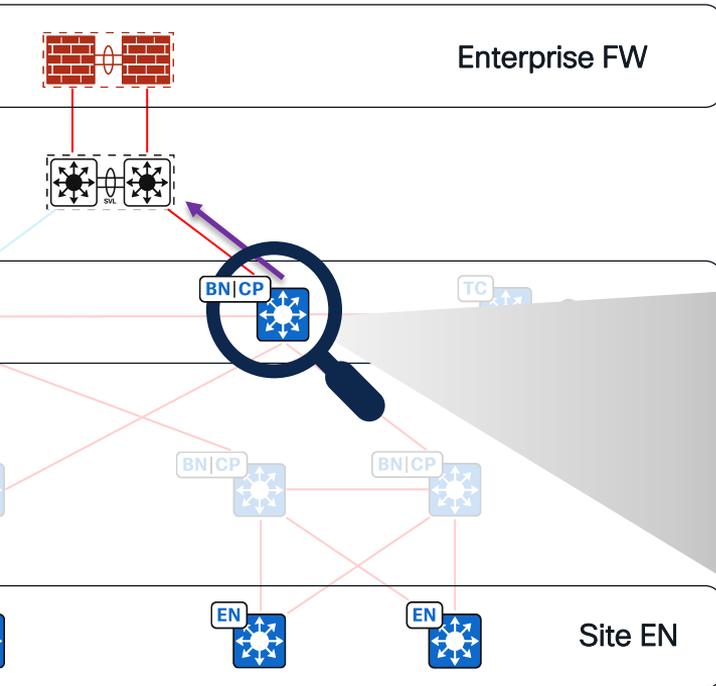


VxLAN-GPO

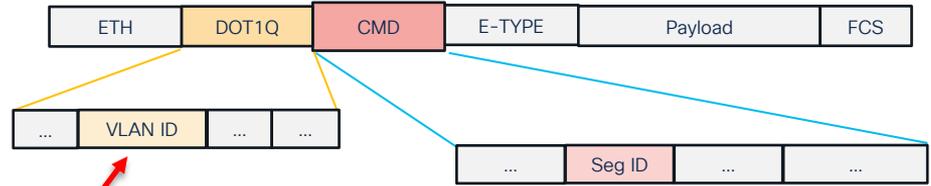


```
router lisp
domain-id 502766789
locator-table default
locator-set rloc_abcff49d-e0a6-4cc5-9f86-9d67136d740a
IPv4-interface Loopback0 priority 10 weight 10
exit-locator-set
!
locator default-set rloc_abcff49d-e0a6-4cc5-9f86-9d67136d740a
service ipv4
encapsulation vxlan
  itr map-resolver 192.168.100.11
  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
  str
  sgt
  no map-cache away-eids send-map-request
  proxy-itr 192.168.100.14
  exit-service-ipv4
!
```

Propagation - Dataplane



DOT1Q + CMD



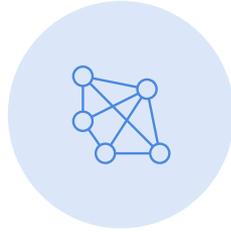
Catalyst 9000 Platforms

```
DC-Border-2# sh run int Gi1/0/1
...
interface GigabitEthernet1/0/1
description I 3-Handoff link
switchport mode trunk
cts manual
policy static sgt 8000 trusted
propagate sgt (hidden)
...
```

Enforcement



Enforcement

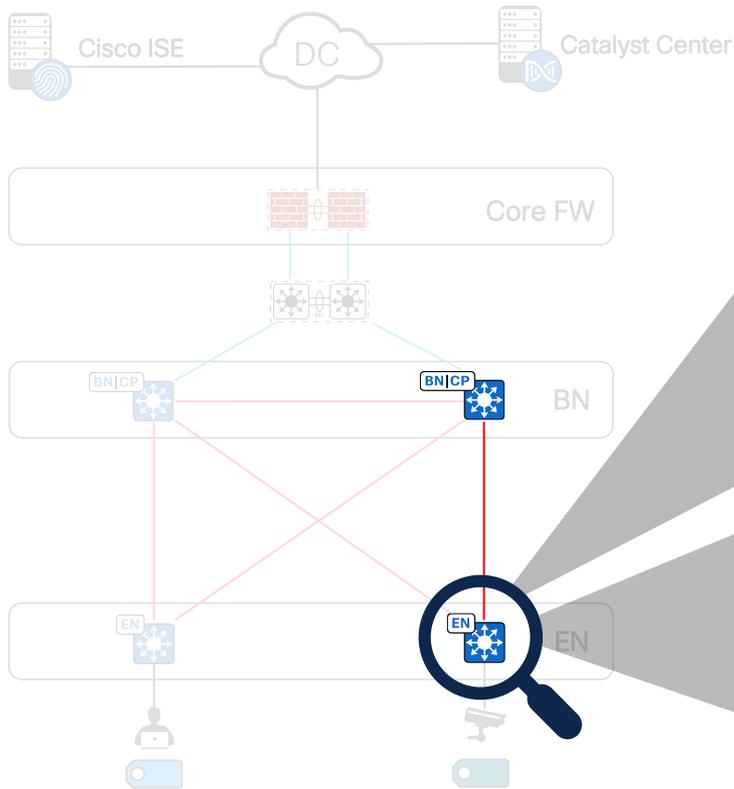


UNDERLAY



OVERLAY

Enforcement - Edges



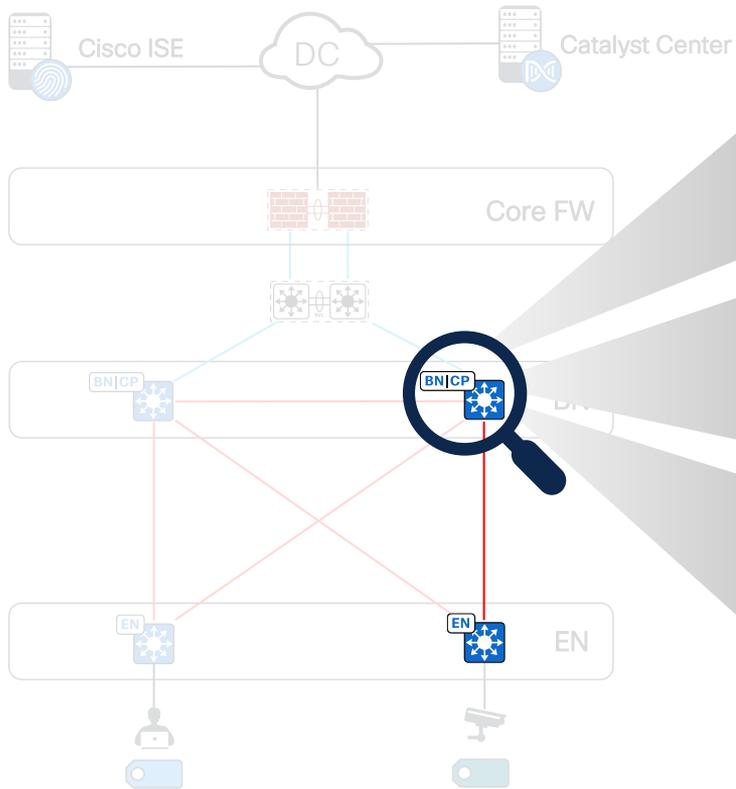
LAN Automated prior Catalyst Center 2.3.7.4

```
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)
...
```

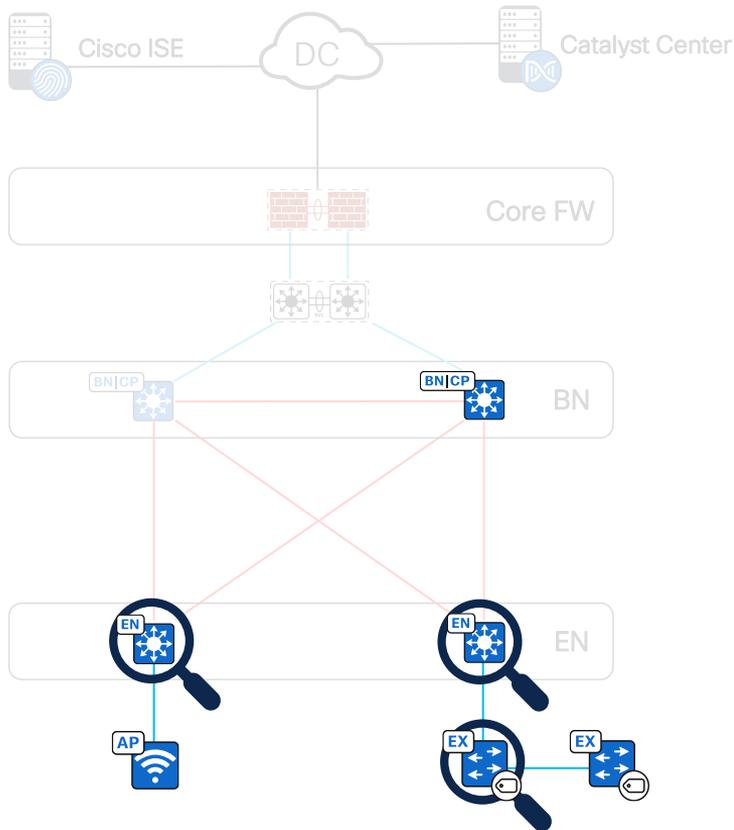
LAN Automated by DNA Center 2.3.3.x

```
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



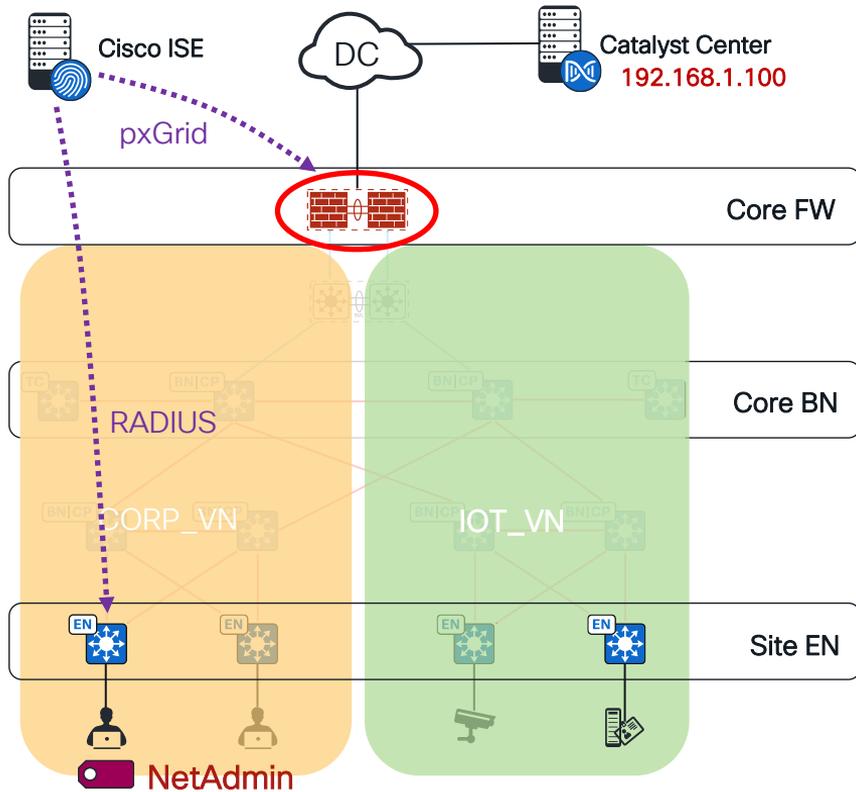
OVERLAY

Enterprise Firewall

(Macro-Seg)



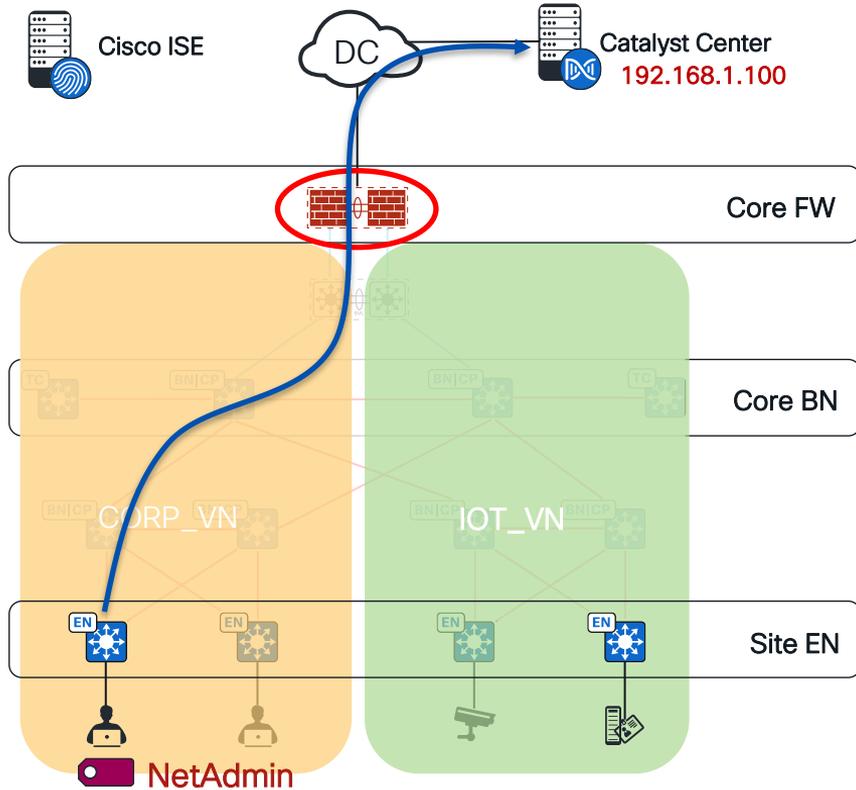
Enforcement



Enterprise Firewall

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

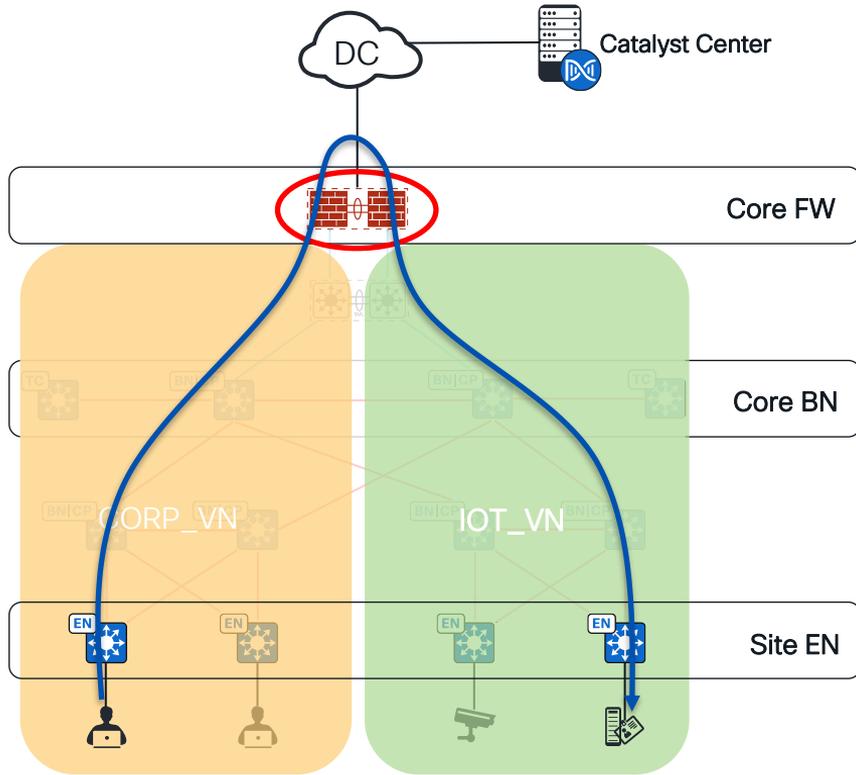
Enforcement



Enterprise Firewall

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

Enforcement



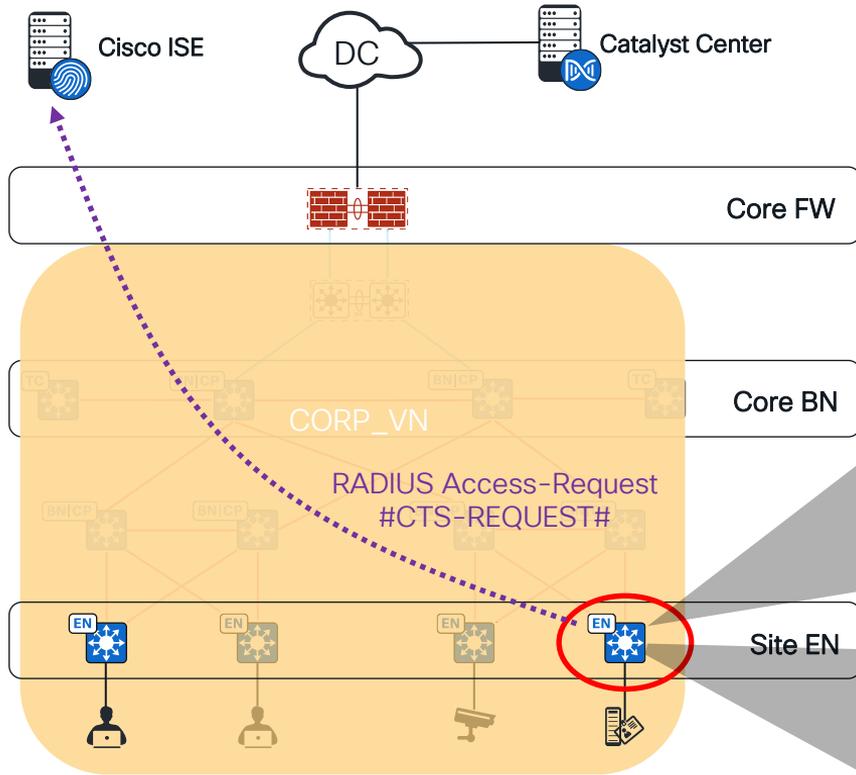
Enterprise Firewall

- 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

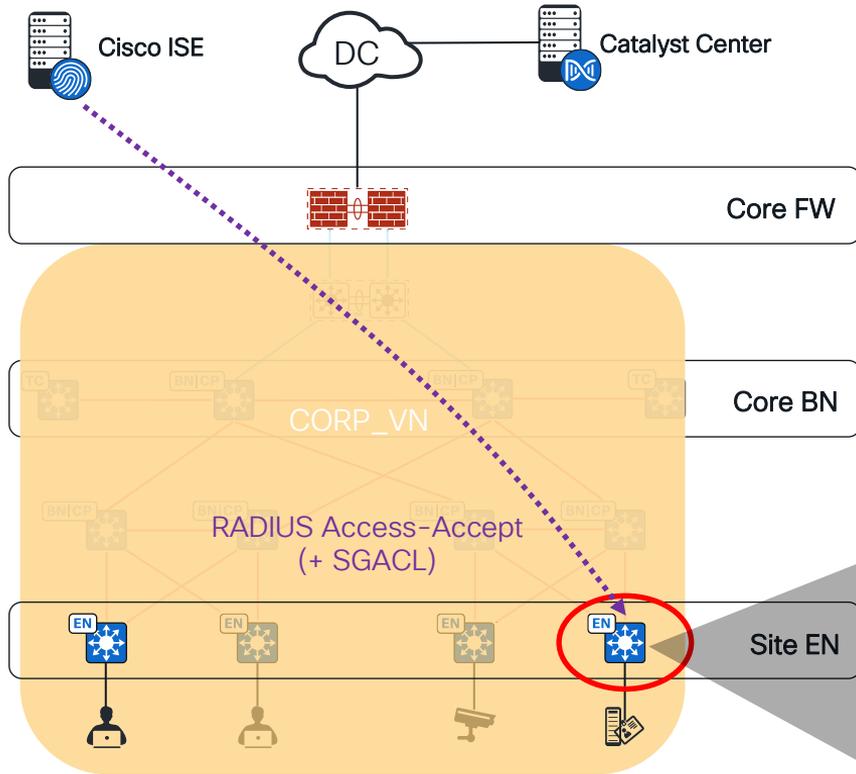
- Stateless inspection
- Protect East <-> West traffic

```
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

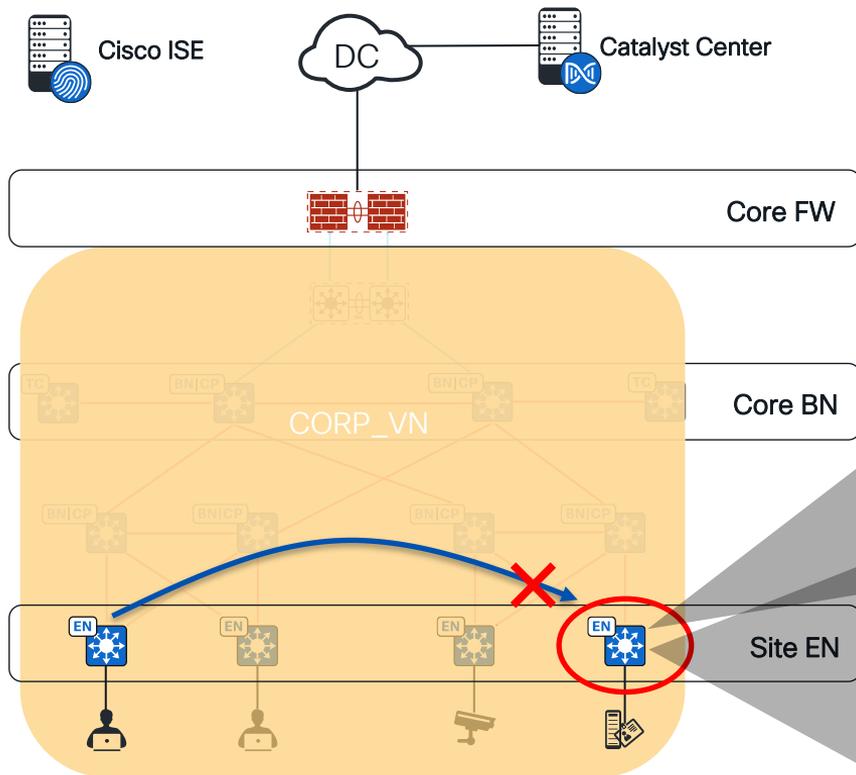


Edge Nodes

- 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



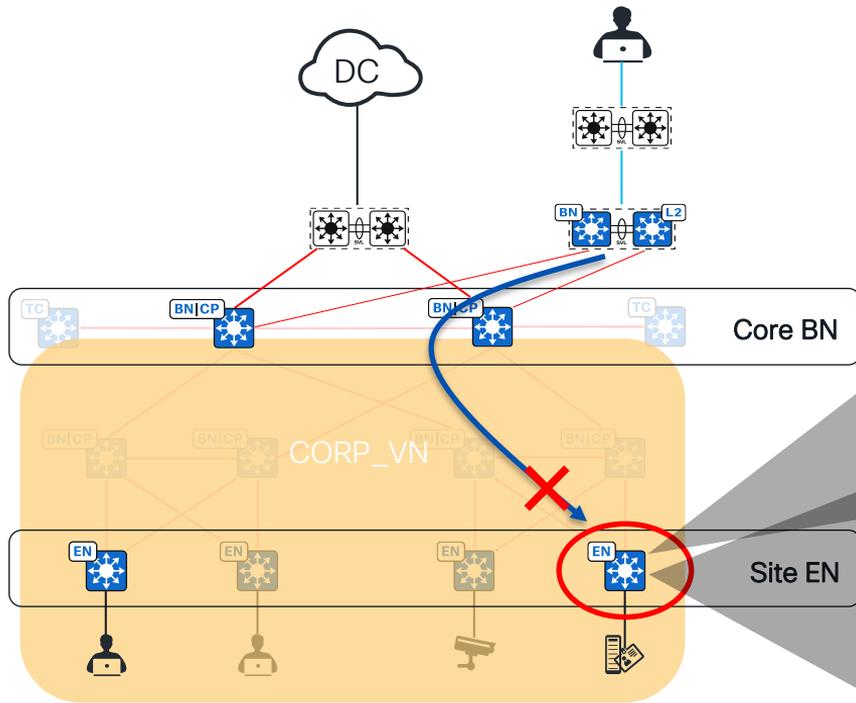
Edge Nodes

- 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
```

```
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 North -> South traffic

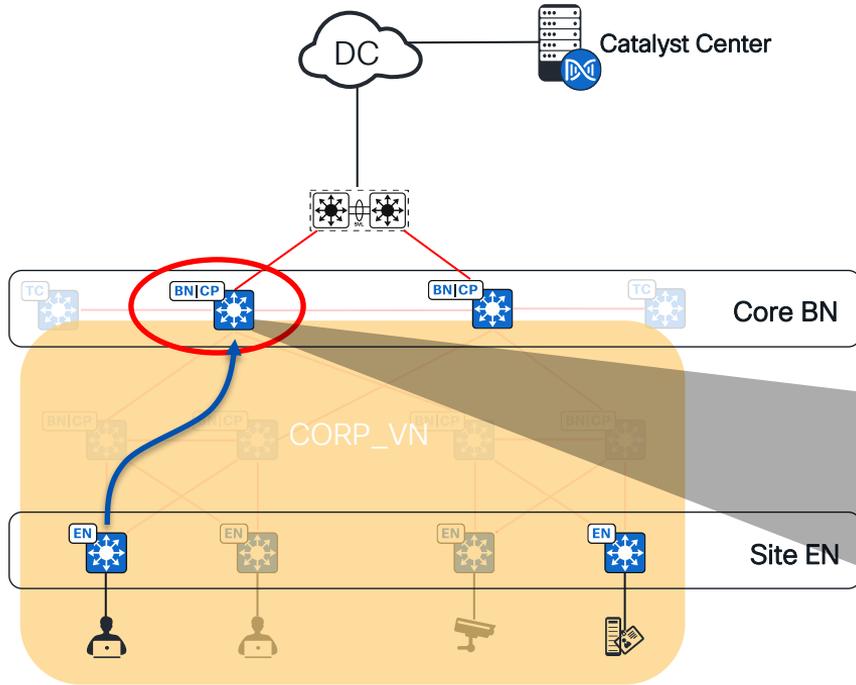
```
S1-Edge-2#sh run | i enforcement
cts role-based enforcement
cts role-based enforcement vlan-list 101,300
```

```
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

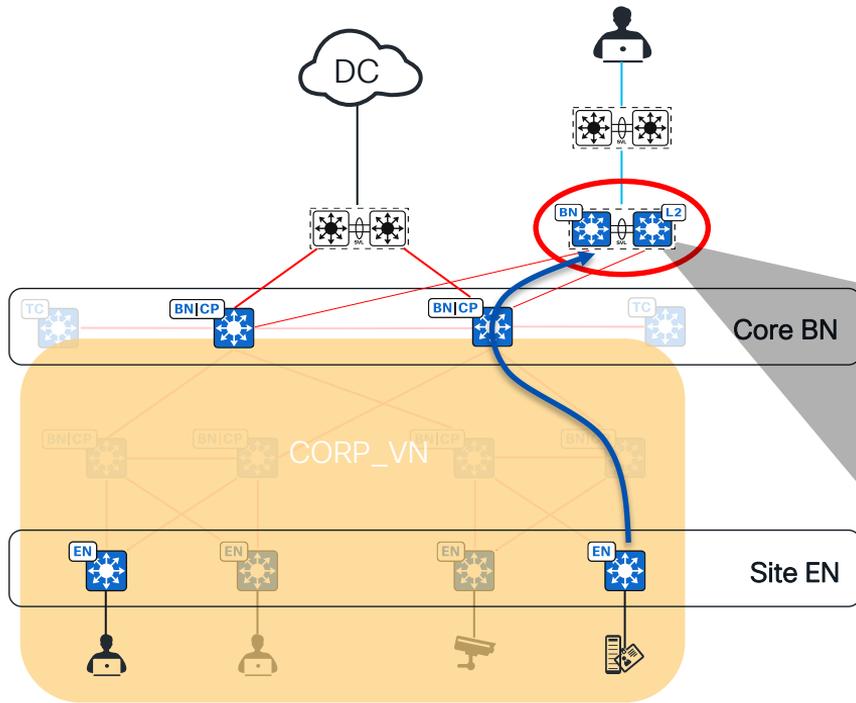


Border Nodes (L3 Handoff)

- 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

Source		Destination				
		Production_User	Production_Srvr	Development_User	Development_Srvr	Unknown
Production_User						
Production_Srvr						
Development_User						
Development_Srvr						
Unknown						

Default_Policy:

Deny-List

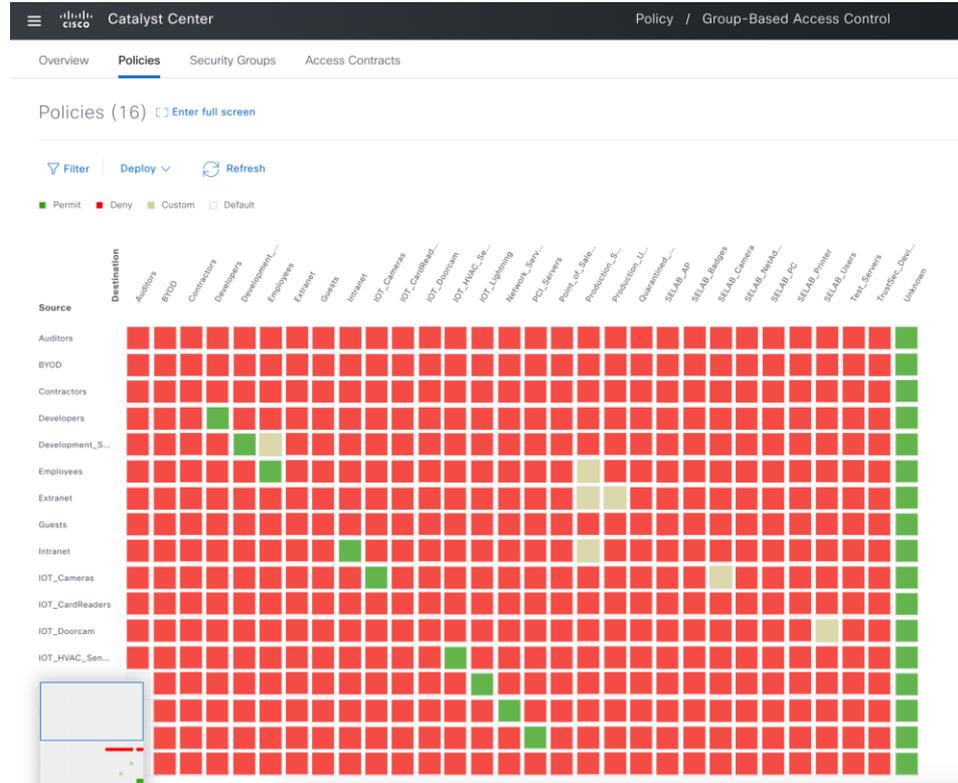
Source		Destination				
		Production_User	Production_Srvr	Development_User	Development_Srvr	Unknown
Production_User						
Production_Srvr						
Development_User						
Development_Srvr						
Unknown						

Default_Policy:

Allow-List

Failed design

Seen this before ?



Logging



Logging

Turn logging on !

o Identity Services Engine will be read-only. You can review the policy migration

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

	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).

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:

Start	Duration	Flow Action	Subject IP Add...	Subject Port/Pr...
Ex. 06/09/	Ex. <=50min41	Ex. permitted	Ex. 10.10.10.1	Ex. 57100/UD
Mar 18, 2024 5:19:33 PM (19min 55s ago)	16min 5s	permitted	33.1.1.12 ...	60/TCP

Start	Duration	Flow Action	Subject IP Add...	Subject Port/Pr...
Ex. 06/09/	Ex. <=50min41	Ex. permitted	Ex. 10.10.10.1	Ex. 57100/UD
Mar 18, 2024 5:19:33 PM (25min 36s ago)	22min 3s	denied	33.1.1.39 ...	60/TCP

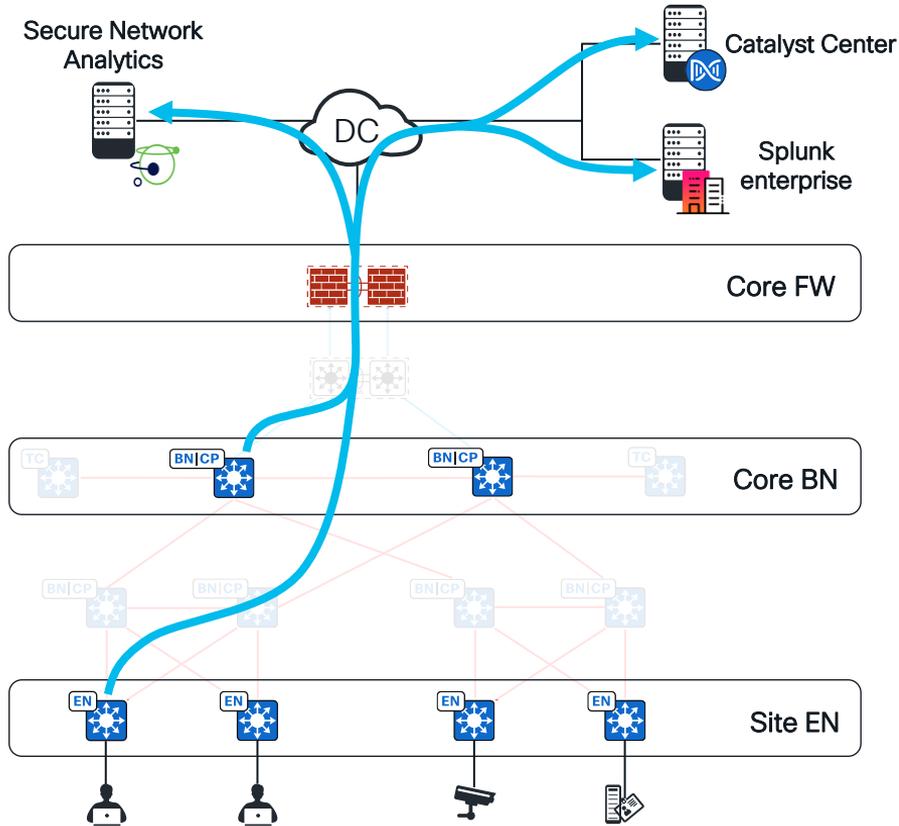
show flow monitor <monitor name> cache:
fw event: 1 (PERMIT) / 3 (DENY)

Agenda

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

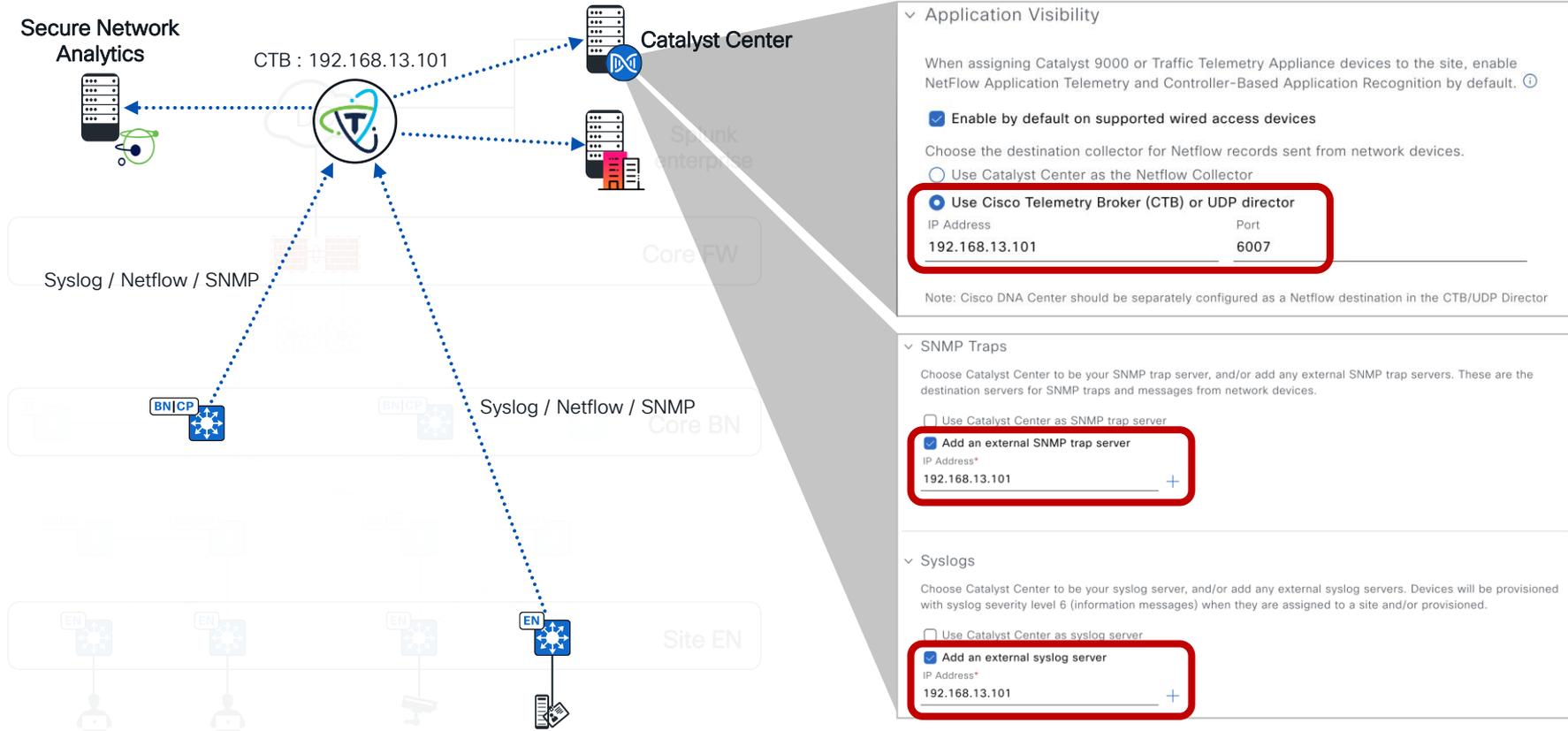
Telemetry Broker

Telemetry Challenge



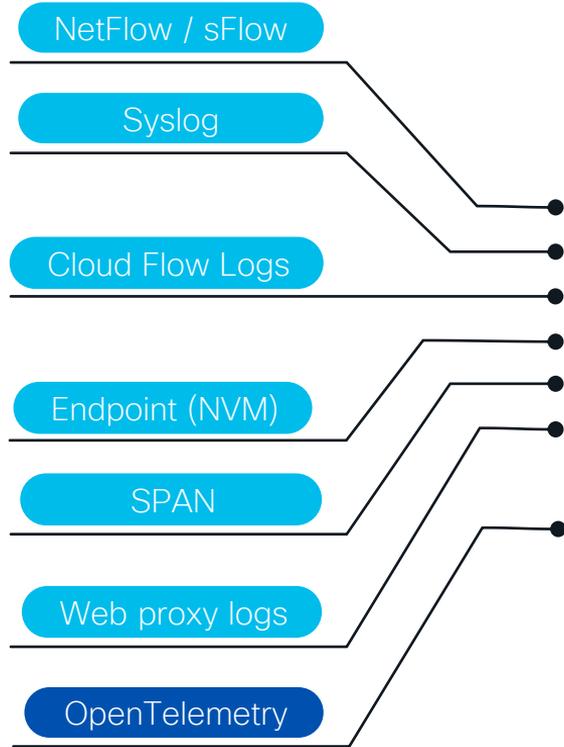
- TrustSec syslog sent to Splunk for analytics.
- System syslog sent to Catalyst Center for Assurance.
- Netflow sent to Catalyst Center, Splunk and SNA.
- Catalyst 9000 Series switches can only send netflow to two destinations
- Advanced telemetry such as AVC and ETA require compute resources

Telemetry Solution

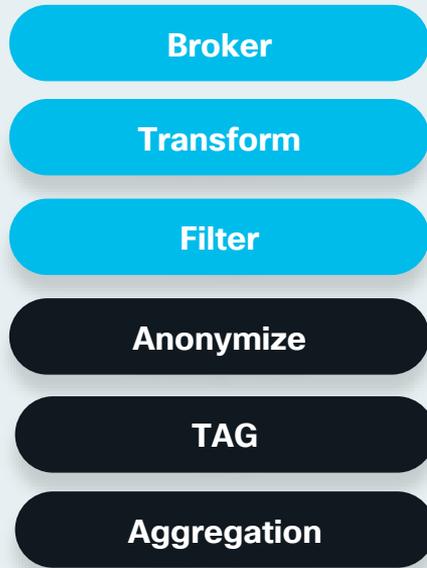


Cisco Telemetry Broker

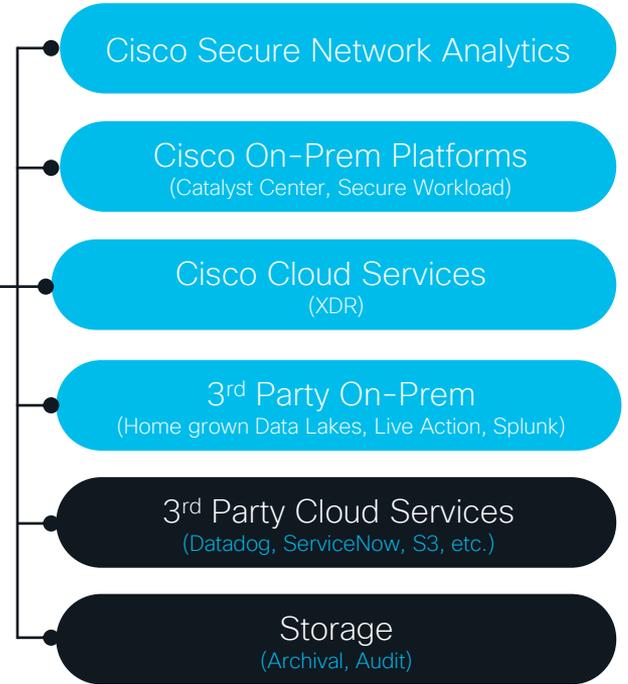
Telemetry Sources



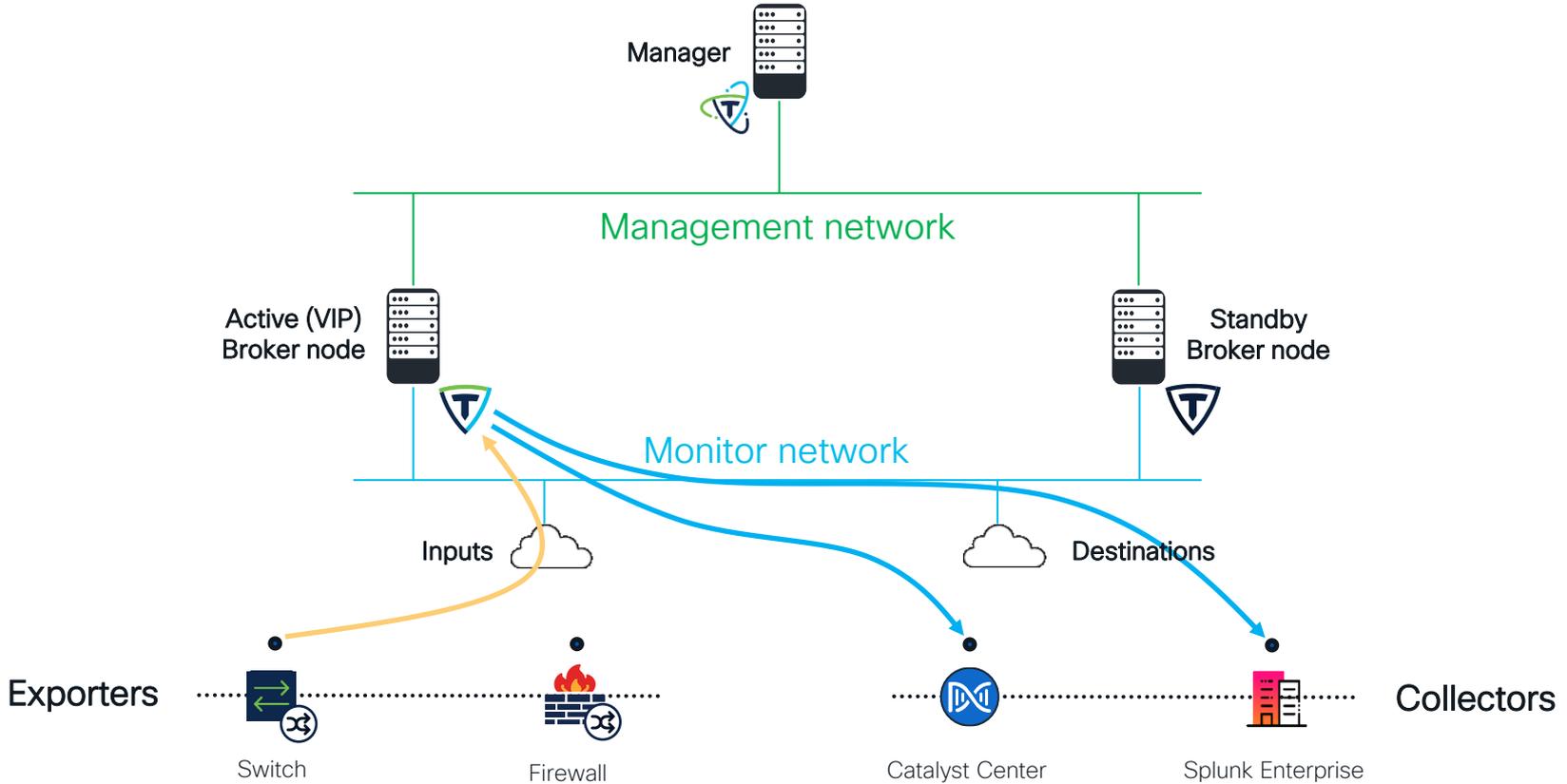
CTB Distributed Nodes



Telemetry Destinations



Cisco Telemetry Broker



- Project
- API Access
- Compute
- Volumes
- Network

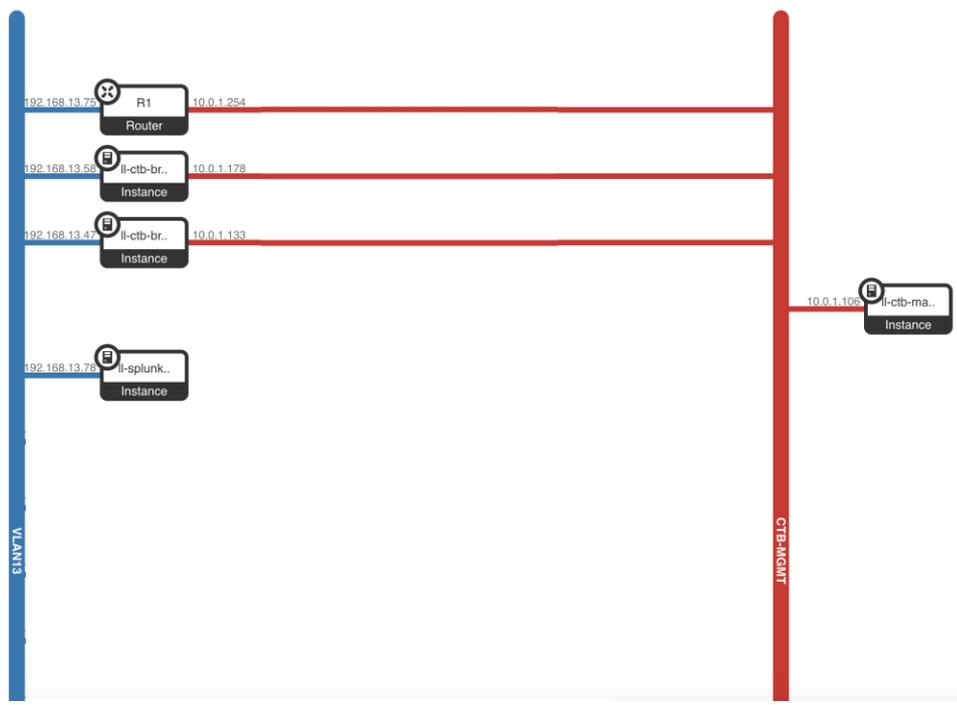
Project / Network / Network Topology

Network Topology

[Launch Instance](#)
[+ Create Network](#)
[+ Create Router](#)

Topology **Graph**
 Small Normal

- Network Topology
- Networks
- Routers
- Security Groups
- Floating IPs
- Object Store
- Admin
- Identity



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

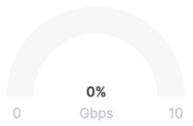
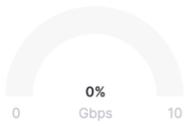


Broker Nodes

HA Cluster: selab

ll-ctb-broker-01

ll-ctb-broker-02



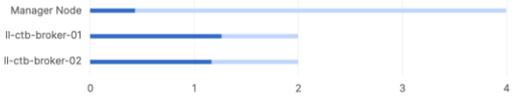
Alerts

All **Unresolved (0)**

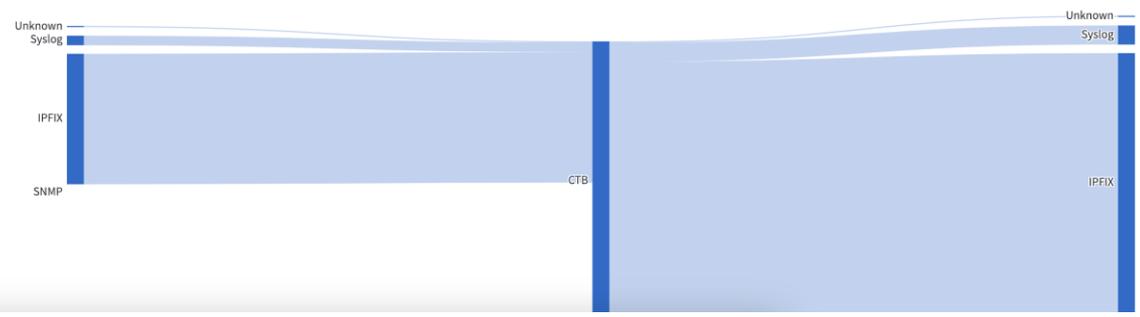
Most Recent on Top

There are no unresolved alerts. To check the alerts configuration see [Notification Settings](#).

CPU



Telemetry Flows



Licensing



Dashboard

Explorer

Settings

Explorer

- Manager Node
 - selab
 - ll-ctb-broker-02
 - ll-ctb-broker-01

← Manager Node

Broker Nodes 2 Clusters 1 Manager Node Details

Search

Broker Node	Alerts	Admin Interface	Telemetry Interface	Capacity	Cluster	Inputs	Received Rate	Sent Rate	S
ll-ctb-broker-01	—	IPv4 10.0.1.133 IPv6 —	IPv4 192.168.13.47 IPv6 —	10 Gbps	selab	0	44.5 kbps 0.01% of 10 Gbps	87.5 kbps 0.01% of 10 Gbps	
ll-ctb-broker-02	—	IPv4 10.0.1.178 IPv6 —	IPv4 192.168.13.58 IPv6 —	10 Gbps	selab	0	0 00.00% of 10 Gbps	0 00.00% of 10 Gbps	

Explorer

- Dashboard
- Explorer
- Settings

Manager Node > selab

Data Flow Inputs 3 Destinations 5 Cluster Details

Manager Node

- selab
 - ||-ctb-broker-02
 - ||-ctb-broker-01



Explorer

Manager Node > selab

Data Flow Inputs 3 Destinations 5 Cluster Details

Inputs 3

+ Add Input

Search

Most Received Last 24h

Input Type	Size	Count
IPFIX	460 MB	2
Syslog	33.7 MB	2
SNMP-Traps	4.15 MB	1

Destinations

Search

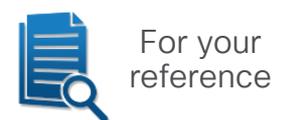
Destination	Count
Cat	1
Spl	1
Spl	1
Cat	1
Cat	1

Add Input

Select Input type

UDP Input

- AWS VPC Flow log
- Azure NSG Flow log
- Flow Generator Input
- Proxy log
- UDP Input



Cancel Next

Explorer

Manager Node > selab

Data Flow Inputs 3 Destinations 5 Cluster Details

Inputs 3

+ Add Input

Search Most Received Last 24h

Input Name	Size	Count
IPFIX	460 MB	2
Syslog	33.7 MB	2
SNMP-Traps	4.15 MB	1

Destinations

Search

Destination Name	Count
Cat	1
Spl	1
Spl	1
Cat	1
Cat	1

Add Input

UDP Input

UDP Input Name *

UDP Port *

Disable Exporters Tracking



For your reference

Cancel **Add Input**

- Dashboard
- Explorer
- Settings

Explorer

Manager Node > selab

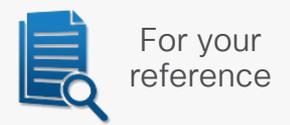
Data Flow Inputs 4 Destinations 5 Cluster Details

Manager Node

- selab
 - ll-ctb-broker-02
 - ll-ctb-broker-01



+ Add Destination



Explorer

Dashboard | Explorer | Settings

Manager Node > selab

Data Flow | Inputs 4 | Destinations 5 | Cluster Details

Manager Node

- selab
 - ll-ctb-broker-02
 - ll-ctb-broker-01

Inputs 4

+ Add Input

Search [] Most Recently Added [v]

- Netflow 0 GB [!]
- SNMP-Traps 4.15 MB [1]
- IPFIX 481 MB [2]
- Syslog 33.8 MB [2]

Destinations

Search []

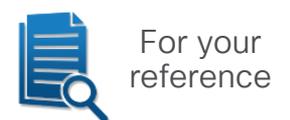
- Cat [1] [✓]
- Spl [1] [✓]
- Spl [1] [✓]
- Cat [1] [✓]
- Cat [1] [✓]

Add Destination

Select Destination type

Type or Select Destination [v]

- UDP Destination**
- SCA (XDR) Destination
- UDP Destination



Cancel [Next]

Explorer

Manager Node > selab

Data Flow Inputs 4 Destinations 6 Cluster Details

Inputs 4

+ Add Input

Search

Most Recently Added

Netflow 0 GB

SNMP-Traps 4.2 MB 1

IPFIX 467 MB 3

Syslog 34.2 MB 2

Destinations

Search

Add Destination

UDP Destination

Destination Name *

Destination IP Address *

Destination UDP Port *

Reachability check



For your reference

Cancel

Add Destination

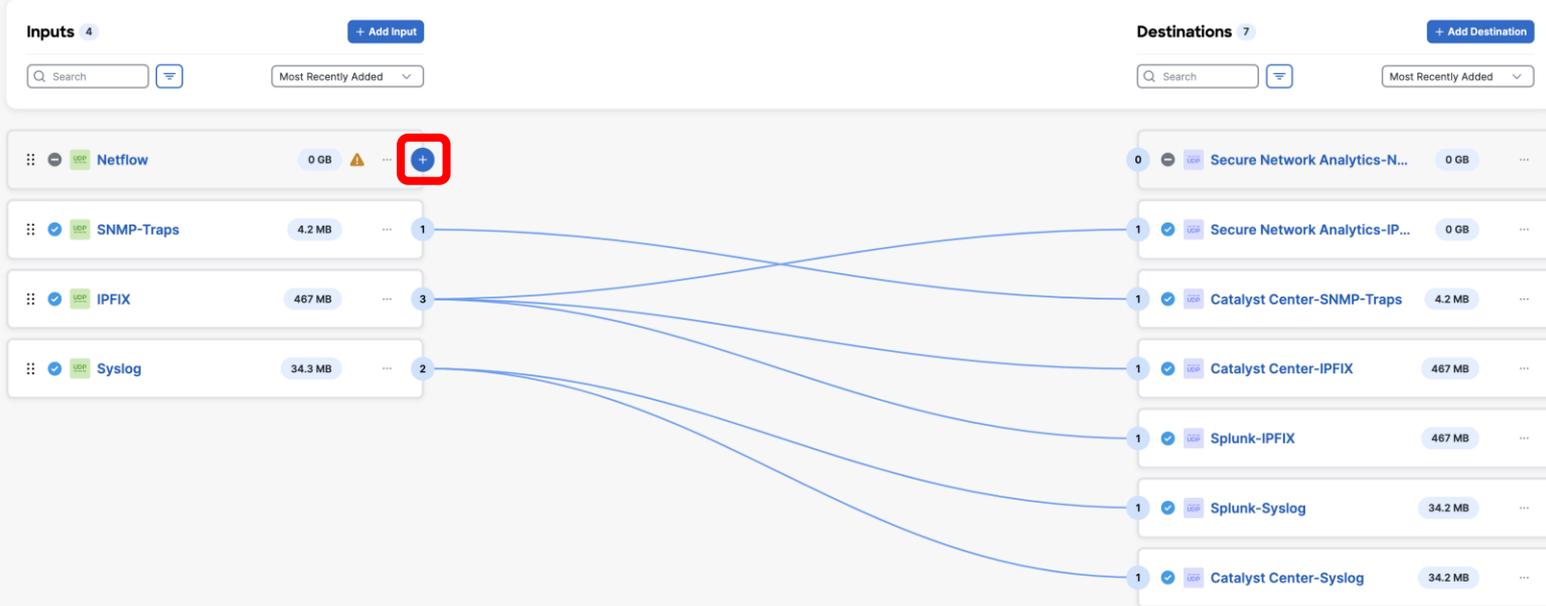
Explorer

Manager Node > selab

Data Flow Inputs 4 Destinations 7 Cluster Details

Manager Node

- selab
 - ll-ctb-broker-02
 - ll-ctb-broker-01



For your reference

Explorer

Manager Node > selab

Data Flow Inputs 4 Destinations 6 Cluster Details

Inputs 4

+ Add Input

Search

Most Recently Added

Netflow	0 GB	...	+
SNMP-Traps	4.17 MB	...	1
IPFIX	462 MB	...	2
Syslog	33.9 MB	...	2

Destinations

Search

Secure Network Analytics	0	...
Catalyst Center-SNMP-Traps	1	...
Catalyst Center-IPFIX	1	...
Splunk-IPFIX	1	...
Splunk-Syslog	1	...
Catalyst Center-Syslog	1	...

Connect to a Destination

Input
Netflow

Destination

- Secure Network Analytics
- Secure Network Analytics
- Catalyst Center-SNMP-Traps
- Catalyst Center-IPFIX
- Splunk-IPFIX
- Splunk-Syslog
- Catalyst Center-Syslog



For your reference

Cancel Save

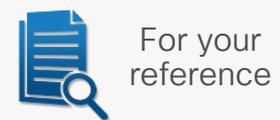
Explorer

Manager Node

- selab
 - ll-ctb-broker-02
 - ll-ctb-broker-01

Manager Node > selab

Data Flow Inputs 4 Destinations 7 Cluster Details

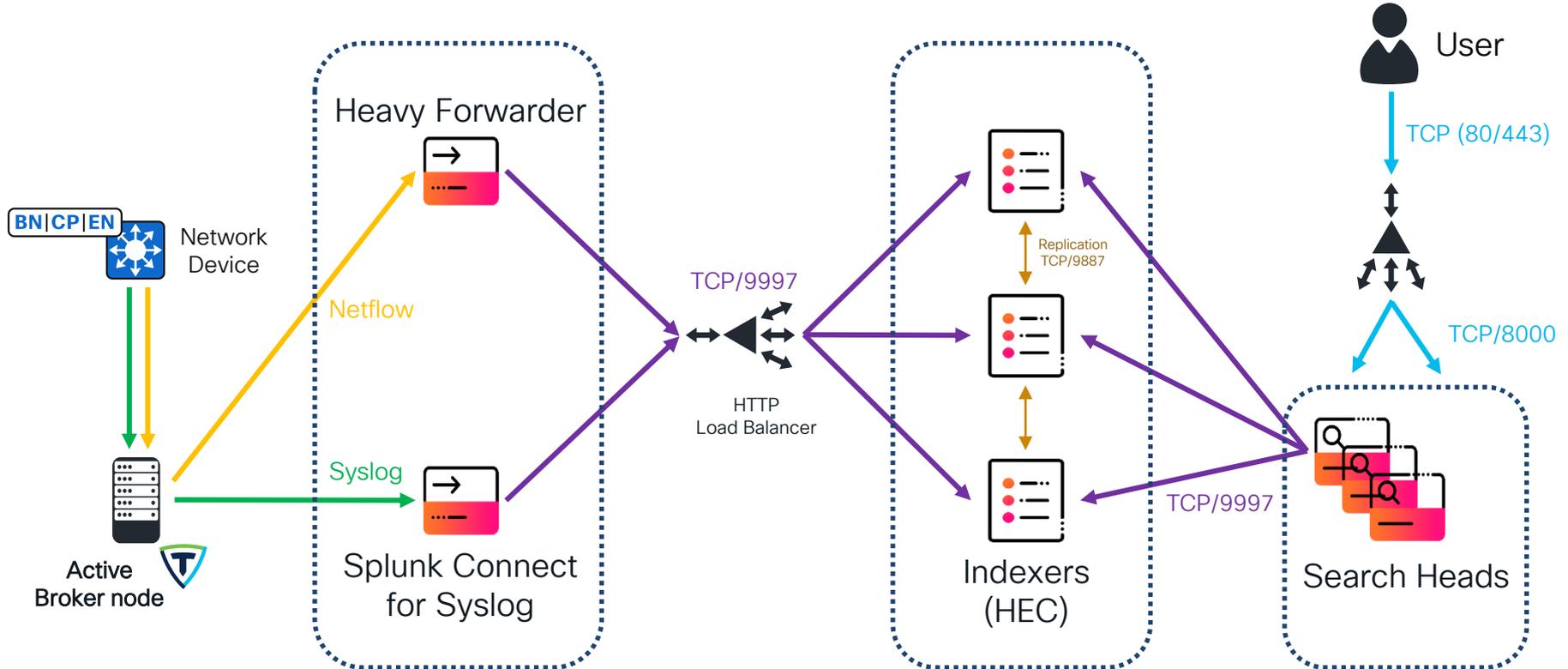


Splunk Enterprise

CISCO *Live!*



Splunk Enterprise Architecture



New Search

sourcetype="cisco:ios" Last 24 hours

271,889 events (12/13/24 3:00:00.000 PM to 12/14/24 3:41:33.000 PM) No Event Sampling

Events (271,889) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column



Raw Format 20 Per Page

Prev 1 2 3 4 5 6 7 8 ... Next

Hide Fields All Fields

SELECTED FIELDS
a host 9
a source 1
a sourcetype 1

INTERESTING FIELDS
a index 1
a linecount 1
a splunk_server 1

+ Extract New Fields

i	Event
>	Dec 14 15:41:32 10.0.255.134 385379: 385371: Dec 14 15:33:56.594: %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='10.16.1.12' dest-port='43903' sgt='2' dgt='18' logging_interval_hits='1'
>	Dec 14 15:41:32 10.0.255.134 385378: 385370: Dec 14 15:33:56.594: %SEC-6-IPACCESSLOGP: list Deny_IP_Log-00 denied tcp 10.16.1.254(80) -> 10.16.1.12(43903), 1 packet
>	Dec 14 15:41:32 10.0.255.134 385379: 385371: Dec 14 15:33:56.594: %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='10.16.1.12' dest-port='43903' sgt='2' dgt='18' logging_interval_hits='1'
>	Dec 14 15:41:32 10.0.255.134 385378: 385370: Dec 14 15:33:56.594: %SEC-6-IPACCESSLOGP: list Deny_IP_Log-00 denied tcp 10.16.1.254(80) -> 10.16.1.12(43903), 1 packet
>	Dec 14 15:41:31 10.0.255.134 385377: 385369: Dec 14 15:33:55.592: %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='10.16.1.12' dest-port='38065' sgt='2' dgt='18' logging_interval_hits='1'
>	Dec 14 15:41:31 10.0.255.134 385376: 385368: Dec 14 15:33:55.592: %SEC-6-IPACCESSLOGP: list Deny_IP_Log-00 denied tcp 10.16.1.254(80) -> 10.16.1.12(38065), 1 packet
>	Dec 14 15:41:31 10.0.255.134 385377: 385369: Dec 14 15:33:55.592: %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='10.16.1.12' dest-port='38065' sgt='2' dgt='18' logging_interval_hits='1'
>	Dec 14 15:41:31 10.0.255.134 385376: 385368: Dec 14 15:33:55.592: %SEC-6-IPACCESSLOGP: list Deny_IP_Log-00 denied tcp 10.16.1.254(80) -> 10.16.1.12(38065), 1 packet
>	Dec 14 15:41:30 10.0.255.134 385375: 385367: Dec 14 15:33:54.590: %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='10.16.1.12' dest-port='40631' sgt='2' dgt='18' logging_interval_hits='1'
>	Dec 14 15:41:30 10.0.255.134 385374: 385366: Dec 14 15:33:54.589: %SEC-6-IPACCESSLOGP: list Deny_IP_Log-00 denied tcp 10.16.1.254(80) -> 10.16.1.12(40631), 1 packet
>	Dec 14 15:41:30 10.0.255.134 385375: 385367: Dec 14 15:33:54.590: %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='10.16.1.12' dest-port='40631' sgt='2' dgt='18' logging_interval_hits='1'
>	Dec 14 15:41:30 10.0.255.134 385374: 385366: Dec 14 15:33:54.589: %SEC-6-IPACCESSLOGP: list Deny_IP_Log-00 denied tcp 10.16.1.254(80) -> 10.16.1.12(40631), 1 packet
>	Dec 14 15:41:23 10.0.255.133 2659: 002663: Dec 14 15:33:47.124: %SESSION_MGR-5-FAIL: Switch 1 R0/0: sessmgrd: Authorization failed or unapplied for client (00a2.ee8a.420e) on Interface GigabitEthernet1/0/48 AuditSessionID 4901000A0000000DC259724A. Failure reason: Authc fail. Authc failure reason: Cred Fail.
>	Dec 14 15:41:22 10.0.255.133 2658: 002662: Dec 14 15:33:47.124: %MAB-5-FAIL: Switch 1 R0/0: sessmgrd: Authentication failed for client (00a2.ee8a.420e) with reason (Cred Fail) on Interface Gi1/0/48 AuditSessionID 4901000A0000000DC259724A
>	Dec 14 15:41:22 10.0.255.133 2657: 002661: Dec 14 15:33:47.088: %DOT1X-5-FAIL: Switch 1 R0/0: sessmgrd: Authentication failed for client (00a2.ee8a.420e) with reason (No Response from Client) on Interface Gi1/0/48 AuditSessionID 4901000A0000000DC259724A



Extract Fields



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 v

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 >

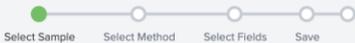
filter Apply Sample: 1,000 events v All events v

_raw

Dec 14 15:54:20 10.0.255.128 267780: 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 15:46:42.387: %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 15:46:42.387: %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 15:54:16 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



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 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='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



< Back **Next >**

Existing fields >

Select Method

Indicate the method you want to use to extract your field(s). [Learn more](#)
I prefer to write the regular expression myself >

Source type
cisco:ios

```
Dec 14 15:54:20 10.0.255.128 267700: Dec 14 15:46:44.252: %RBM-6-SGACLHIT: ingress_interface='TenGigabitEthernet1/0/39' sgac1_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'
```

(.*?)

Regular Expression

Splunk Enterprise will extract fields using a Regular Expression.

x|y|z

Delimiters

Splunk Enterprise will extract fields using a delimiter (such as commas, spaces, or characters). Use this method for delimited data like comma separated values (CSV files).

Extract Fields

Select Sample Select Method Select Fields Validate Save

< Back

Next >

Existing fields >

Select Fields

Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event for the regular expression to match. Click on highlighted values in the sample event to modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. [Learn more](#)

```
Dec 14 15:54:20 10.0.255.128 267700: Dec 14 15:46:44.252: %RBM-6-SGACLHIT: ingress_interface='TenGigabitEthernet1/0/39' gac1_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'
```

Extract Require

Field Name ingress_interface

Sample Value
TenGigabitEthernet1/0/39

Add Extraction

Extract Fields



< Back Next >

Existing fields >

Select Fields

Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event for the regular expression to match. Click on highlighted values in the sample event to modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. [Learn more](#)

```
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'
```

Hide Regular Expression

View in Search

^(?!\n)"(?<ingress_interface>\w+/\d+/\d+)

Edit the Regular Expression

Preview

If you see incorrect results below, click an additional event to add it to the set of sample events. Highlight its values to improve the extraction. You can remove incorrect values in the next step.

Events ingress_interface

1,000 events (9/15/24 12:00:00.000 AM to 12/14/24 3:57:22.000 PM)

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

filter Apply Sample: 1,000 events All events All Events Matches Non-Matches

	_raw	ingress_interface
✓	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'	TenGigabitEthernet1/0/39
✗	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'	



Extract Fields Existing fields >

Use the event listing below to validate the field extractions produced by your regular expression.

Regular Expression Regular Expression Reference View in Search

```
ingress_interface=(?<ingress_interface>{^}) sgACL_name=(?<sgACL_name>{^}) action=(?<action>{^}) protocol=(?<protocol>{^}) src_vrf=(?<src_vrf>{^}) src_ip=(?<src_ip>{^}) src_port=(?<src_port>{^}) dest_vrf=(?<dest_vrf>{^}) dest_ip=(?<dest_ip>{^}) dest_port=(?<dest_port>{^}) sgt=(?<sgt>{^}) dgt=(?<dgt>{^}) logging_interval_hits=(?<logging_interval_hits>{^})
```

Preview Save

Events ingress_interface sgACL_name action protocol src_vrf src_ip src_port dest_vrf dest_ip dest_port sgt dgt logging_interval_hits

1,000 events (9/15/24 12:00:00.000 AM to 12/14/24 4:01:55.000 PM) 20 per page < Prev 1 2 3 4 5 6 7 8 ... Next >

filter Apply Sample: 1,000 events All events All Events Matches Non-Matches

	_raw	ingress_interface	sgACL_name	action	protocol	src_vrf	src_ip	src_port	dest_vrf	dest_ip	dest_port	sgt	dgt	logging_interval_hits
✓	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'	TenGigabitEthernet1/0/39	Deny_IP_Log-00	Monitor	icmp	default	10.0.254.18	5	unknown	10.0.254.17	1	0	2	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'	Control Plane	Deny_IP_Log-00	Deny	tcp	CORP_VN	10.16.1.254	80	CORP_VN	10.16.1.15	59397	2	4	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'	Control Plane	Deny_IP_Log-00	Deny	tcp	CORP_VN	10.16.1.254	80	CORP_VN	10.16.1.15	59397	2	4	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'	Control Plane	Deny_IP_Log-00	Deny	tcp	CORP_VN	10.16.1.254	80	CORP_VN	10.16.1.15	43703	2	4	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'	Control Plane	Deny_IP_Log-00	Deny	tcp	CORP_VN	10.16.1.254	80	CORP_VN	10.16.1.15	43703	2	4	1



Save

Name the extraction and set permissions.

Extractions Name **EXTRACT-**

Owner **ubuntu**

App **search**

Permissions Owner App All apps

Source type **cisco:ios**

Fields **ingress_interface,sgaci_name,action,protocol,src_vrf,src_ip,src_port,dest_vrf,dest_ip,dest_port,sgt,dgt,logging_interval_hits**

Regular Expression **ingress_interface=(?<ingress_interface>{^})' sgaci_name=(?<sgaci_name>{^})' action=(?<action>{^})' protocol=(?<protocol>{^})' src_vrf=(?<src_vrf>{^})' src_ip=(?<src_ip>{^})' src_port=(?<src_port>{^})' dest_vrf=(?<dest_vrf>{^})' dest_ip=(?<dest_ip>{^})' dest-port=(?<dest_port>{^})' sgt=(?<sgt>{^})' dgt=(?<dgt>{^})' logging_interval_hits=(?<logging_interval_hits>{^})'**

New Search

sourcetype=cisco:ios Last 24 hours

28,373 of 28,373 events matched No Event Sampling

Events (28,373) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

Fast Mode
Field discovery off for event searches. No event or field data for stats searches.

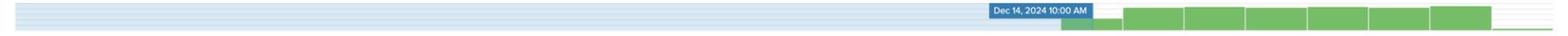
Smart Mode
Field discovery on for event searches. No event or field data for stats searches.

Verbose Mode
All event & field data.

Event
Dec 14 16:03:50 10.0.255.134 387681: 387673: Dec 14 15:56:13.958: %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='10.16.1.12' dest-port='42569' sgt='2' dgt='18' logging_interval_hits='1'
Dec 14 16:03:50 10.0.255.134 387681: 387673: Dec 14 15:56:13.958: %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='10.16.1.12' dest-port='42569' sgt='2' dgt='18' logging_interval_hits='1'
Dec 14 16:03:49 10.0.255.134 387680: 387672: Dec 14 15:56:12.927: %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='10.16.1.12' dest-port='48685' sgt='2' dgt='18' logging_interval_hits='1'
Dec 14 16:03:49 10.0.255.134 387680: 387672: Dec 14 15:56:12.927: %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='10.16.1.12' dest-port='48685' sgt='2' dgt='18' logging_interval_hits='1'
Dec 14 16:03:48 10.0.255.134 387679: 387671: Dec 14 15:56:11.902: %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='10.16.1.12' dest-port='44563' sgt='2' dgt='18' logging_interval_hits='1'
Dec 14 16:03:48 10.0.255.134 387679: 387671: Dec 14 15:56:11.902: %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='10.16.1.12' dest-port='44563' sgt='2' dgt='18' logging_interval_hits='1'
Dec 14 16:03:46 10.0.255.134 387678: 387670: Dec 14 15:56:10.881: %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='39251' sgt='2' dgt='4' logging_interval_hits='1'
Dec 14 16:03:46 10.0.255.134 387678: 387670: Dec 14 15:56:10.881: %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='39251' sgt='2' dgt='4' logging_interval_hits='1'
Dec 14 16:03:45 10.0.255.134 387677: 387669: Dec 14 15:56:10.879: %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='10.16.1.12' dest-port='38595' sgt='2' dgt='18' logging_interval_hits='1'
Dec 14 16:03:45 10.0.255.134 387676: 387668: Dec 14 15:56:10.878: %SEC-6-IPACCESSLOGP: list Deny_IP_Log-00 denied tcp 10.16.1.254(80) -> 10.16.1.12(38595), 1 packet
Dec 14 16:03:45 10.0.255.134 387677: 387669: Dec 14 15:56:10.879: %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='10.16.1.12' dest-port='38595' sgt='2' dgt='18' logging_interval_hits='1'
Dec 14 16:03:45 10.0.255.134 387676: 387668: Dec 14 15:56:10.878: %SEC-6-IPACCESSLOGP: list Deny_IP_Log-00 denied tcp 10.16.1.254(80) -> 10.16.1.12(38595), 1 packet
Dec 14 16:03:45 10.0.255.134 387675: 387667: Dec 14 15:56:09.881: %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='50645' sgt='2' dgt='4' logging_interval_hits='1'

- INTERESTING FIELDS
- a action 6
 - a app 1
 - # date_hour 4
 - # date_mday 1
 - # date_minute 60
 - # date_month 1
 - # date_second 60
 - # date_wday 1
 - # date_year 1
 - # date_zone 1
 - a dest 20
 - a dest_ip 15
 - # dest_port 100+
 - a dest_vrf 3
 - a device_time 100+
 - # dgt 4
 - a dvc 8
 - # event_id 100+
 - a eventtype 7
 - a facility 13
 - a index 1
 - a ingress_interface 9
 - # linecount 1
 - # logging_interval_hits 100+
 - message_text 100+





SELECTED FIELDS
a host 9
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 6
a app 1
date_hour 8
date_mday 1
date_minute 60
a date_month 1
date_second 60
a date_wday 1
date_year 1
a date_zone 1
a dest 21
a dest_ip 15
dest_port 100+
a dest_vrf 3
a device_time 100+
dgt 4
a dvc 9
event_id 100+
a eventtype 7
a facility 14
a index 1
a ingress_interface 9
linecount 1
logging_interval_hits 100+
a message_text 100+

Dec 14 16:03:50 10.0.255.134 387681: 387673: Dec 14 15:56:13.958: %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='10.16.1.12' dest-port='42569' sgt='2' dgt='18' logging_interval_hits='1'

mnemonic
15 Values, 100% of events
Reports
Top values Top values by time Rare values
Events with this field
Top 10 Values
SGACLHIT 58,140 65.323%
IPACCESSLOGP 26,993 30.328%
IPACCESSLOGRL 1,088 1.222%
IPACCESSLOGDP 894 1.004%
FAIL 804 0.903%
LOGIN_SUCCESS 203 0.228%
SSH2_CLOSE 202 0.227%
SSH2_SESSION 202 0.227%
SSH2_USERAUTH 202 0.227%
AUTH_PASSED 120 0.135%

Dec 14 16:03:49 10.0.255.134 387680: 387672: Dec 14 15:56:12.927: %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='10.16.1.12' dest-port='48685' sgt='2' dgt='18' logging_interval_hits='1'
Dec 14 16:03:48 10.0.255.134 387679: 387671: Dec 14 15:56:11.902: %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='10.16.1.12' dest-port='44563' sgt='2' dgt='18' logging_interval_hits='1'
IT: 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='10.16.1.12' dest-port='42569' sgt='2' dgt='18' logging_interval_hits='1'
IT: 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='10.16.1.12' dest-port='48685' sgt='2' dgt='18' logging_interval_hits='1'
IT: 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='10.16.1.12' dest-port='44563' sgt='2' dgt='18' logging_interval_hits='1'
SSLOGP: list Deny_IP_Log-00 denied tcp 10.16.1.254(80) -> 10.16.1.12(38595), 1 packet
IT: 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='10.16.1.12' dest-port='42569' sgt='2' dgt='18' logging_interval_hits='1'
SSLOGP: list Deny_IP_Log-00 denied tcp 10.16.1.254(80) -> 10.16.1.12(38595), 1 packet
IT: 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='10.16.1.12' dest-port='48685' sgt='2' dgt='18' logging_interval_hits='1'
IT: 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='10.16.1.12' dest-port='44563' sgt='2' dgt='18' logging_interval_hits='1'
IT: 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='10.16.1.12' dest-port='42569' sgt='2' dgt='18' logging_interval_hits='1'





New Search

Save As ▾ Create Table View Close

sourcetype=cisco:ios memonics=SGACLHIT Last 24 hours ▾ 🔍

5,080 of 5,096 events matched No Event Sampling ▾ Job ▾ || ▣ ↶ ↷ ⌵ ⌶ Smart Mode ▾

Events (5,080) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect 1 hour per column

Dec 14, 2024 4:00 PM

Raw ▾ ✓ Format 20 Per Page ▾

< Prev 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields All Fields

Selected Fields: a host 5, a source 1, a sourcetype 1

Interesting Fields: a action 3, a app 1, # date_hour 2, # date_mday 1, # date_minute 36, a date_month 1, # date_second 59, a date_wday 1, # date_year 1, a date_zone 1, a dest 14, a dest_ip 14, # dest_port 100+, a dest_vrf 3, a device_time 100+, a dgt 4, a dvc 5, # event_id 100+, a eventtype 4, a facility 1, a index 1, a ingress_interface 9, # linecount 1, # logging_interval_hits 88, a message_text 100+

Time	Source	Destination	Action	Protocol	Interface	Log Type	Severity	Message
Dec 14 15:58:08.882	10.0.255.134	10.16.1.15	Deny	tcp	Control Plane	Deny_IP_Log-00'	Deny	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' N' dest-ip='10.16.1.15' dest-port='38437' sgt='2' dgt='4' logging_interval_hits='1'
Dec 14 16:05:43	10.0.255.134	10.16.1.12	Deny	tcp	Control Plane	Deny_IP_Log-00'	Deny	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' N' dest-ip='10.16.1.12' dest-port='40843' sgt='2' dgt='18' logging_interval_hits='1'
Dec 14 16:05:43	10.0.255.134	10.16.1.15	Deny	tcp	Control Plane	Deny_IP_Log-00'	Deny	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' N' dest-ip='10.16.1.15' dest-port='39749' sgt='2' dgt='4' logging_interval_hits='1'
Dec 14 16:05:43	10.0.255.134	10.16.1.12	Deny	tcp	Control Plane	Deny_IP_Log-00'	Deny	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' N' dest-ip='10.16.1.12' dest-port='40843' sgt='2' dgt='18' logging_interval_hits='1'
Dec 14 16:05:42	10.0.255.134	10.16.1.15	Deny	tcp	Control Plane	Deny_IP_Log-00'	Deny	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' N' dest-ip='10.16.1.15' dest-port='56565' sgt='2' dgt='4' logging_interval_hits='1'
Dec 14 16:05:41	10.0.255.134	10.16.1.12	Deny	tcp	Control Plane	Deny_IP_Log-00'	Deny	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' N' dest-ip='10.16.1.12' dest-port='58869' sgt='2' dgt='18' logging_interval_hits='1'
Dec 14 16:05:41	10.0.255.134	10.16.1.15	Deny	tcp	Control Plane	Deny_IP_Log-00'	Deny	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' N' dest-ip='10.16.1.15' dest-port='41771' sgt='2' dgt='4' logging_interval_hits='1'
Dec 14 15:58:05.823	10.0.255.134	10.16.1.12	Deny	tcp	Control Plane	Deny_IP_Log-00'	Deny	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' N' dest-ip='10.16.1.12' dest-port='58201' sgt='2' dgt='18' logging_interval_hits='1'





New Search

Save As ▾ Create Table View Close

sourcetype=cisco:ios mnemonic=SGACLHIT action=Monitor Last 24 hours 🔍

✓ 11,184 events (12/13/24 4:00:00.000 PM to 12/14/24 4:13:05.000 PM) No Event Sampling ▾ Job ▾ || ▢ ↶ ↷ ⏏ ⏴ ⏵ Smart Mode ▾

Events (11,184) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect 1 hour per column



Table ▾ Format 20 Per Page ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields All Fields

i	_time	host	protocol	ingress_interface	dest_vrf	src_ip	dest_ip	src_port	dest_port	sgt	dgt	action	sgacl_name
---	-------	------	----------	-------------------	----------	--------	---------	----------	-----------	-----	-----	--------	------------

>	12/14/24 4:13:04.000 PM	10.0.2.66	udp	TenGigabitEthernet1/1/4	unknown	192.168.13.95	10.0.2.65	46520	161	0	2	Monitor	Deny_IP_Log-00
>	12/14/24 4:13:04.000 PM	10.0.2.66	udp	TenGigabitEthernet1/1/4	unknown	192.168.13.95	10.0.2.65	34223	161	0	2	Monitor	Deny_IP_Log-00
>	12/14/24 4:13:04.000 PM	10.0.255.129	udp	TenGigabitEthernet1/0/39	unknown	192.168.13.95	10.0.255.129	46520	161	0	2	Monitor	Deny_IP_Log-00
>	12/14/24 4:12:59.000 PM	10.0.255.129	tcp	TenGigabitEthernet1/0/39	unknown	10.0.255.130	10.0.255.129	4342	30654	0	2	Monitor	Deny_IP_Log-00
>	12/14/24 4:12:59.000 PM	10.0.255.129	tcp	TenGigabitEthernet1/0/39	unknown	10.0.255.131	10.0.255.129	4342	44547	0	2	Monitor	Deny_IP_Log-00
>	12/14/24 4:12:56.000 PM	10.0.255.129	tcp	TenGigabitEthernet1/0/39	unknown	10.0.255.128	10.0.255.129	37809	4342	0	2	Monitor	Deny_IP_Log-00
>	12/14/24 4:12:56.000 PM	10.0.255.129	tcp	TenGigabitEthernet1/0/39	unknown	10.0.255.128	10.0.255.129	4342	14024	0	2	Monitor	Deny_IP_Log-00
>	12/14/24 4:12:35.000 PM	10.0.255.129	tcp	TenGigabitEthernet1/0/39	unknown	10.0.255.128	10.0.255.129	45666	639	0	2	Monitor	Deny_IP_Log-00
>	12/14/24 4:12:25.000 PM	10.0.255.128	tcp	TenGigabitEthernet1/0/39	unknown	10.0.255.129	10.0.255.128	17052	179	0	2	Monitor	Deny_IP_Log-00

SELECTED FIELDS
 a action 1
 a dest_ip 10
 # dest_port 100+
 a dest_vrf 3
 # dgt 2
 a host 5
 a ingress_interface 7
 a protocol 3
 a sgacl_name 1
 # sgt 2
 a src_ip 27
 # src_port 100+

INTERESTING FIELDS
 a app 1
 # date_hour 24
 # date_mday 2
 # date_minute 60
 a date_month 1
 # date_second 60
 a date_wday 2
 # date_year 1
 a date_zone 1
 a dest 10
 a device_time 100+
 a dvc 5
 # event_id 100+
 a eventtype 4
 a facility 1
 a index 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

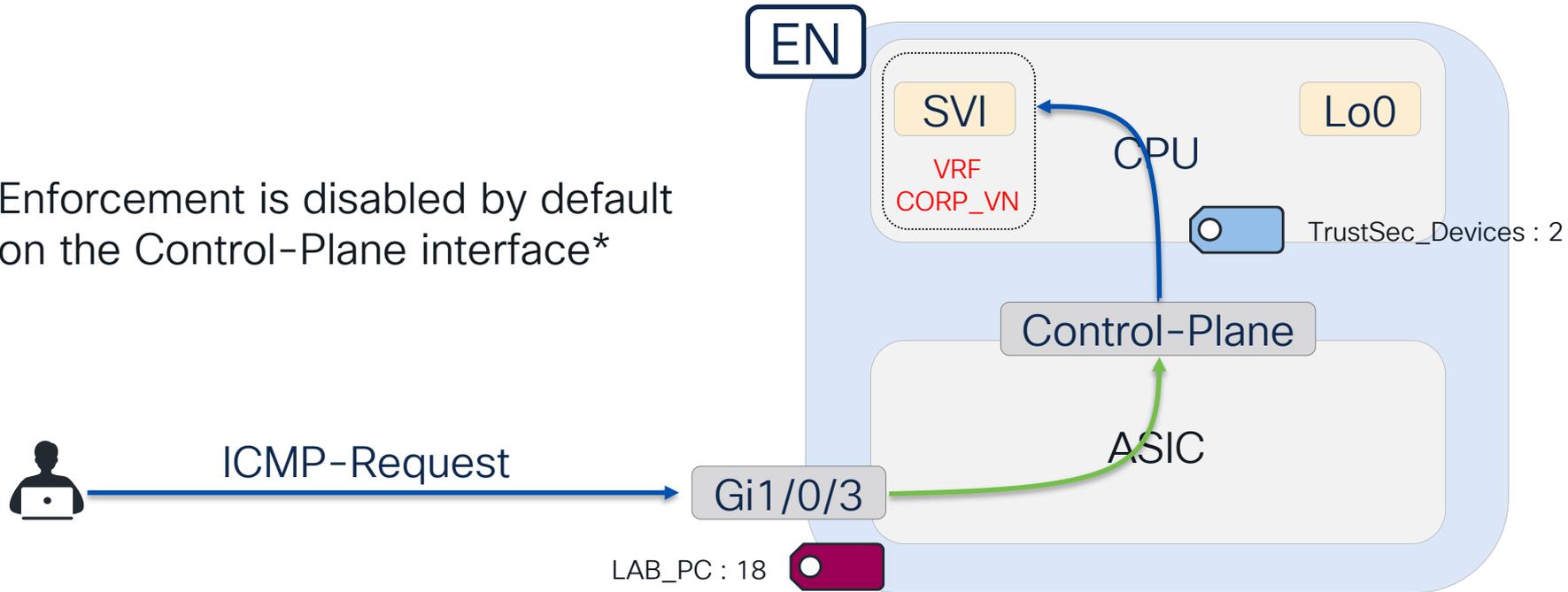
Traffic to Anycast Gateway

CISCO *Live!*



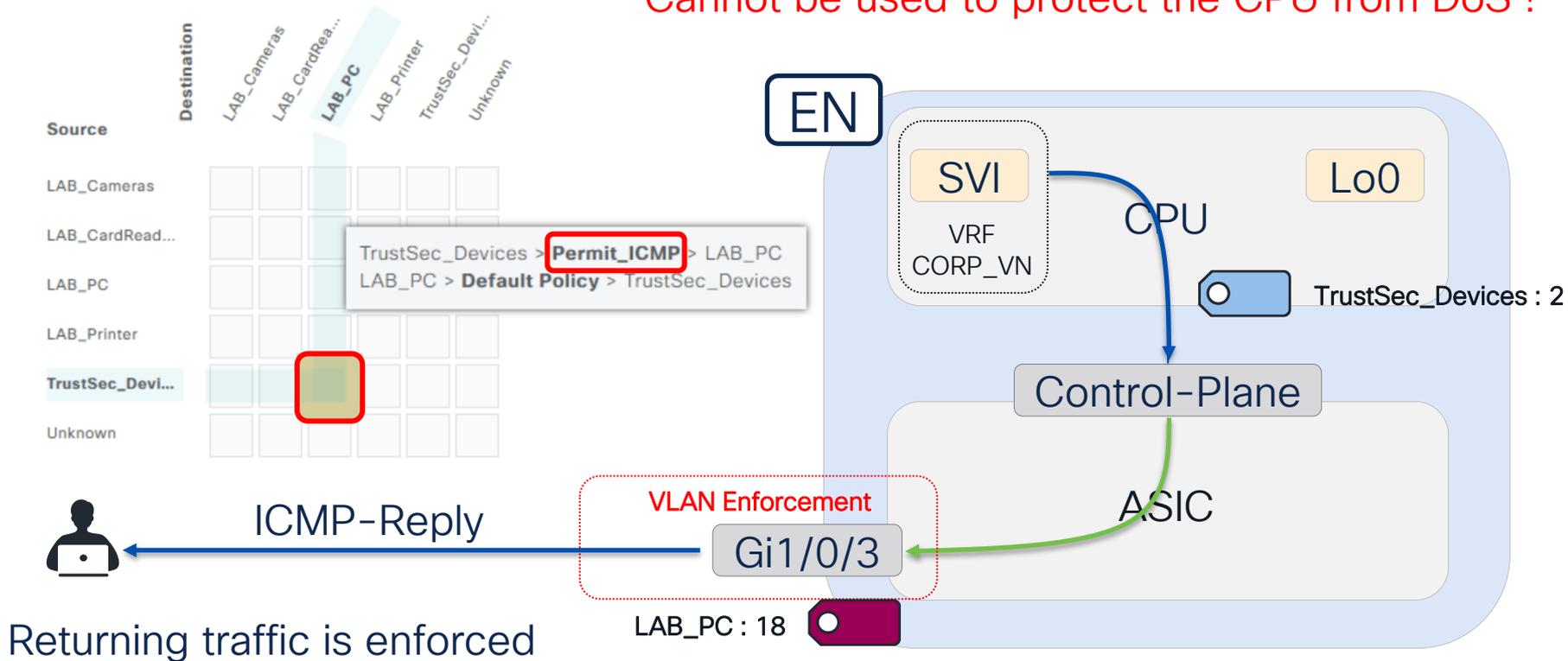
Traffic to Anycast Gateway

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

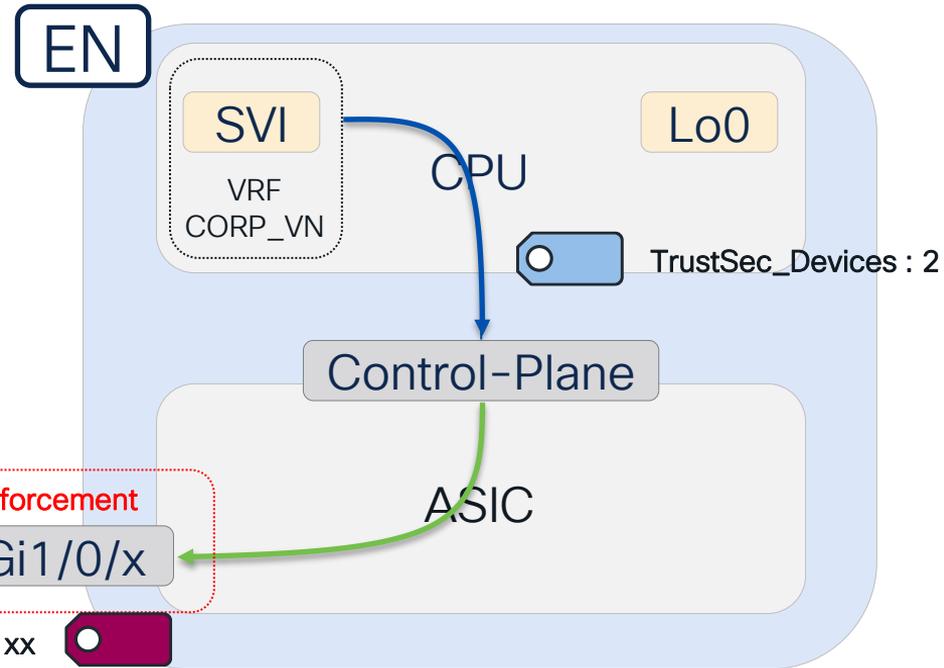
Traffic to Anycast Gateway

Repeat for other overlay SGTs

Source	Destination	LAB_Cameras	LAB_CardRead...	LAB_PC	LAB_Printer	TrustSec_Devi...	Unknown
LAB_Cameras							
LAB_CardRead...							
LAB_PC							
LAB_Printer							
TrustSec_Devic...							
Unknown							



ICMP-Reply

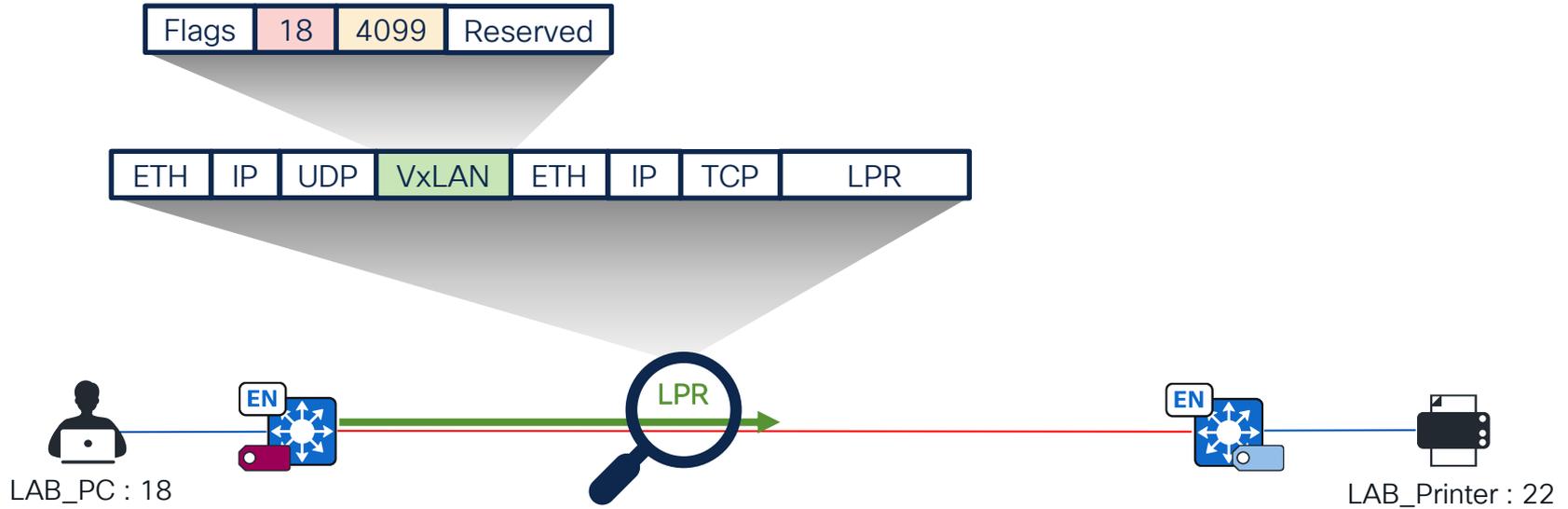


East-West Traffic

CISCO *Live!*



East-West Traffic



East-West Traffic

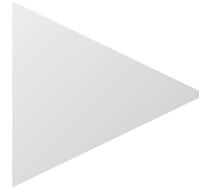
Access Contract

Name* Permit_LPR_ICMP Description

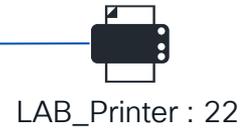
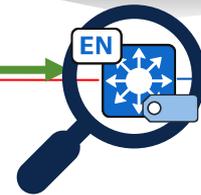
CONTRACT CONTENT (3)

#	Action	Application	Transport Protocol	Source / Destination	Port	Logging	Action
1	Permit	Advanced	TCP	Destination Source	515 ANY	<input type="checkbox"/>	+ X
2	Permit	Advanced	TCP	Destination Source	ANY 515	<input type="checkbox"/>	+ X
3	Permit	Advanced	ICMP	-	-	<input type="checkbox"/>	+ X

Default Action Deny Logging



Source	Destination	LAB_Cameras	LAB_CardRea...	LAB_PC	LAB_Printer	TrustSec_Devi...	Unknown
LAB_Cameras							
LAB_CardRead...							
LAB_PC							
LAB_Printer							
TrustSec_Devic...							
Unknown							



East-West Traffic

```
S1-Edge-2#sh cts role-based permissions from 18 to 22
IPv4 Role-based permissions from group 18:LAB_PC to group 22:LAB_Printer:
Permit_LPR_ICMP-02
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

```
S1-Edge-2#sh cts rbacl Permit_LPR_ICMP
CTS RBACL Policy
=====
RBACL IP Version Supported: IPv4 & IPv6
name = Permit_LPR_ICMP-02
IP protocol version = IPV4, IPV6
refcnt = 2
flag = 0xC1000000
stale = FALSE
RBACL ACEs:
permit tcp dst eq 515
permit tcp src eq 515
permit icmp
deny ip
```



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

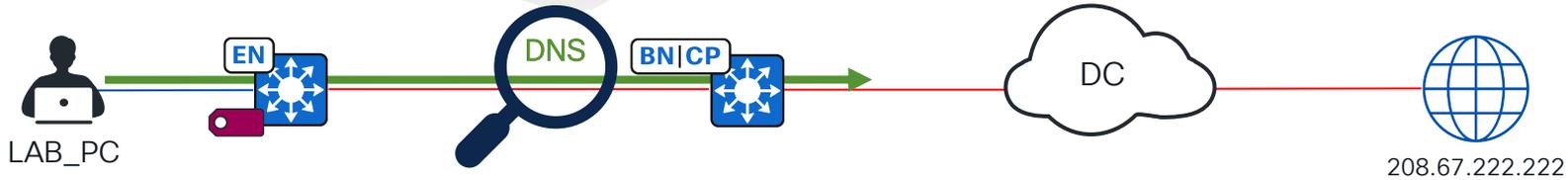
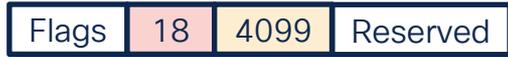
- Start by creating all obvious contracts
- Apply Permit_IP_Log where traffic needs monitoring
- Leave the rest to default

South->North Traffic with BN Enforcement



South->North Traffic w/ BN Enforcement

Traffic to Unknown should be allowed to cross the Border.



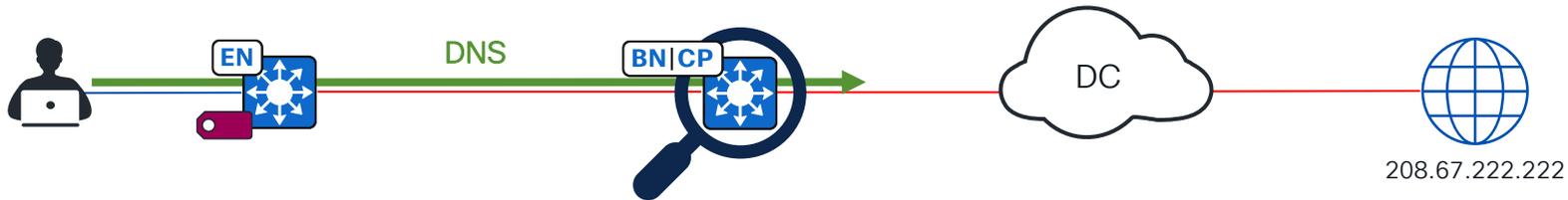
Source	LAB_Cameras	LAB_CardRead...	LAB_PC	LAB_Printer	TrustSec_Devi...	Unknown
LAB_Cameras						
LAB_CardRead...						
LAB_PC						
LAB_Printer						
TrustSec_Devic...						
Unknown						

Unclassified destination

South->North Traffic w/ BN Enforcement

Repeat for any SGTs that need to go out.

Source	Destination	LAB_Cameras	LAB_CardRead...	LAB_PC	LAB_Printer	TrustSec_Devi...	Unknown
LAB_Cameras							Green
LAB_CardRead...							Green
LAB_PC					Yellow		Green
LAB_Printer				Yellow			Green
TrustSec_Devices		Yellow	Yellow	Yellow	Yellow		
Unknown							

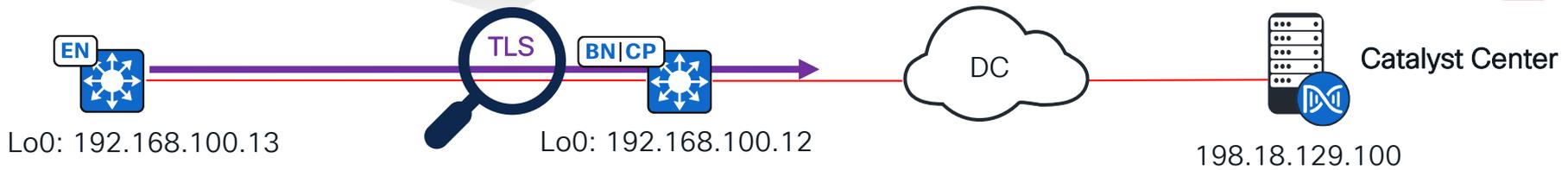


South->North Traffic w/ BN Enforcement

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

SRC: 192.168.100.13 DST:198.18.129.100

Permit from Unknown to Unknown = NOT Recommended



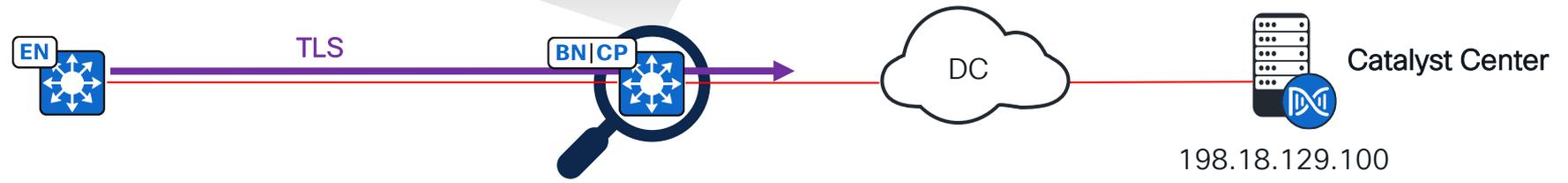
Source	Destination
LAB_AP	
LAB_CatC	
LAB_ISE	
LAB_WLC	
TrustSec_Devic...	
Unknown	

South->North Traffic w/ BN Enforcement

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

```
S1-Border-1#sh cts role-based sgt-map all | i SXP  
192.168.100.0/28      2      SXP
```

Source	LAB_AP	LAB_CatC	LAB_CTB	LAB_ISE	LAB_WLC	TrustSec_Devi...	Unknown
LAB_AP							
LAB_CatC							
LAB_CTB							
LAB_ISE							
LAB_WLC							
TrustSec_Devi...							
Unknown							



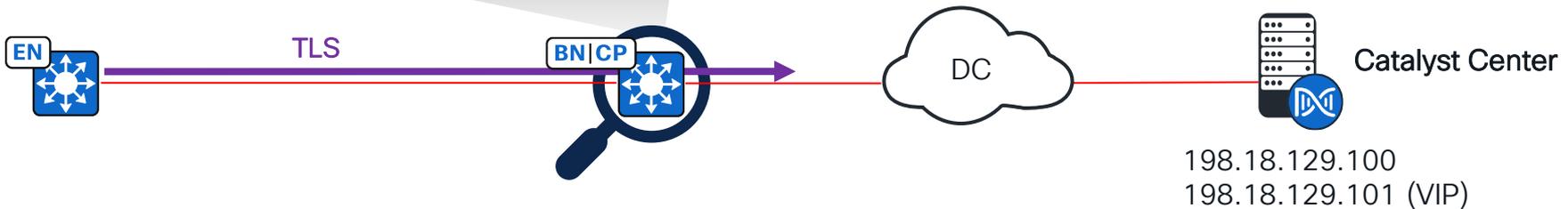
South->North Traffic w/ BN Enforcement

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
    
```

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



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.

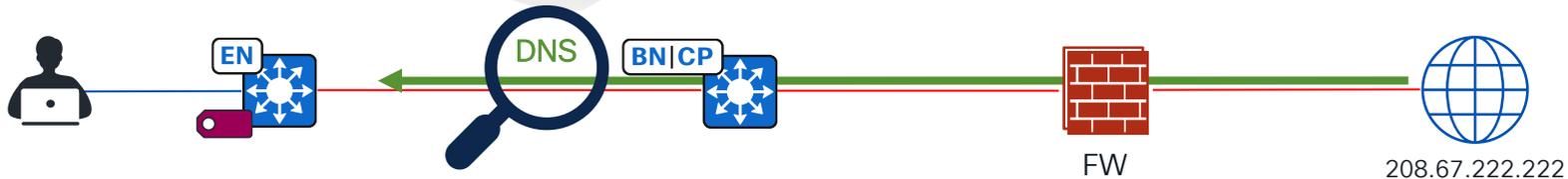
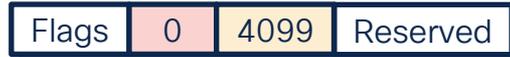
North->South Traffic

CISCO *Live!*



North->South Traffic

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

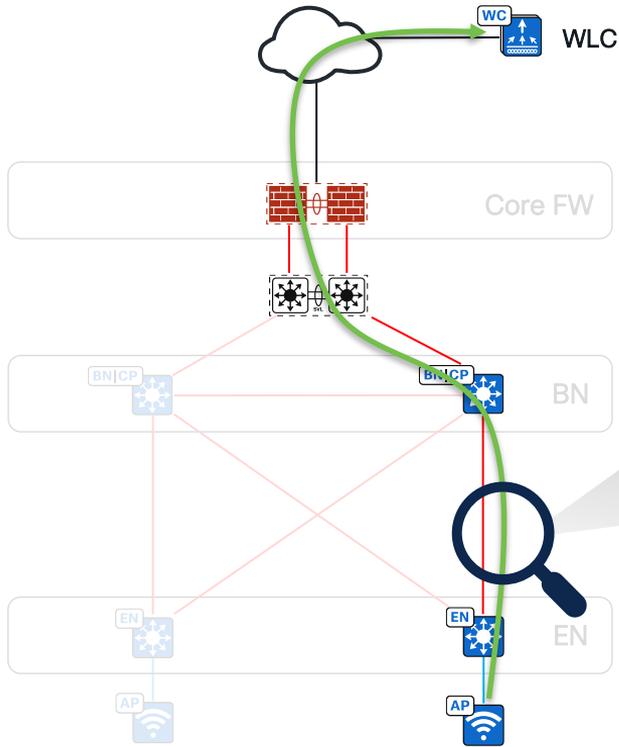


Source	Destination				
	LAB_Cameras	LAB_CardRead...	LAB_PC	LAB_Printer	TrustSec_Devi...
LAB_Cameras					Green
LAB_CardRead...					Green
LAB_PC			Yellow		Green
LAB_Printer			Yellow		Green
TrustSec_Devic...	Yellow	Yellow	Yellow	Yellow	
Unknown	Green	Green	Green	Green	

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

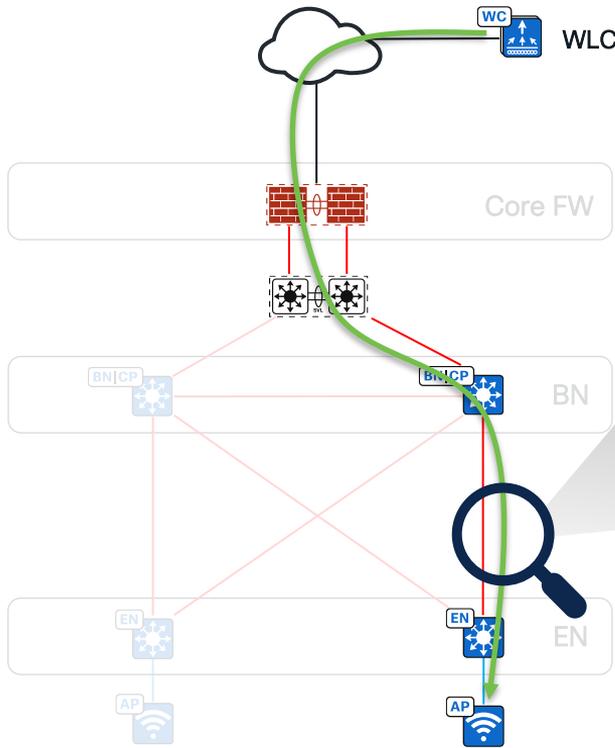
If Enforcement is enabled on INFRA_VN L3 Handoff:

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

Source	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 – WLC to AP



Capwap returning from WLC to Fabric AP is VxLAN encapsulated.



Any re-classification on BN will be propagated.

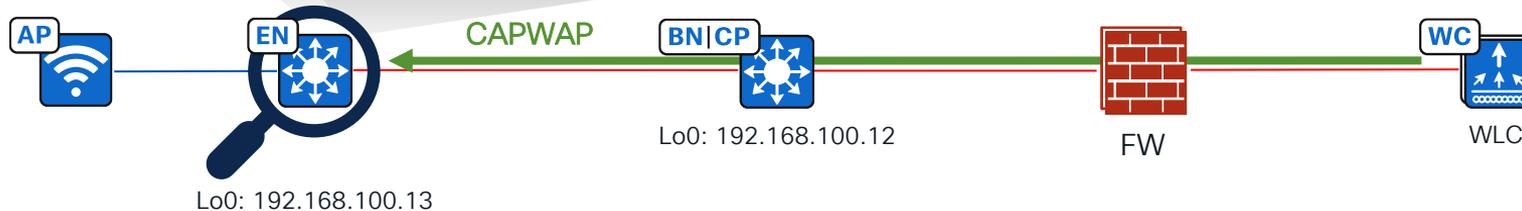
Fabric Enabled Wireless – WLC to AP

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	LAB_AP	LAB_CatC	LAB_CTB	LAB_ISE	LAB_WLC	TrustSec_Devi...	Unknown
LAB_AP							
LAB_CatC							
LAB_CTB							
LAB_ISE							
LAB_WLC							
TrustSec_Devi...							
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

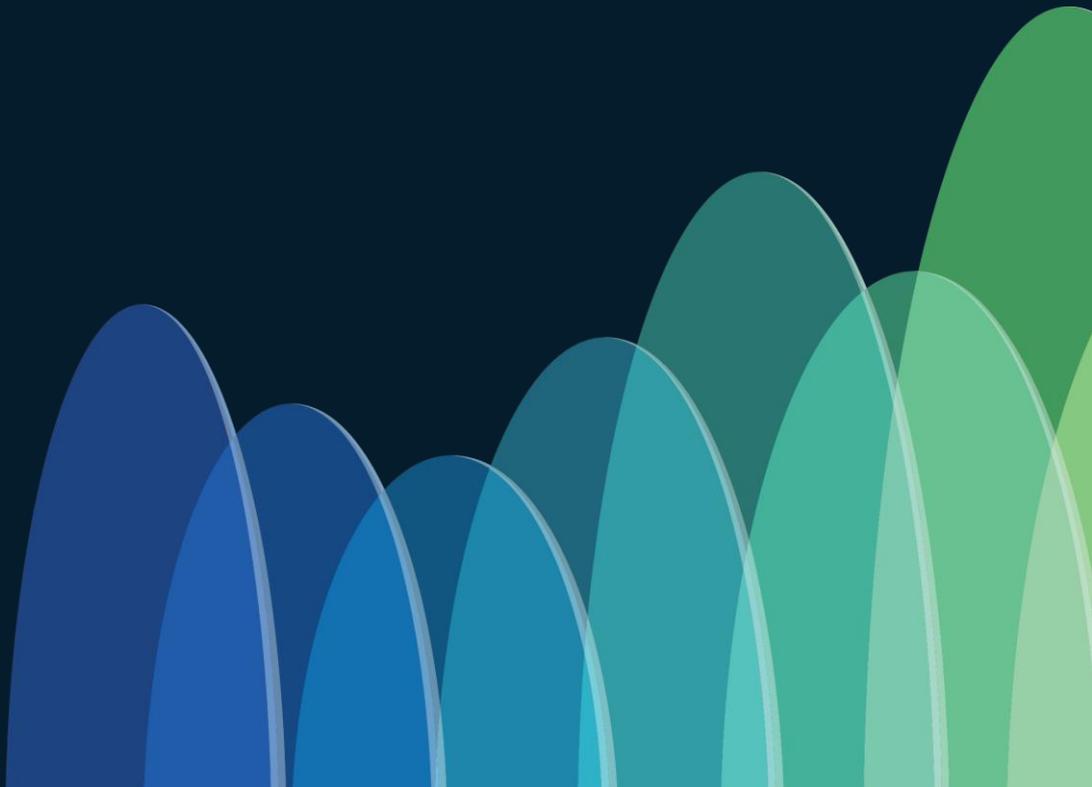


Excluded Traffic

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



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

Source	Auditors	BYOD	Contractors	Developers	Development_S...	Employees	Extranet	Guests	Intranet	IOT_Cameras	IOT_CardReaders	IOT_Doorcam	IOT_HVAC_Sen...	IOT_Lightning	Network_Servic...	PCI_Servers	Point_of_Sale_...	
Auditors																		
BYOD																		
Contractors																		
Developers																		
Development_S...																		
Employees																		
Extranet																		
Guests																		
Intranet																		
IOT_Cameras																		
IOT_CardReaders																		
IOT_Doorcam																		
IOT_HVAC_Sen...																		
IOT_Lightning																		
Network_Servic...																		
PCI_Servers																		
Point_of_Sale_...																		

Expand Minimap 



Policies (20) Enter full screen

Filter Deploy Refresh

Legend: Permit Deny Custom Default

Source	Auditors	BYOD	Contractors	Developers	Development_S...	Employees	Extranet	Guests	Intranet	IOT_Cameras	IOT_CardReaders	IOT_Doorcam	IOT_HVAC_Sen...	IOT_Lightning	Network_Servic...	PCI_Servers	Point_of_Sale_...
Auditors																	
BYOD																	
Contractors																	
Developers																	
Development_S...																	
Employees																	
Extranet																	
Guests																	
Intranet																	
IOT_Cameras																	
IOT_CardReaders																	
IOT_Doorcam																	
IOT_HVAC_Sen...																	
IOT_Lightning																	
Network_Servic...																	
PCI_Servers																	
Point_of_Sale_...																	

Upcoming In Progress Failed Default: F

Default Policy

Action

Deny_IP_Log

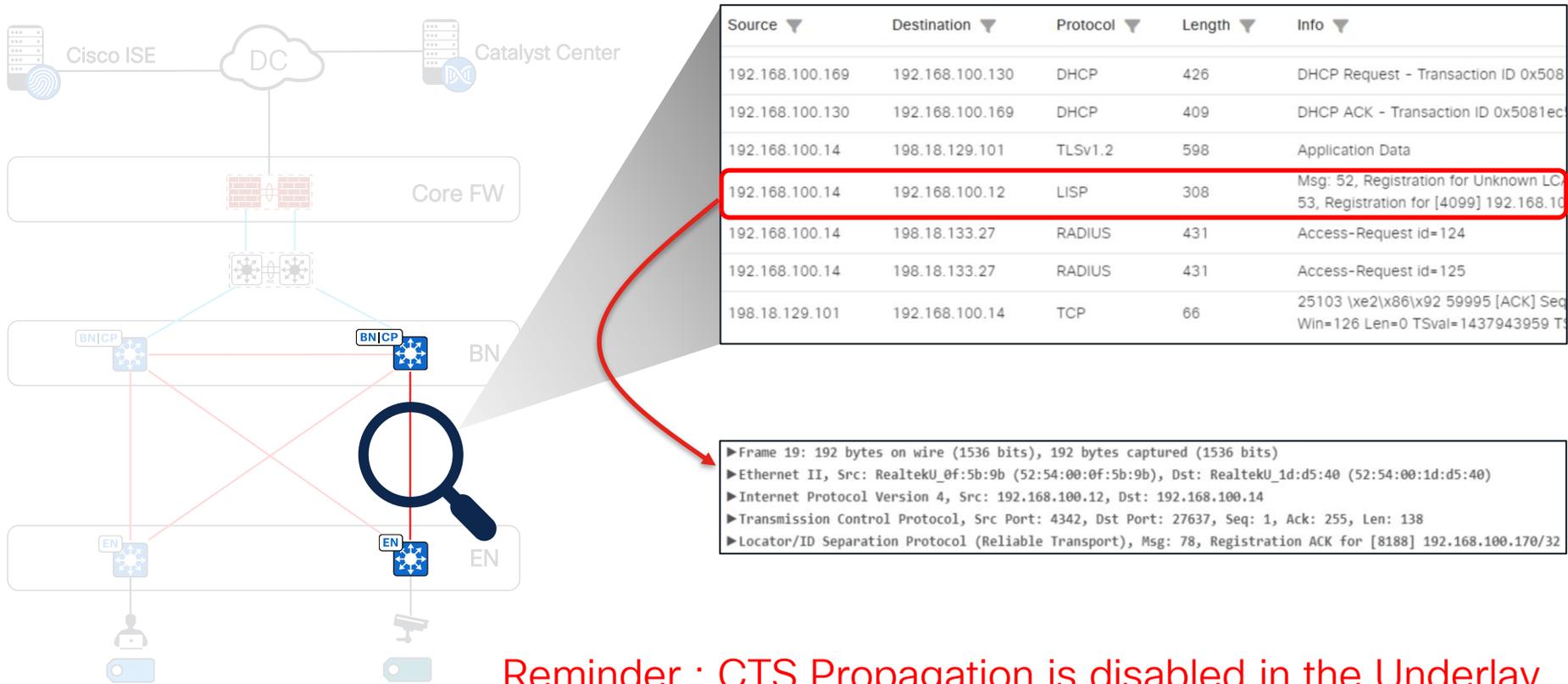
Once the allow-list model (default deny) is in place, all traffic in the network is blocked for all source-destination policies where there is no selected contract to explicitly permit traffic. That includes traffic from/to the network device, both management-plane (e.g., SSH, SNMP) and control-plane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

Cancel **Save Now** ⋮



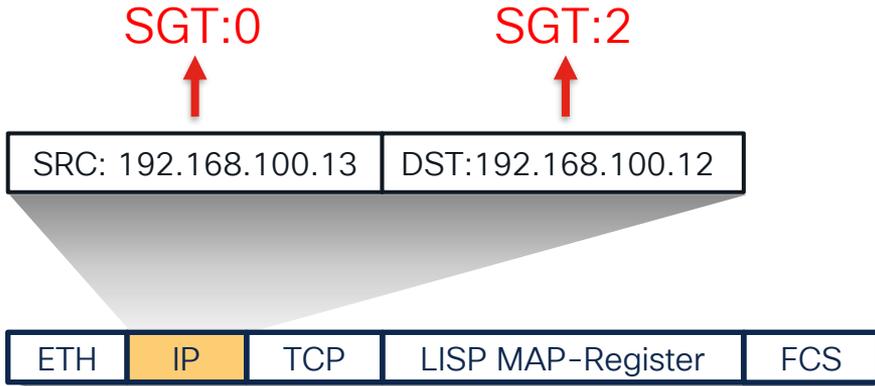
Forgot to disable
enforcement on
Fabric Links ?

Underlay – Enforcement on Fabric Links



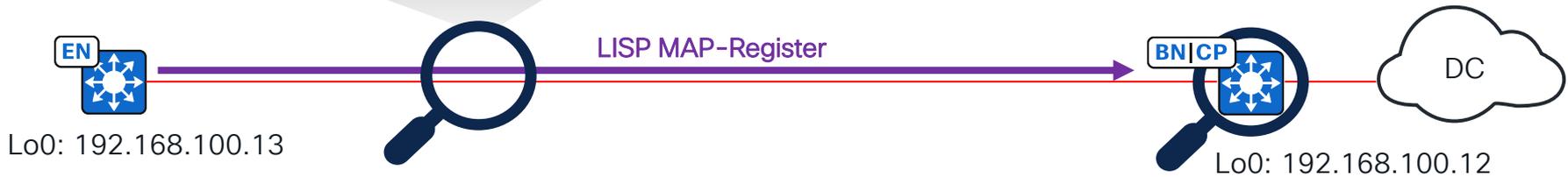
Reminder : CTS Propagation is disabled in the Underlay

Underlay – Enforcement on Fabric Links



Expectation:

There is no enforcement on ingress traffic, right ?



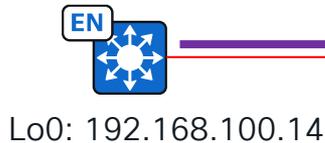
Underlay – Enforcement on Fabric Links

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

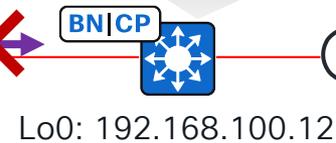
SRC: 192.168.100.14 DST:192.168.100.12



```
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
```



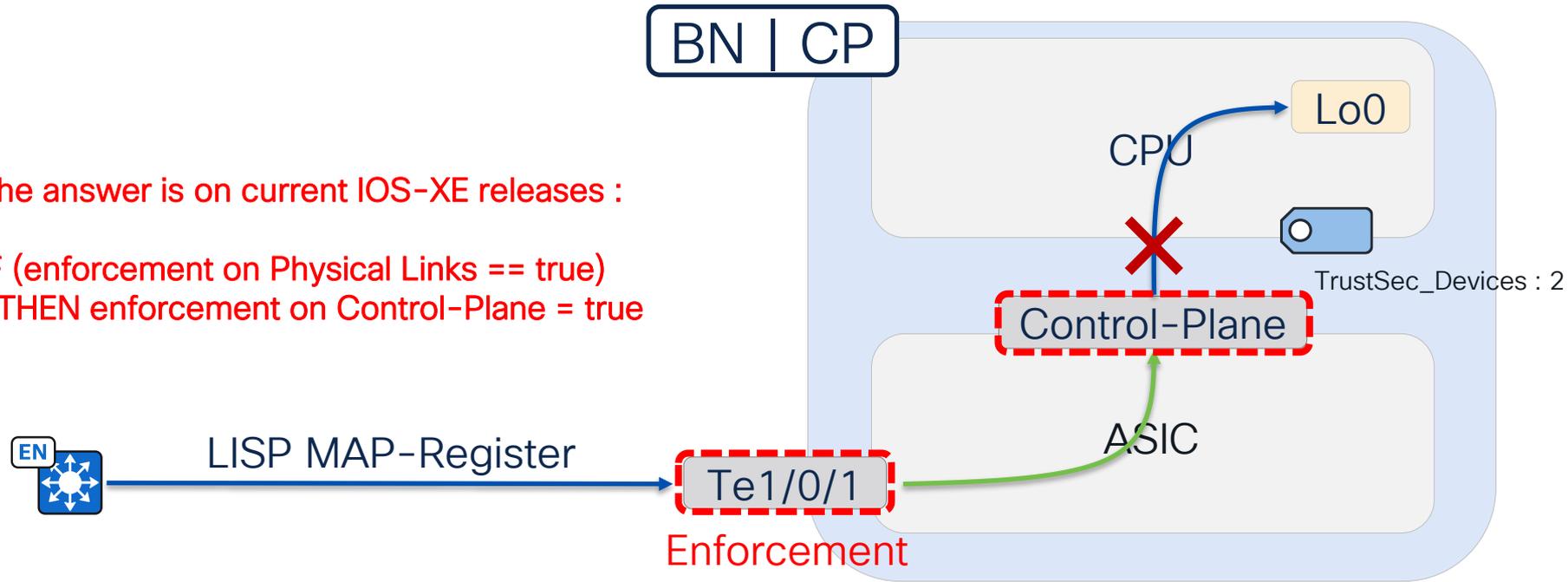
LISP MAP-Register



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



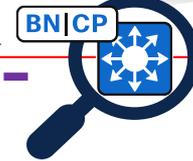
Underlay – Enforcement on Fabric Links

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

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_Devic...								
Unknown								



LISP MAP-Register



LISP MAP-Register ACK



Monitor & Adapt



New Search

Save As Create Table View Close

sourcetype=cisco:ios mnemonic=SGACLHI (src_port=53 OR dst_port=53) action=Deny Last 24 hours

8 events (12/13/24 5:00:00.000 PM to 12/14/24 5:18:25.000 PM) No Event Sampling Job Smart Mode

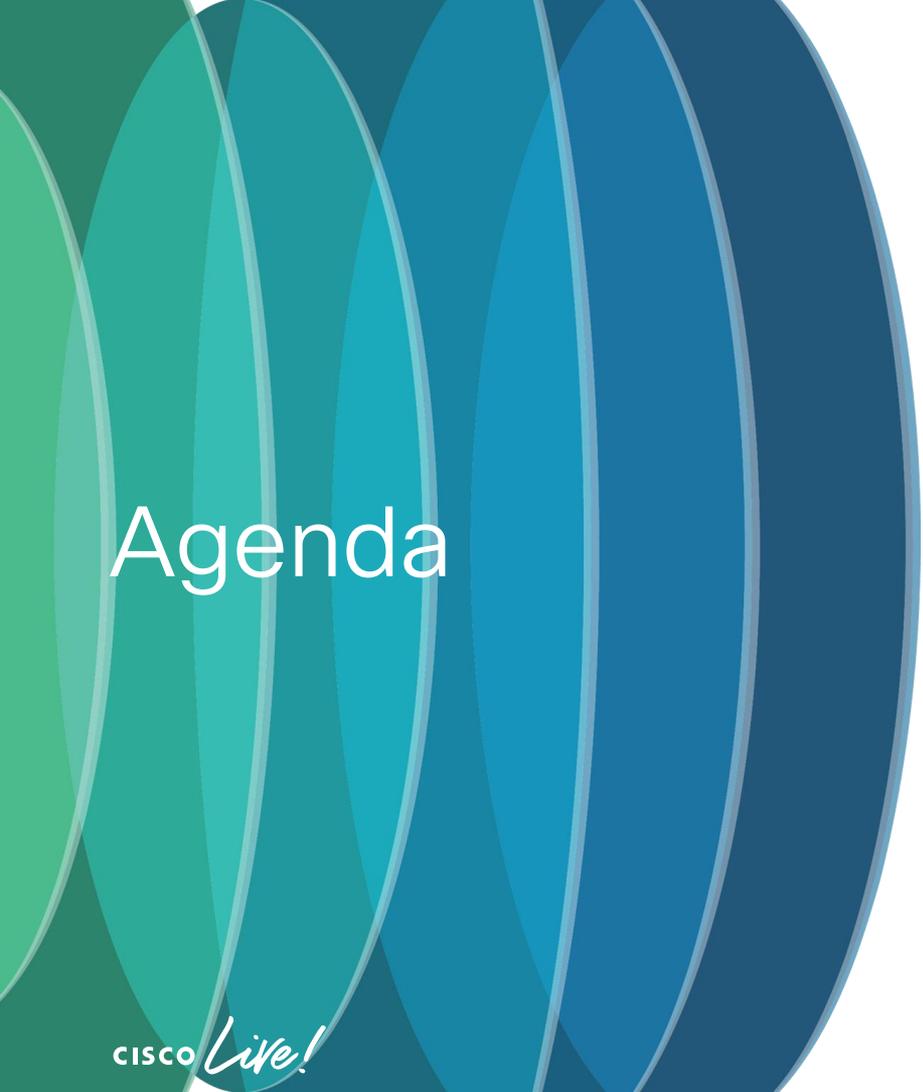
Events (8) Patterns Statistics Visualization



Show Fields Table Format 20 Per Page

i	_time	host	protocol	ingress_interface	dest_vrf	src_ip	dest_ip	src_port	dest_port	sgt	dgt	action	sgacl_name
>	12/14/24 4:09:02.000 PM	10.0.255.132	udp	TenGigabitEthernet1/17	CORP_VN	192.168.13.42	10.16.1.16	53	48879	33152	18	Deny	Deny_IP_Log-00
>	12/14/24 5:25:05.000 AM	10.0.255.134	udp	GigabitEthernet1/0/48	CORP_VN	192.168.13.42	10.16.1.30	53	48879	33168	18	Deny	Deny_IP_Log-00
>	12/14/24 5:25:05.000 AM	10.0.255.134	udp	GigabitEthernet1/0/48	CORP_VN	192.168.13.42	10.16.1.30	53	48879	33168	18	Deny	Deny_IP_Log-00
>	12/14/24 3:52:08.000 AM	10.0.255.134	udp	GigabitEthernet1/0/48	CORP_VN	192.168.13.42	10.16.1.42	53	48879	33168	18	Deny	Deny_IP_Log-00
>	12/14/24 3:52:08.000 AM	10.0.255.134	udp	GigabitEthernet1/0/48	CORP_VN	192.168.13.42	10.16.1.42	53	48879	33168	18	Deny	Deny_IP_Log-00
>	12/14/24 2:26:25.000 AM	10.0.255.132	udp	TenGigabitEthernet1/17	CORP_VN	192.168.13.42	10.16.1.52	53	48879	33152	18	Deny	Deny_IP_Log-00
>	12/13/24 11:39:09.000 PM	10.0.255.134	udp	GigabitEthernet1/0/48	CORP_VN	192.168.13.42	10.16.1.42	53	48879	33168	18	Deny	Deny_IP_Log-00
>	12/13/24 11:39:09.000 PM	10.0.255.134	udp	GigabitEthernet1/0/48	CORP_VN	192.168.13.42	10.16.1.42	53	48879	33168	18	Deny	Deny_IP_Log-00





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?

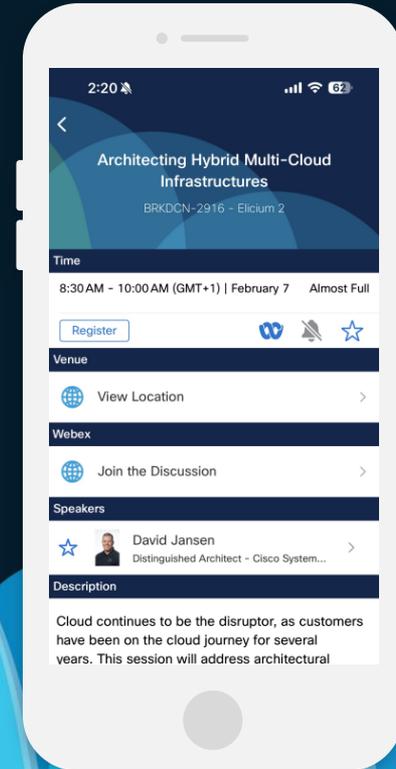
Use the Webex app to chat with the speaker after the session

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.

CISCO *Live!*



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



Thank you

CISCO *Live!*

CISCO *Live!*

GO BEYOND

A series of overlapping, rounded, teardrop-shaped abstract forms in various shades of blue, ranging from light to dark, positioned on the right side of the image.