



The bridge to possible

Next-Gen Segmentation: A Deep Dive into Group-Based Policy, SXPv5 and PxGrid Direct

Jonathan Casillas, Security Technical Leader
Ruben De La Vega, Escalation Engineer

BRKSEC-2154

CISCO *Live!*

#CiscoLive

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

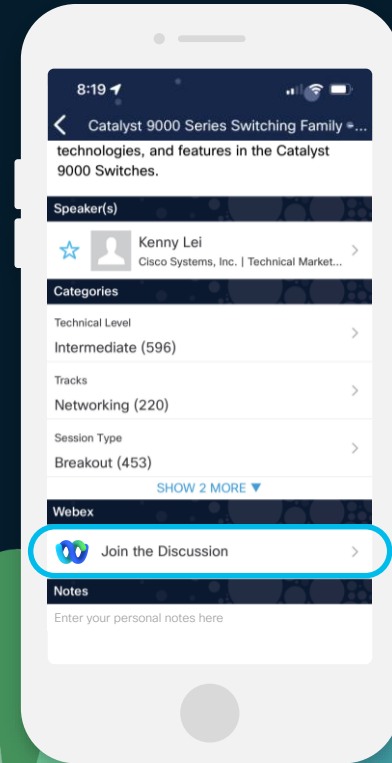
How

- 1 Find this session in the Cisco Live 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 June 7, 2024.

CISCO *Live!*

<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2154>



About me



- Been at Cisco for 6 years
- Escalation Engineer AAA
- Second time. in CLUS
- Favorite activities:
 - Friends and Family
 - Car guy
 - Walking/Landscapes
 - Videogames

About me



- Security TAC Technical Leader
- 7+ years working with AAA technologies
- 15+ published documents
- Favorite activities
 - Family time
 - Music
 - Astrophotography

Session Objectives

Session will cover:

- Overview of TrustSec fundamentals and latest innovations
- Configuration examples
- Advanced troubleshooting tips
- Demo

Session will not cover:

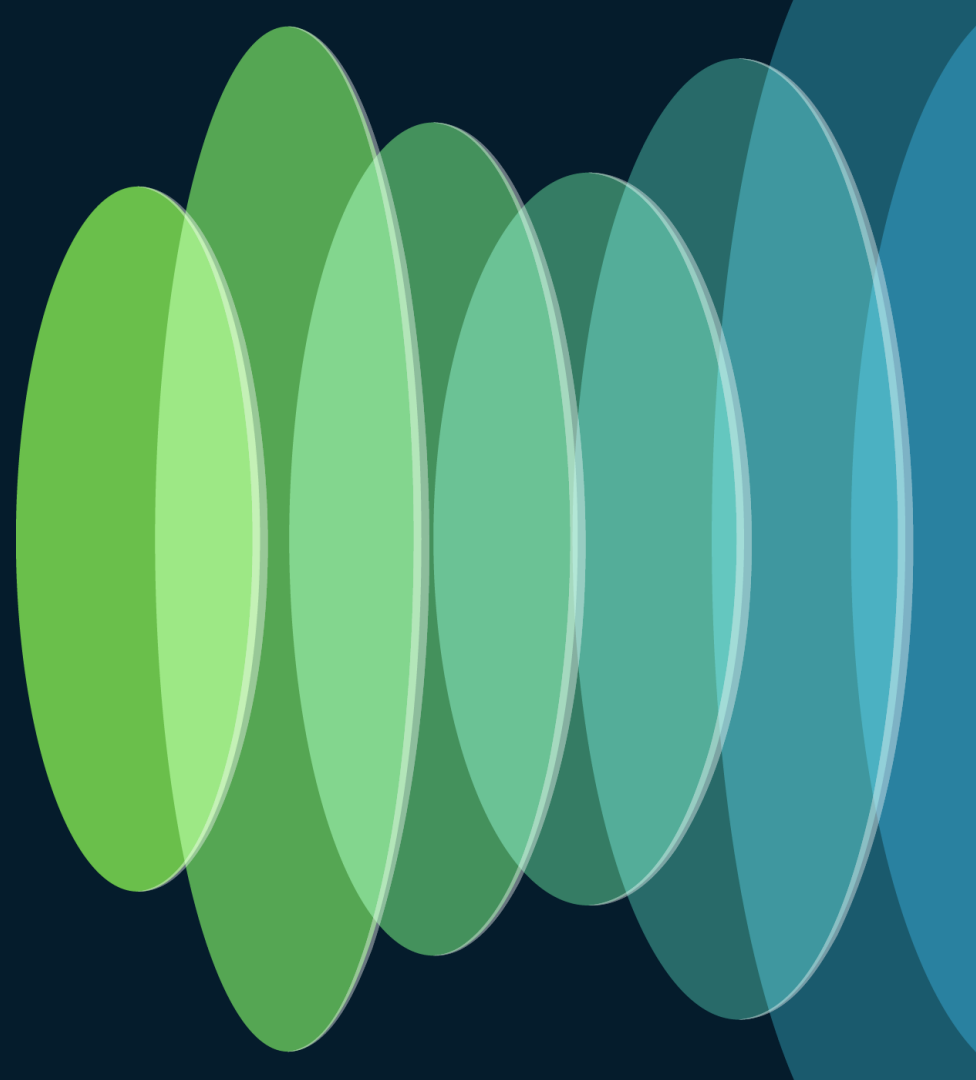
- Detailed aspects of TrustSec related to Catalyst Center
- TAC cases discussion
- Marketing
- Roadmaps



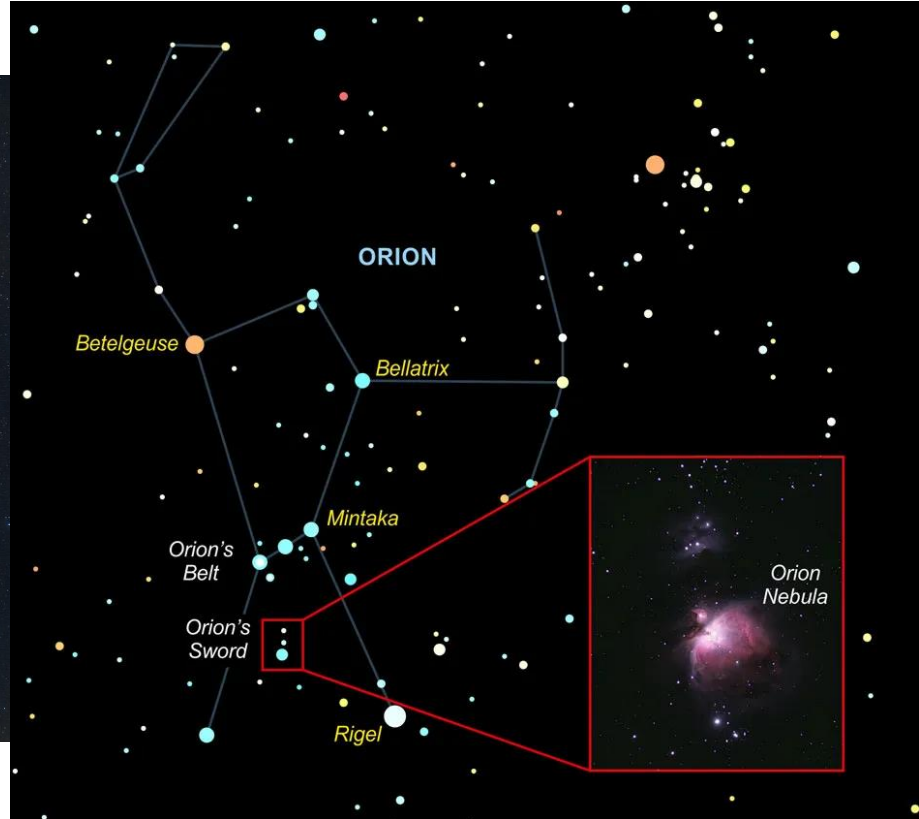
Agenda

- Introduction
- The Pillars of Trustsec
 - Demo
- PxGrid Direct
- Demo
- Key Takeaways
- The path forward
- Q&A

Introduction



Simplify complexity

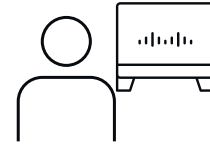
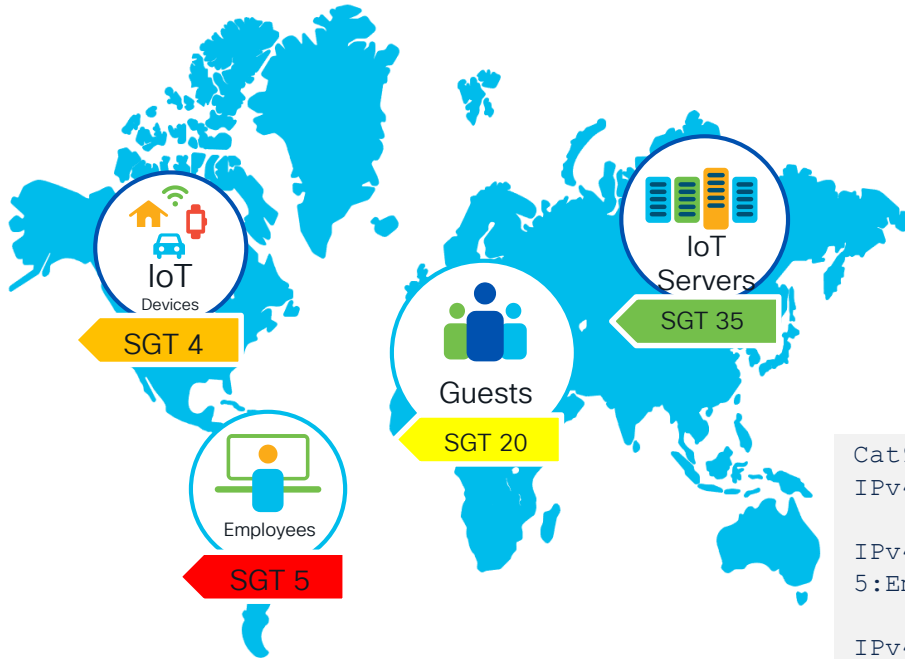


The scalability challenge



```
access-list 02 permit tcp...
access-list 02 permit udp...
access-list 02 permit icmp...
access-list 02 deny ip...
access-list 02 permit ucp...
access-list 02 deny ip...
access-list 02 deny icmp...
access-list 02 permit tcp...
access-list 02 permit tcp...
access-list 02 permit ip...
access-list 02 permit ip...
access-list 02 deny icmp...
access-list 02 permit udp...
access-list 02 permit icmp...
access-list 02 permit ip...
access-list 02 permit ip...
..
..
..
```

The solution

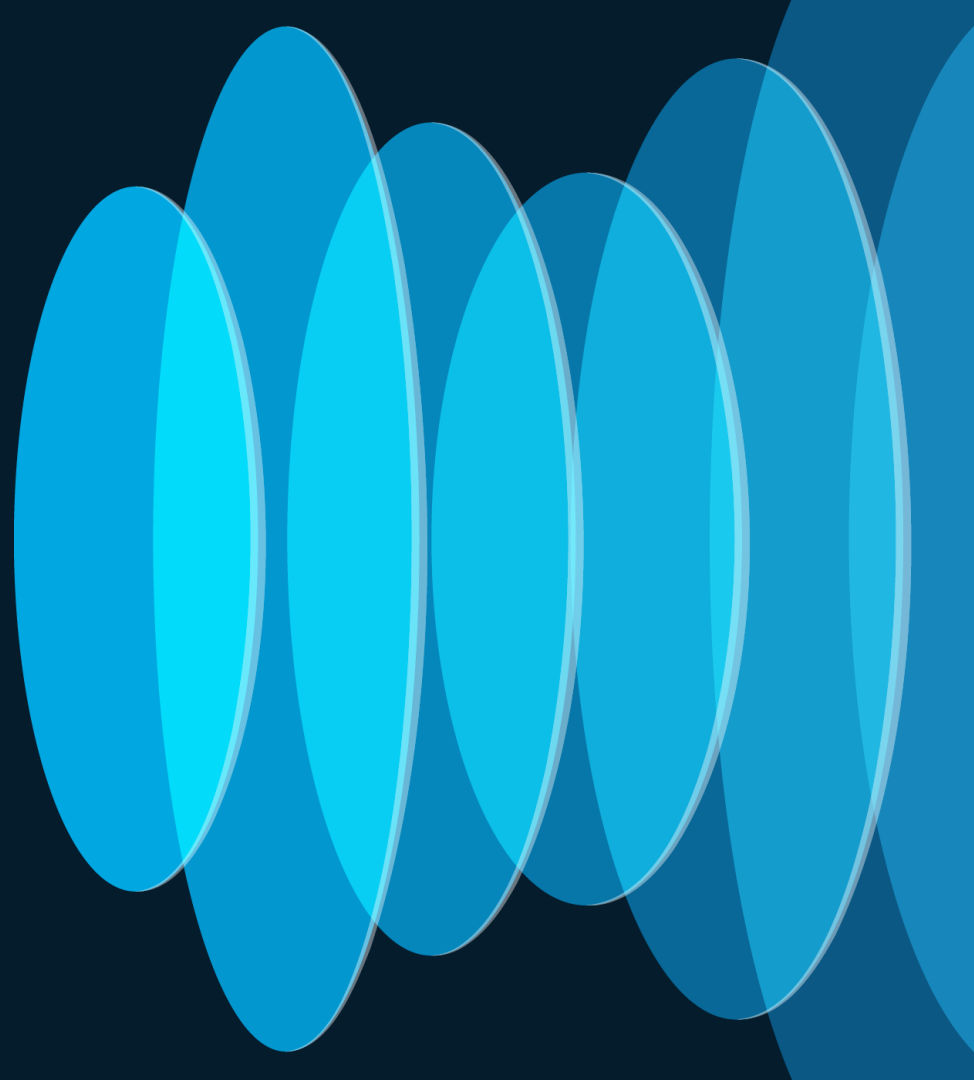


 Group tag management

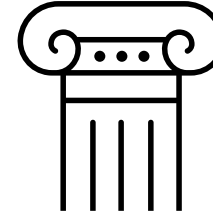
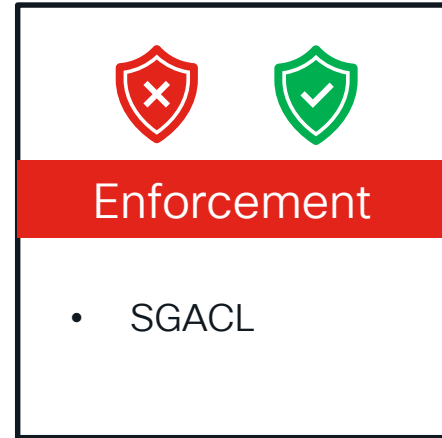
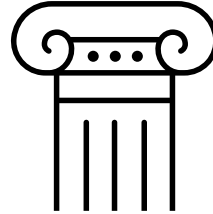
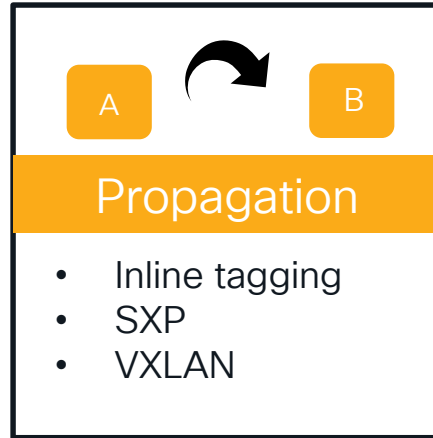
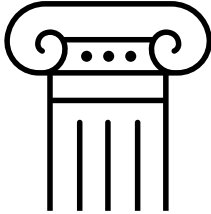
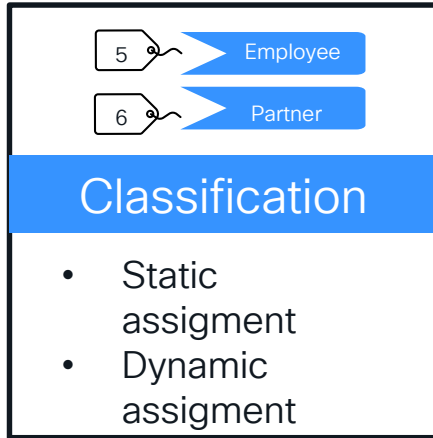
 Group policy management

```
Cat9300#show cts role-based permissions
IPv4 Role-based permissions default:
  Permit_IP-00
IPv4 Role-based permissions from group 4:Iot to group
5:Employees:
  Permit_IP_Log-01
IPv4 Role-based permissions from group 20:Guests to
group 4:Iot:
  Deny_IP_Log-00
```

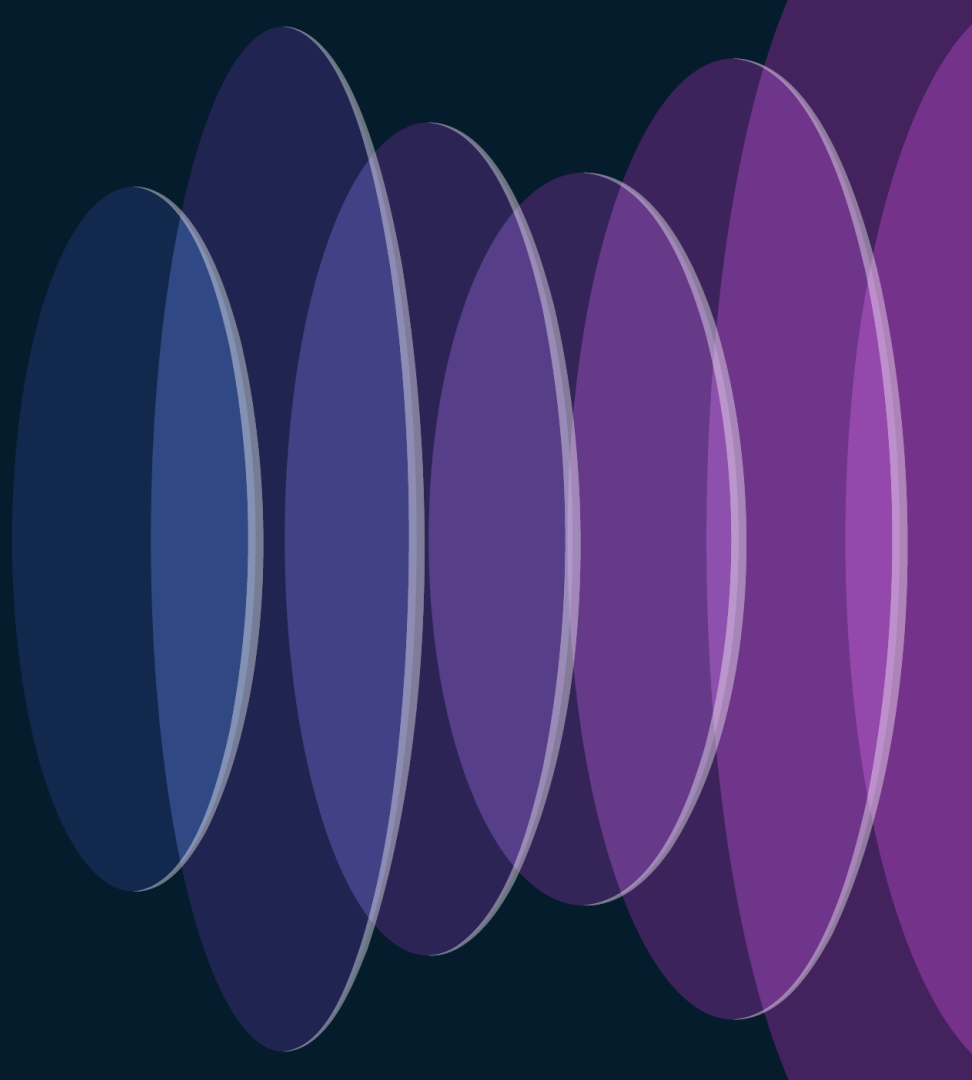
The Pillars of Trustsec



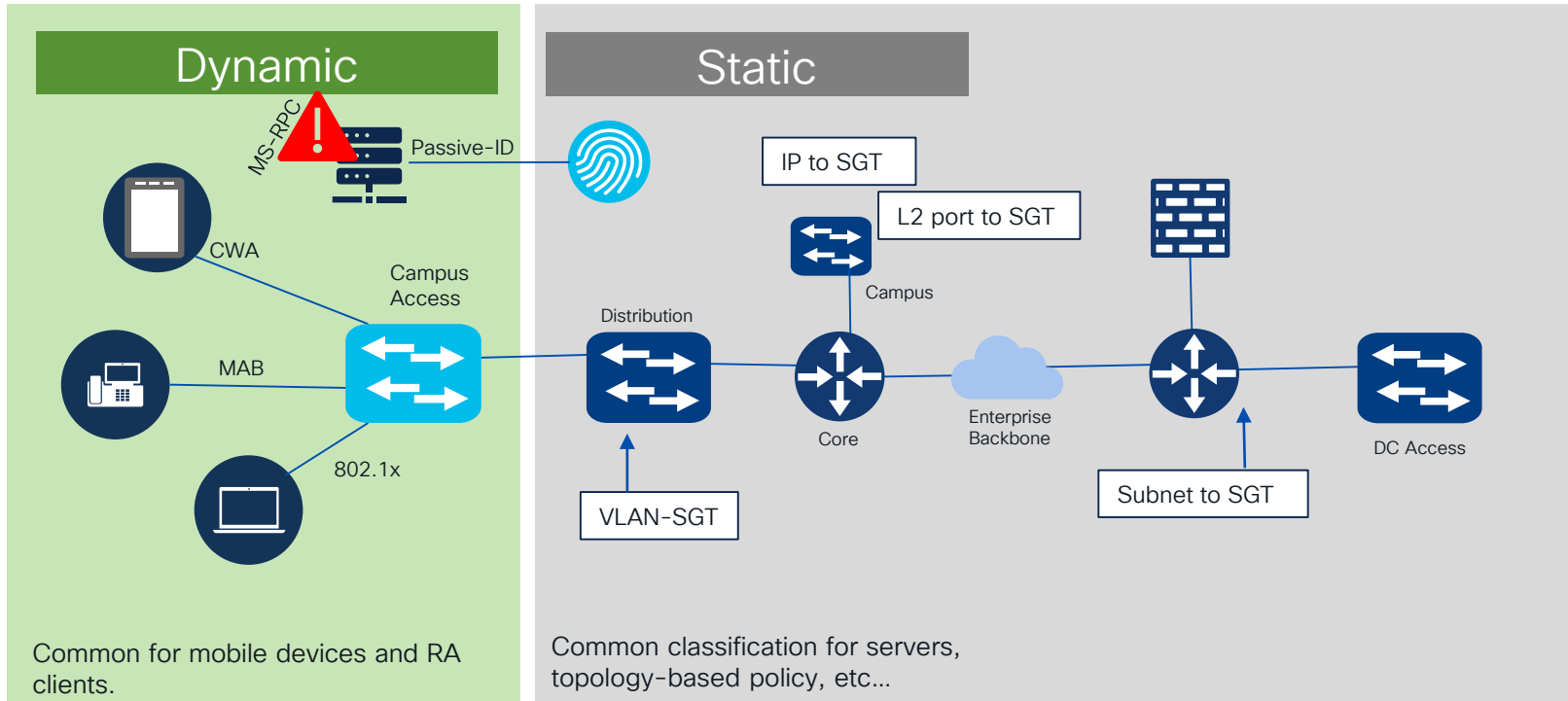
Three pillars



Classification



Classification types



Static classification configuration

IOS CLI Example



Reference

IP to SGT mapping

```
cts role-based sgt-map  
A.B.C.D sgt SGT
```

VLAN to SGT mapping

```
cts role-based sgt-map vlan-list  
VLAN sgt SGT
```

Subnet to SGT mapping

```
cts role-based sgt-map  
A.B.C.D/nn sgt SGT
```

L2IF to SGT mapping

```
(config-if-cts-manual)#policy  
static sgt SGT
```

L3IF to SGT mapping

```
cts role-based sgt-map  
interface name sgt SGT
```

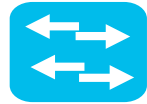
L3ID to Port Mapping

```
(config-if-cts-manual)#policy  
dynamic identity name
```

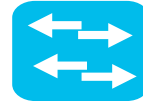
Static classification - Considerations



Reference



3560X
3560-CX
3750X
Industrial Ethernet



3650
3850
C6K
C9K

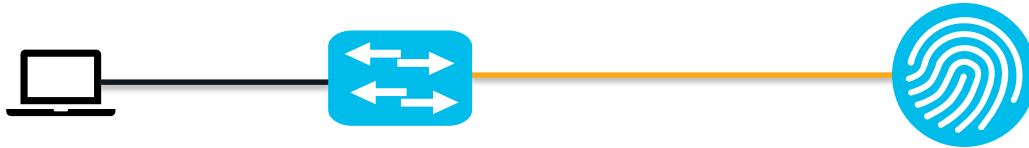
Port/VLAN (adjacent)

- Requires the MAC address of the endpoint to be learned for successful classification.
- These devices are better suited to classification only.

IP/Subnet

- Enforcement decisions are layer-3 specific and use the FIB table to determine destination SGT information.

Dynamic classification



RADIUS Access-Request



RADIUS Access-Accept



cisco-av-pair="cts:security-group-tag=16-00"

```
Switch#sh auth sess int Tw1/0/3 det
  Interface: TwoGigabitEthernet1/0/3
  IIF-ID: 0x17494F04
  MAC Address: c85b.768f.51b4
  IPv6 Address: fe80::9eb:a795:7e46:ffaf
  IPv4 Address: 10.4.18.167
  User-Name: C8-58-76-8F-51-B4
  Status: Authorized
  Domain: DATA
  Oper host mode: multi-host
  Oper control dir: both
  Session timeout: N/A
  Common Session ID: 28781F0A0000000C28913AE3
  Acct Session ID: 0x00000004
  Handle: 0x2f000002
  Current Policy: POLICY_Tw1/0/3

Local Policies:
  Service Template: DEFAULT_LINKSEC_POLICY_
  Security Policy: Should Secure

Server Policies:
  SGT Value: 16
```

NAS IPv4 Address	10.31.120.40
NAS Port Id	TwoGigabitEthernet1/0/3
NAS Port Type	Ethernet
Authorization Profile	PermitAccess
Security Group	PCA
Response Time	40 milliseconds

<input type="checkbox"/>	<input checked="" type="checkbox"/>	PCA	16/0010
--------------------------	-------------------------------------	-----	---------

Dynamic classification, considerations



```
Switch#sh auth sess int Tw1/0/3 det
      Interface: TwoGigabitEthernet1/0/3
      IIF-ID: 0x17494F04
      MAC Address: c85b.768f.51b4
      IPv6 Address: fe80::9eb:a795:7e46:ffaf
      IPv4 Address: 10.4.18.167
      User-Name: C8-5B-76-8F-51-B4
      Status: Authorized
      Domain: DATA
      Oper host mode: multi-host
      Oper control dir: both
      Session timeout: N/A
      Common Session ID: 28781F0A000000C28913AE3
      Acct Session ID: 0x00000004
      Handle: 0x2f000002
      Current Policy: POLICY_Tw1/0/3

Local Policies:
  Service Template: DEFAULT_LINKSEC_POLICY_
  Security Policy: Should Secure

Server Policies:
  SGT Value: 16
```

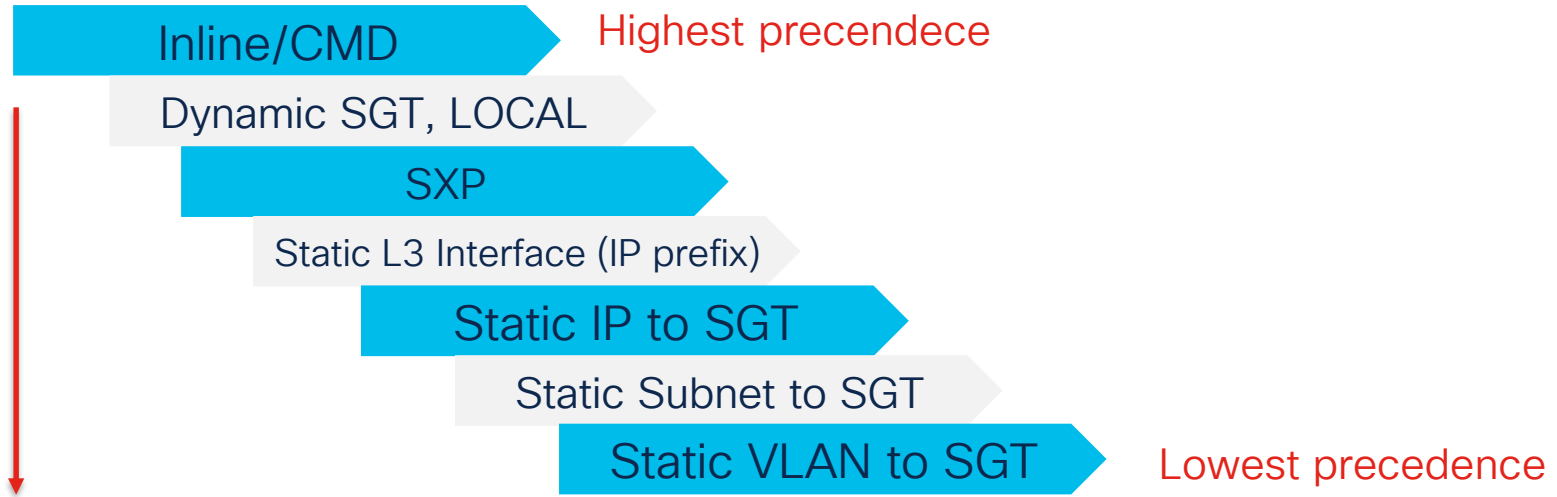
- ✓ SISF is turned ON
- ✓ Classification doesn't require PAC/env-data download.
- ✓ One IP-SGT table per VRF

```
Switch# sh cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address          SGT    Source
-----
10.4.18.167        16     LOCAL
10.10.10.10         9      SXP
10.31.120.40       2      INTERNAL

IP-SGT Active Bindings Summary
```

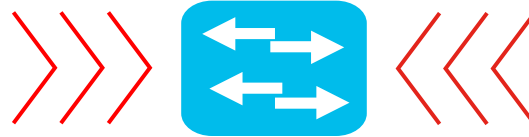
Order of precedence



Classification entries



Reference

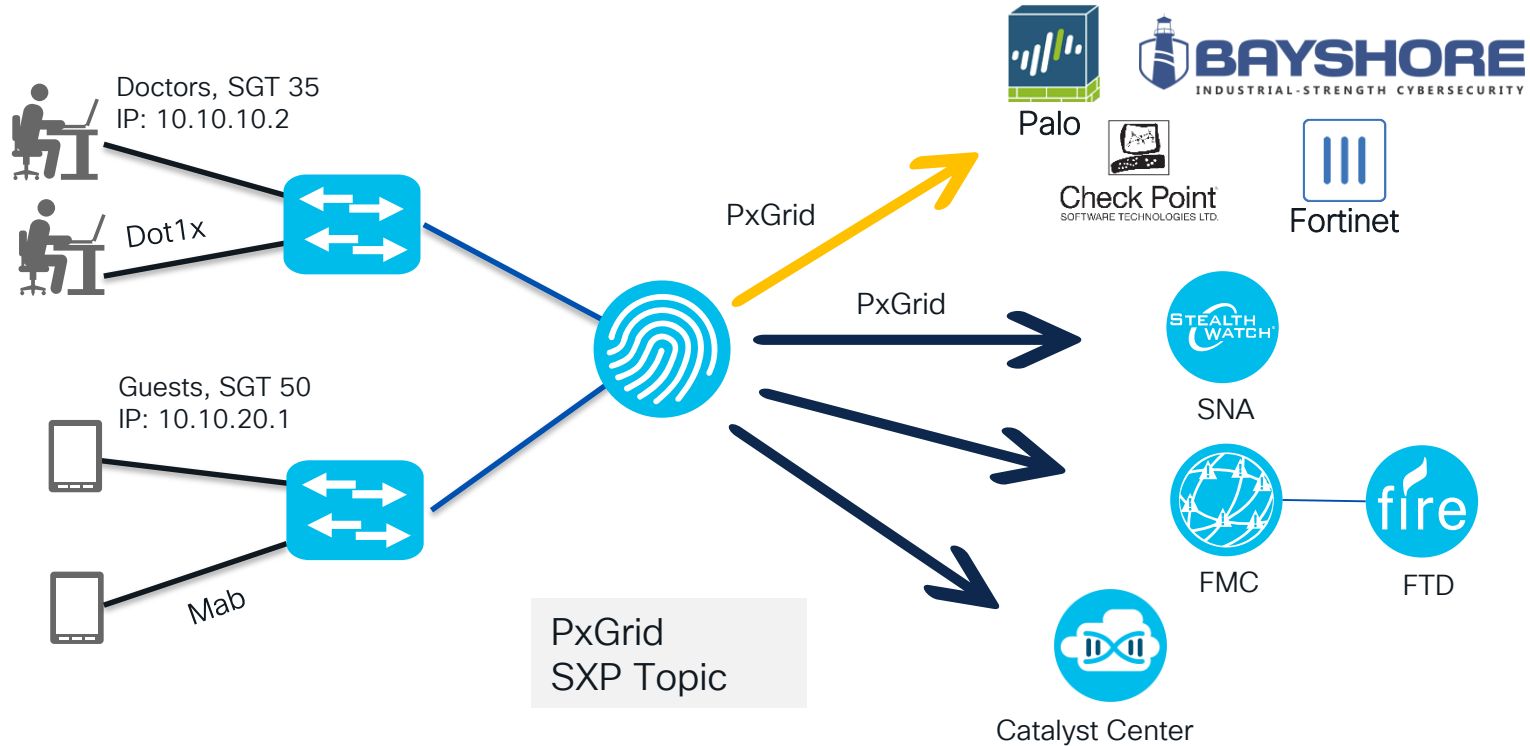


```
#show cts role-based sgt-map all
```

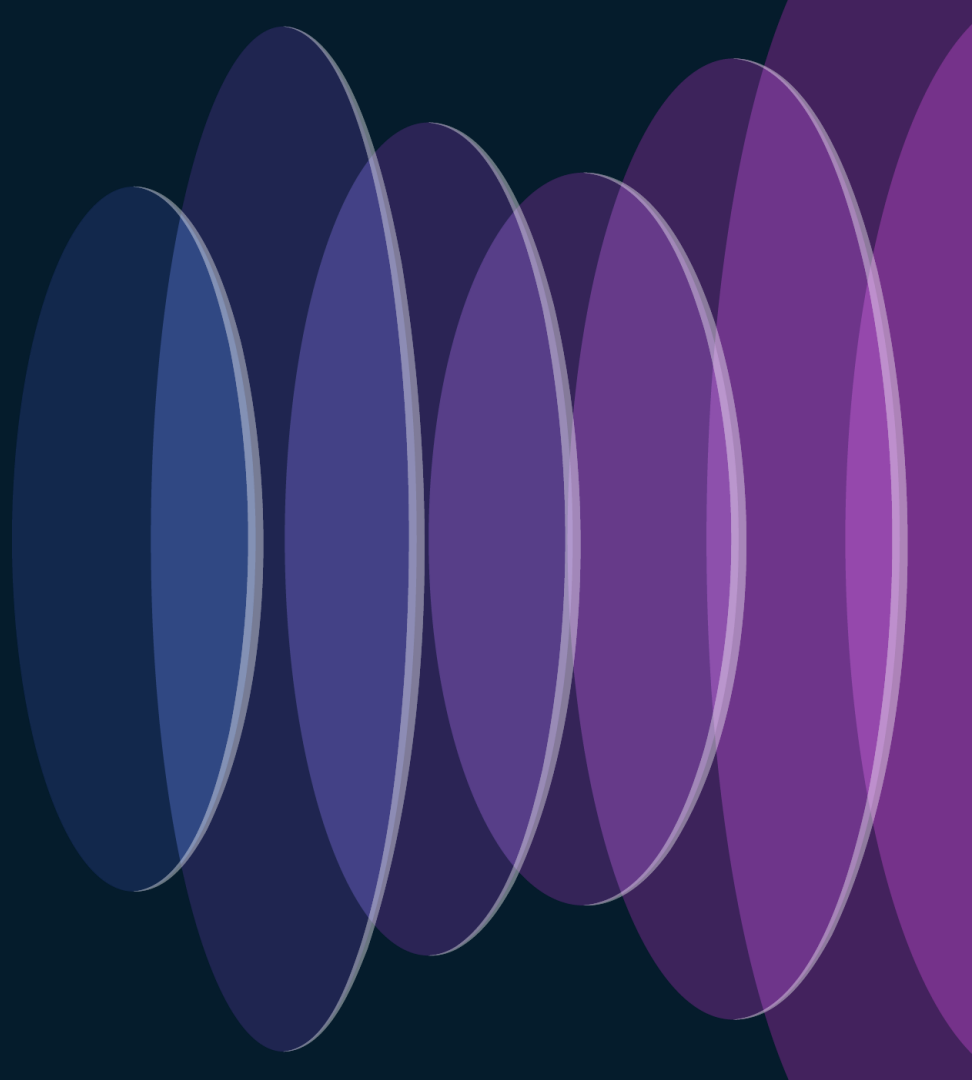
```
Active IPv4-SGT Bindings Information
```

IP Address	SGT	Source	
14.36.148.251	2	INTERNAL	<i>Locally configured IP address</i>
172.18.249.66	2	LOCAL	<i>Learned dynamically from ISE</i>
192.168.45.164	15	VLAN	<i>Learned from VLAN-SGT mapping</i>
192.168.199.10	5	CLI	<i>Configured using "cts role-based sgt-map"</i>
192.168.15.160	10	L3IF	<i>FIB entries that have a path through that interface</i>
192.168.15.161	8	L2IF	<i>Statically configured using "interface <interface> sgt manual policy static sgt <sgt-number>"</i>
192.168.15.123	7	SXP	<i>Learned through SXP peers</i>

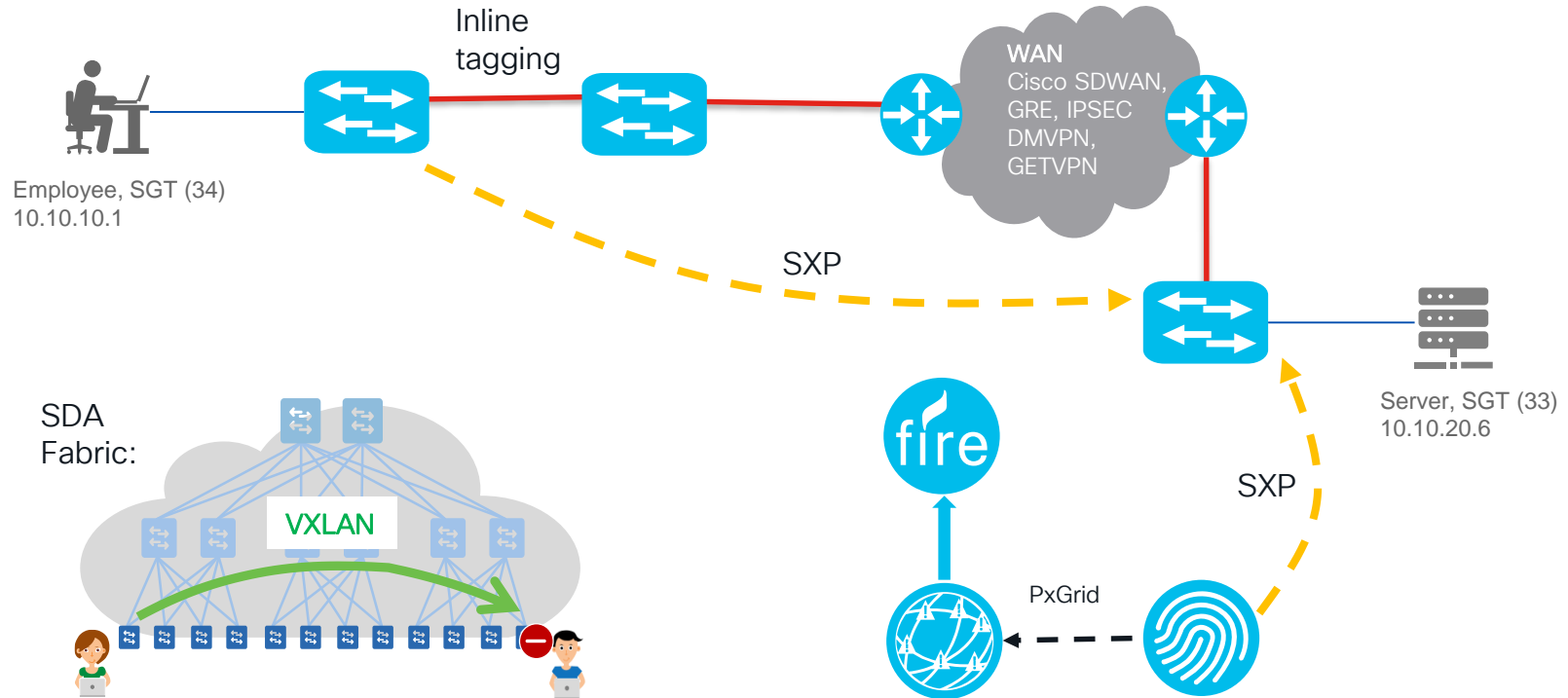
Use case: Dynamic Classification



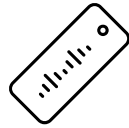
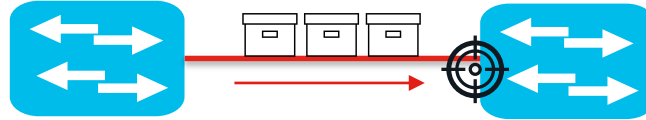
Propagation



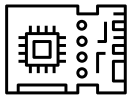
Propagation



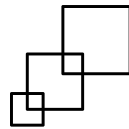
Inline tagging



Easy to configure
Its hardware-dependent

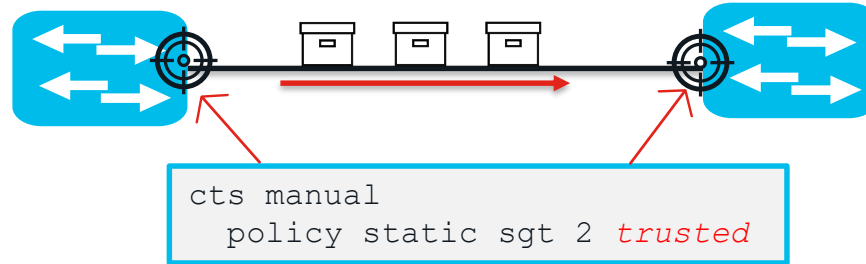


Tagging process prior
to other L2 services
such as QoS



No impact IP
MTU/Fragmentation
~ 20 bytes

Inline tagging, configuration



With *trusted*,
trust ingress SGT on wire

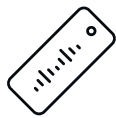
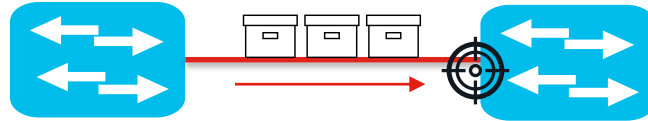
SGT 2 does nothing



Without *trusted*,
classify traffic with SGT 2

=Port:SGT classification

Inline tagging, troubleshooting



Bindings from inline tagging are not displayed in the mapping table (unless you configure SGT caching)



Instead, to see the tags take a pcap at the ingress interface.



OR you can use NetFlow instead.



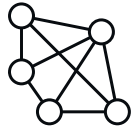
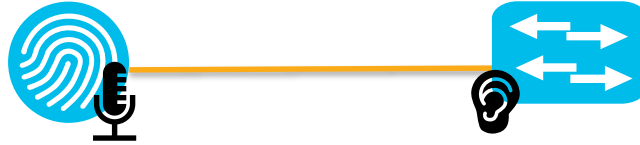
```
(config)# flow monitor cts-monitor-ipv4
Switch(config-flow-monitor)# record cts-record-ipv4
Switch(config)# interface TenGigabitEthernet 8/1
Switch(config-if)# ip flow monitor cts-monitor-ipv4
layer2-switched input
```

Example of CMD header in a pcap

No.	Time	Source	Destination	Protocol	Length	Info
6	2021-02-02 11:25:41	172.16.100.20	172.16.100.1	ICMP	122	Echo (ping) request id=0x001f, seq=0/0, ttl=254 (reply in 7)
7	2021-02-02 11:25:41	172.16.100.1	172.16.100.20	ICMP	114	Echo (ping) reply id=0x001f, seq=0/0, ttl=255 (request in 6)
8	2021-02-02 11:25:41	172.16.100.20	172.16.100.1	ICMP	122	Echo (ping) request id=0x001f, seq=1/256, ttl=254 (reply in 9)
9	2021-02-02 11:25:41	172.16.100.1	172.16.100.20	ICMP	114	Echo (ping) reply id=0x001f, seq=1/256, ttl=255 (request in 8)
10	2021-02-02 11:25:41	172.16.100.20	172.16.100.1	ICMP	122	Echo (ping) request id=0x001f, seq=2/512, ttl=254 (reply in 11)
11	2021-02-02 11:25:41	172.16.100.1	172.16.100.20	ICMP	114	Echo (ping) reply id=0x001f, seq=2/512, ttl=255 (request in 10)
12	2021-02-02 11:25:41	172.16.100.20	172.16.100.1	ICMP	122	Echo (ping) request id=0x001f, seq=3/768, ttl=254 (reply in 13)
13	2021-02-02 11:25:41	172.16.100.1	172.16.100.20	ICMP	114	Echo (ping) reply id=0x001f, seq=3/768, ttl=255 (request in 12)
14	2021-02-02 11:25:41	172.16.100.20	172.16.100.1	ICMP	122	Echo (ping) request id=0x001f, seq=4/1024, ttl=254 (reply in 15)
15	2021-02-02 11:25:41	172.16.100.1	172.16.100.20	ICMP	114	Echo (ping) reply id=0x001f, seq=4/1024, ttl=255 (request in 14)
16	2021-02-02 11:25:43	172.16.100.20	172.16.100.1	ICMP	122	Echo (ping) request id=0x0020, seq=0/0, ttl=254 (reply in 17)
17	2021-02-02 11:25:43	172.16.100.1	172.16.100.20	ICMP	114	Echo (ping) reply id=0x0020, seq=0/0, ttl=255 (request in 16)

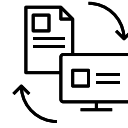
Frame 6: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
Ethernet II, Src: Cisco_d1:fd:46 (00:3c:10:d1:fd:46), Dst: Cisco_5d:f0:7d (6c:b2:ae:5d:f0:7d)
Cisco MetaData
Version: 1
Length: 1
Options: 0x0001
SGT: 6
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.16.100.20, Dst: 172.16.100.1
Internet Control Message Protocol

Security Group Tag Exchange Protocol, SXP



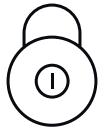
SXP very simple to enable

- No hardware dependencies



Uses TCP for transport protocol

- TCP 6499



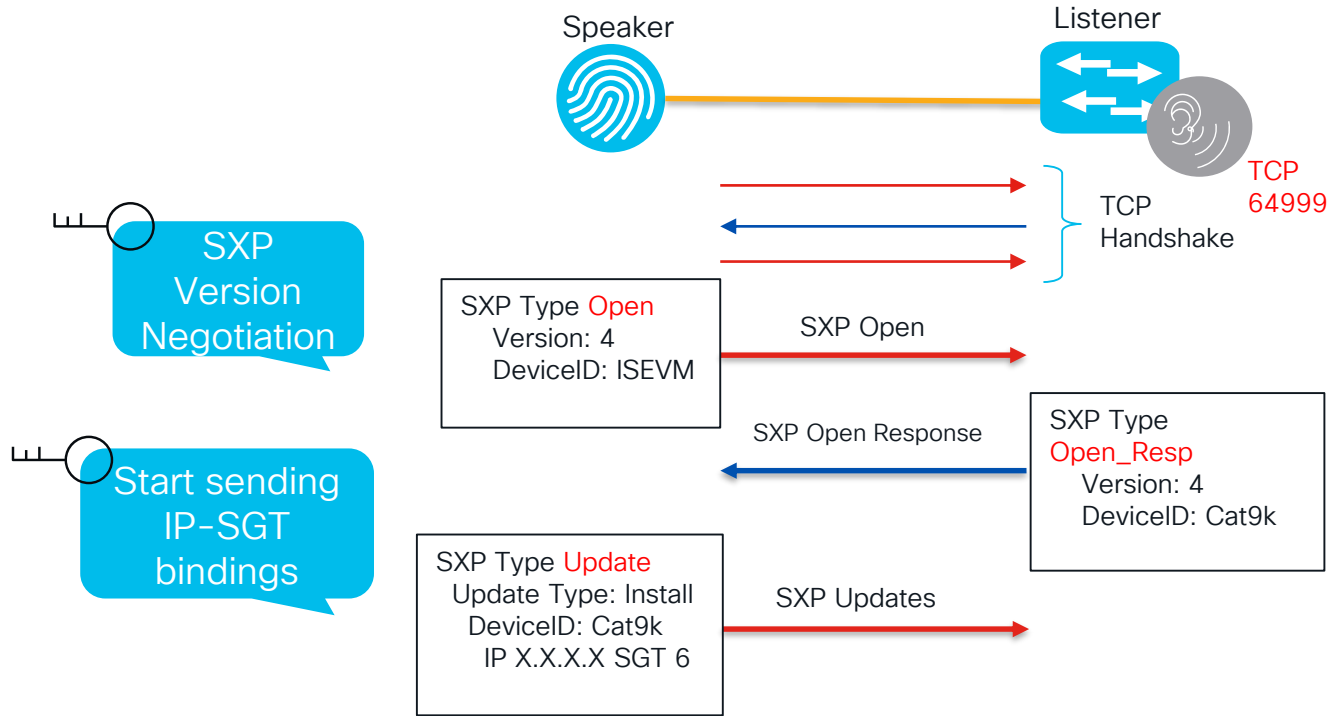
Uses MD5 for authentication and integrity check



SXP roles

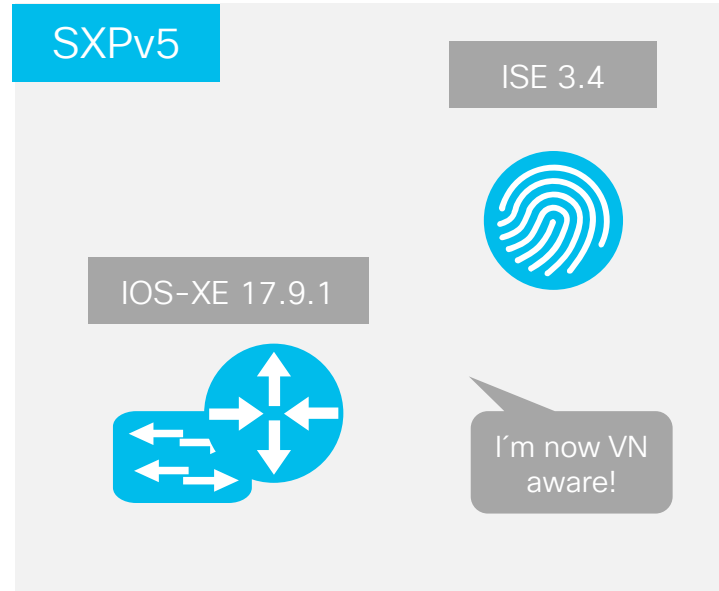
- Speaker
- Listener
- Both

SXP flow

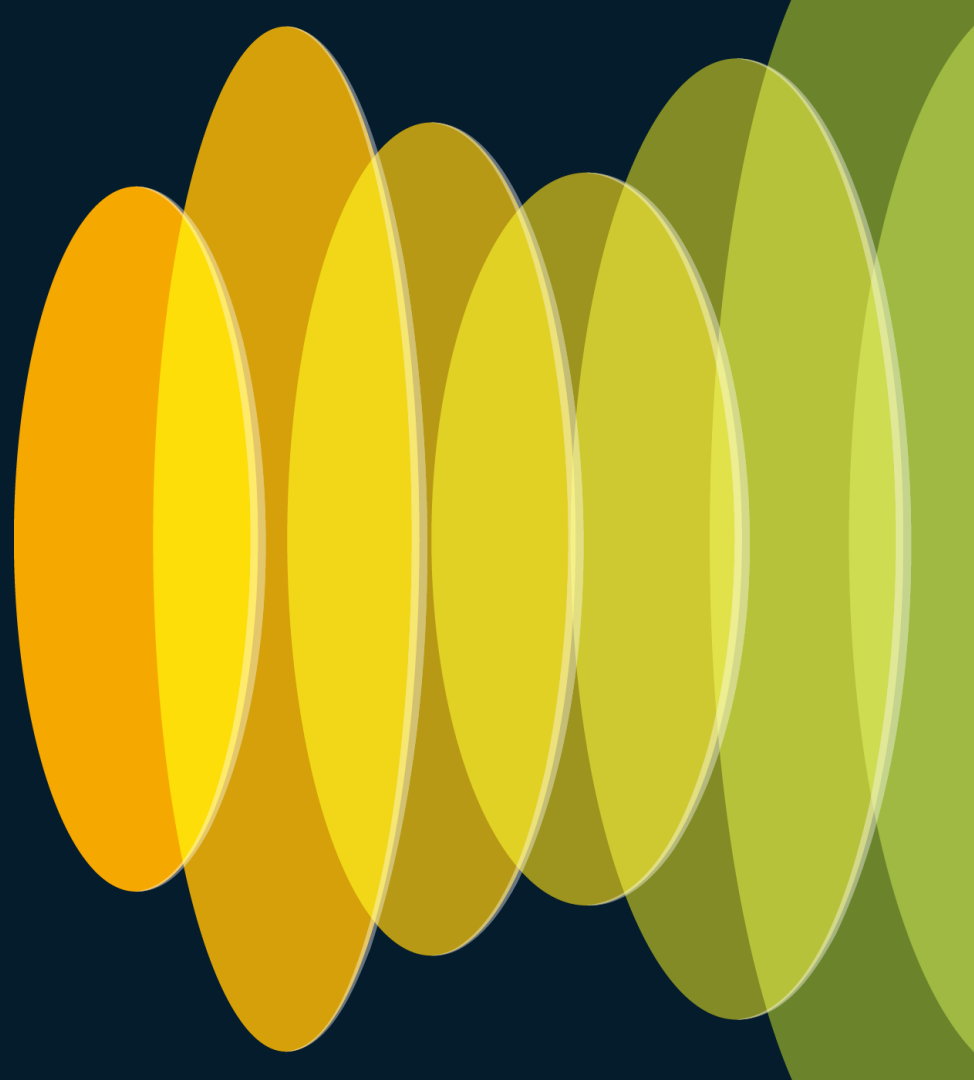


SXP versions

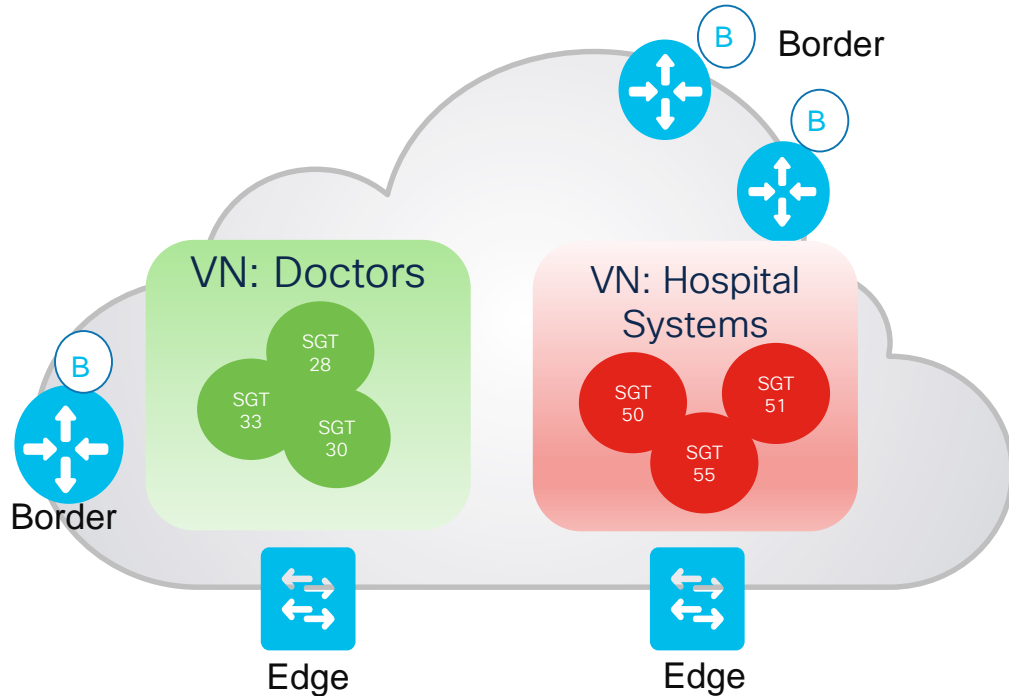
SXP Version 1	Initial SXP version supporting IPv4 binding propagation.
SXP Version 2	Includes support for IPv6 binding propagation and version negotiation.
SXP Version 3	Adds support for Subnet-SGT binding propagation.
SXP Version 4	Loop detection and prevention, capability exchange and built-in keep-alive mechanism.



Discover SXPv5



SDA Fabric Segmentation



Macro-Segmentation

- Virtual Network level
- Based on VRF
- Hosts in different VNs should not communicate

Micro-Segmentation

- Within one Virtual Network
- Based on SGTs
- Hosts communicate based on role-based permissions

Why SXPv5?

SXPv4
IP:SGT mappings

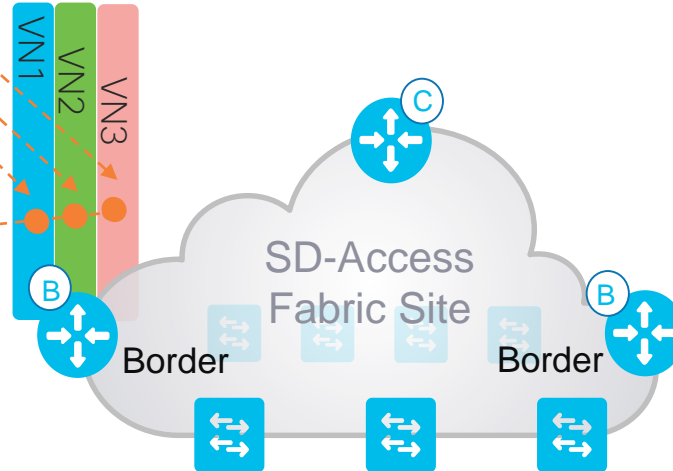


SXP connection per VN

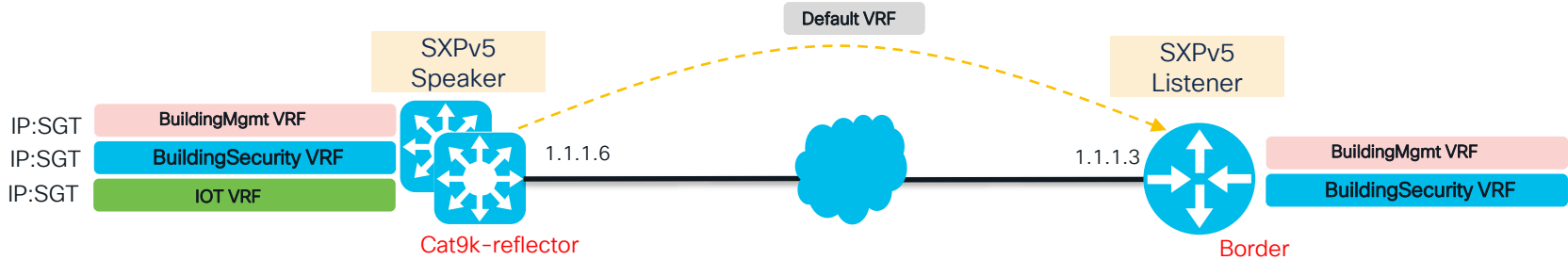


Single SXP connection with
all VNs

SXPv5
Same IP:SGT



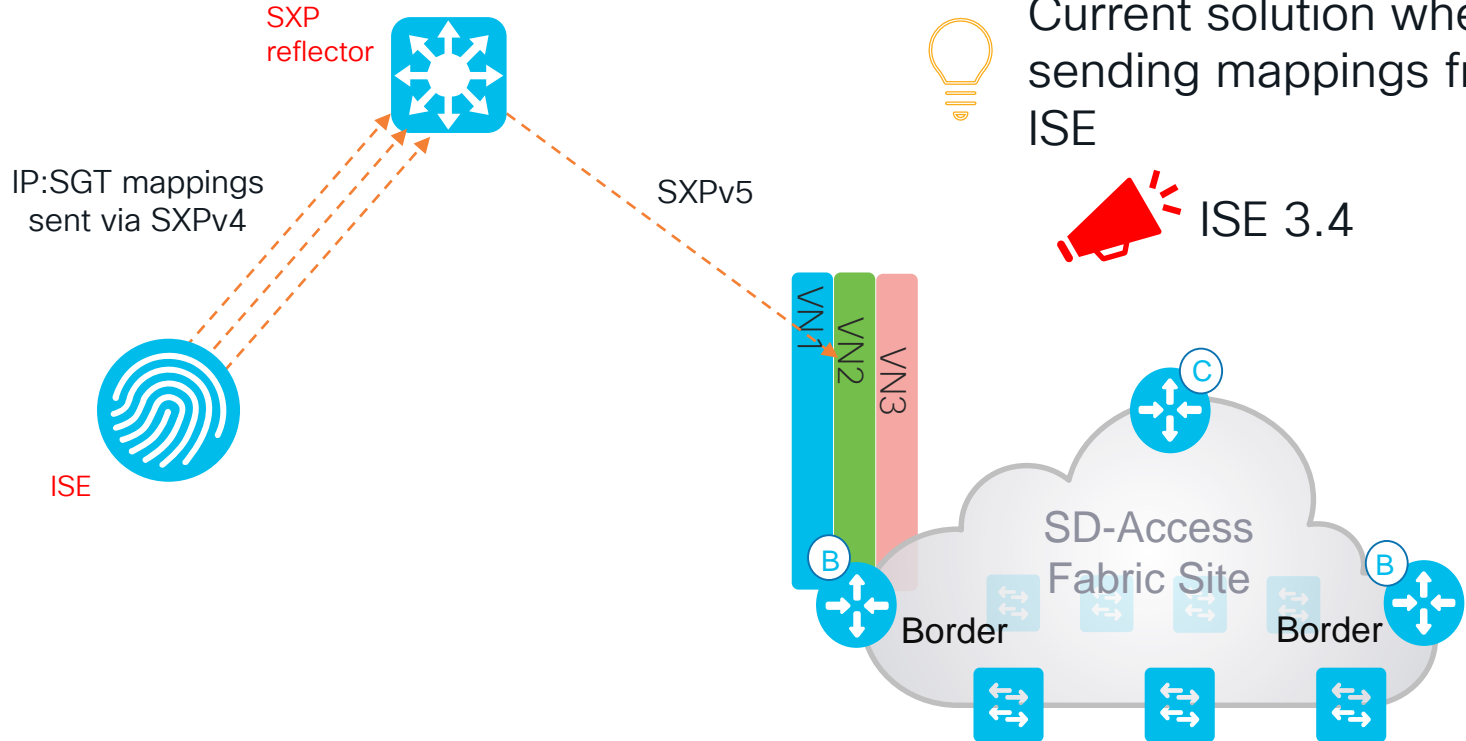
SXPv5 configuration



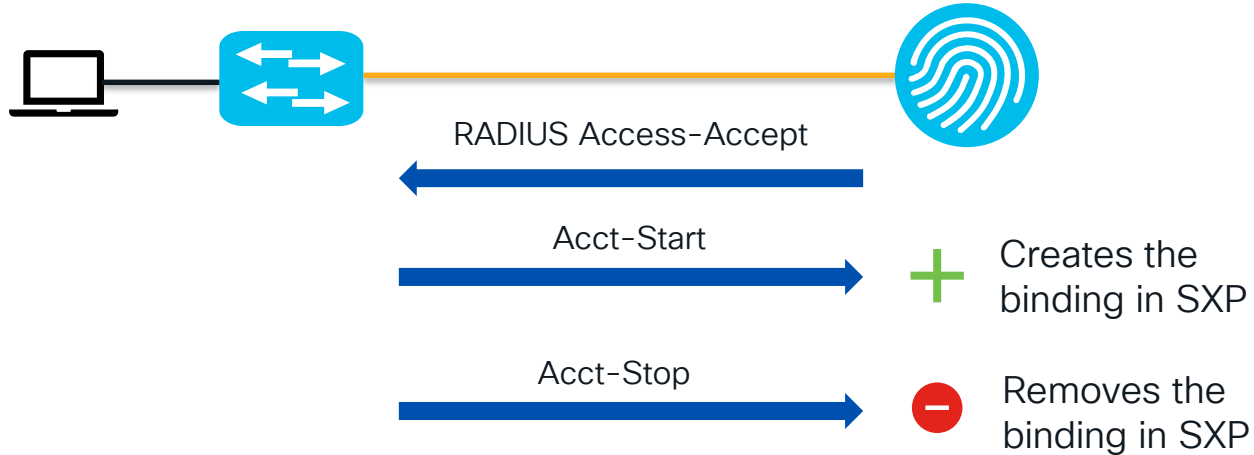
```
cts sxp export-list SXPv5-export-VRFs-to-Border
vrf BuildingMgmt
vrf BuildingSecurity
!
cts sxp export-import-group speaker SXPv5-
speaker-grp-to-Border
export-list SXPv5-export-VRFs-to-Border
peer 1.1.1.3
```

```
cts sxp import-list SXPv5-import-from-Reflector
vrf
!
cts sxp export-import-group listener SXPv5-import-grp-
from-Reflector
import-list SXPv5-import-from-Reflector
peer 1.1.1.6
```

SXP reflector



Use case: Dynamic classification and SXP



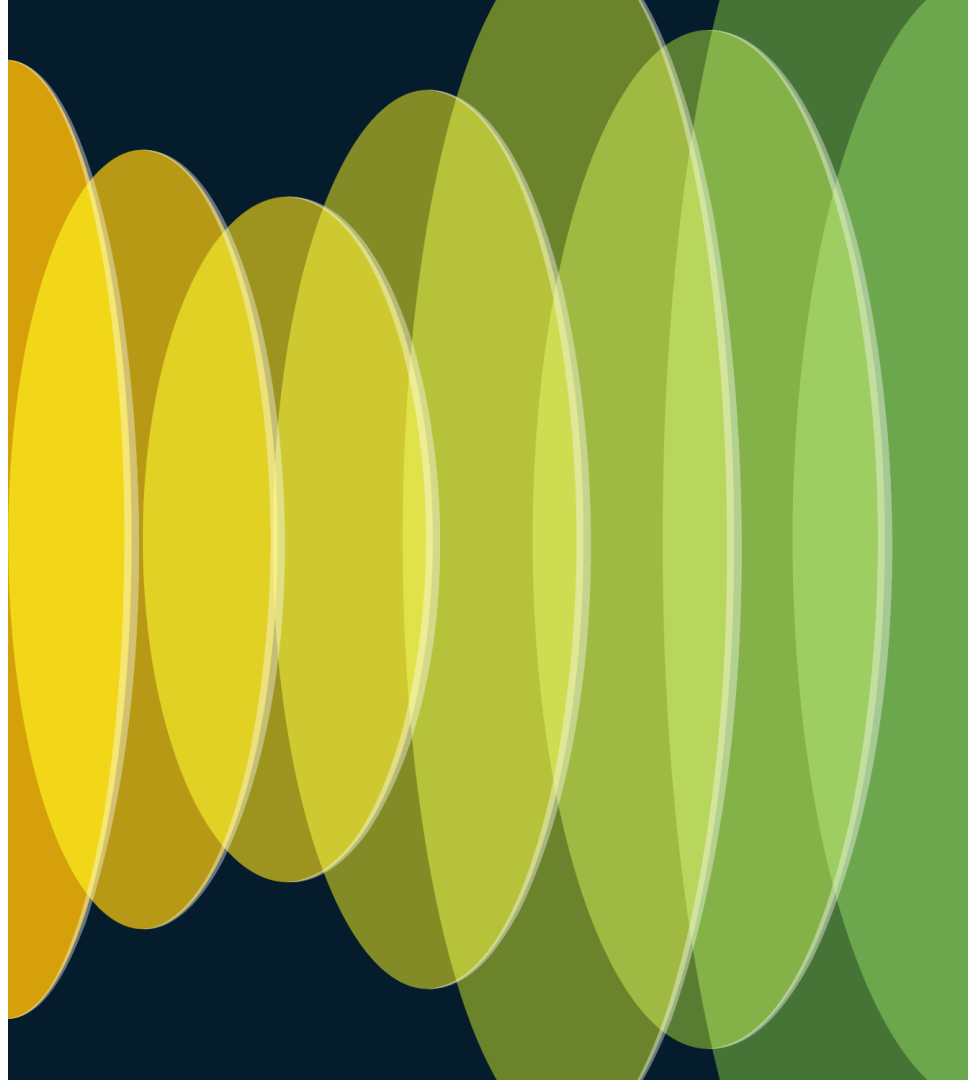
IP-SGT mapping in ISE SXP table is maintained with Accounting packets.



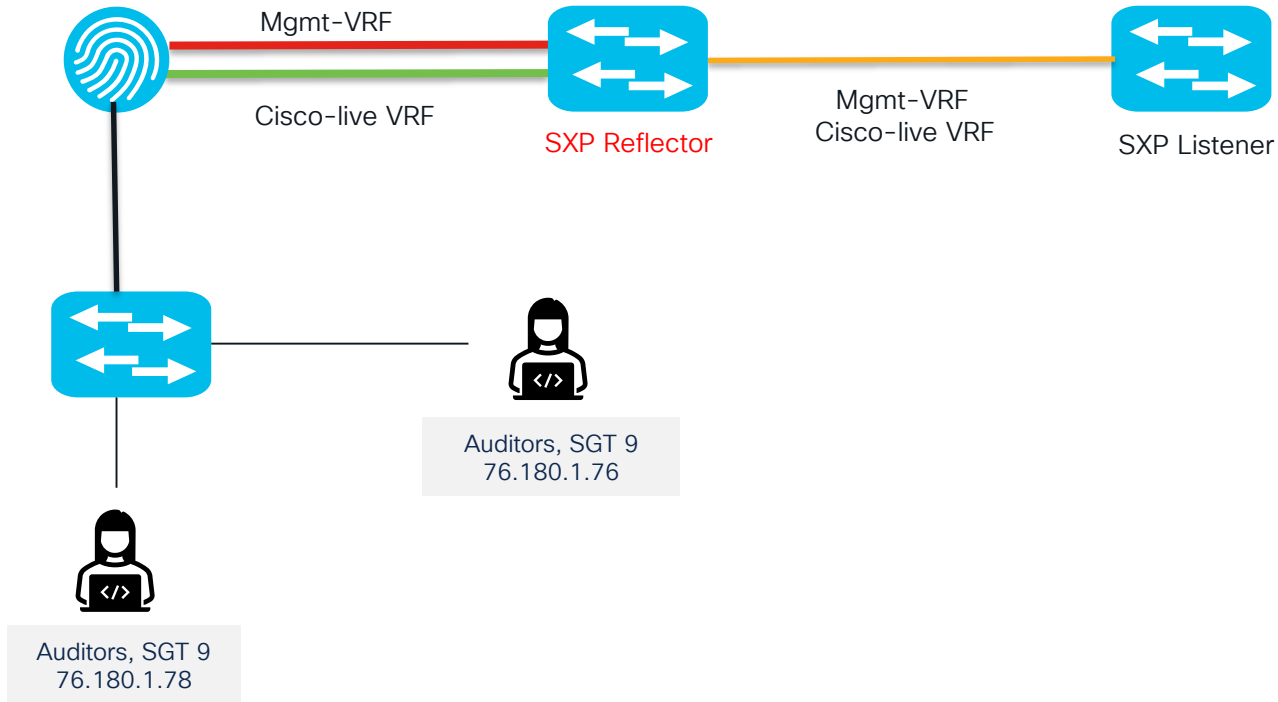
If a binding doesn't get an interim-acct/stop ISE will remove it after 5 days.

Demo






CISCO *Live!*




















SXPv5 Reflector



▼ Authorization Policy(15)

				Results		
 Status	Rule Name	Conditions		Profiles	Security Groups	
<input type="text" value="Search"/>						
	Sprt	 Network Access·NetworkDeviceName EQUALS sprt		PermitAccess	  Auditors	

us	Details	Identity	Security Group	Authentication Policy	Authorization Policy	Authorizatio...	IP Address	Network Device
		Identity	Security Group	Authentication Policy	Authorization Policy	Authorization Pro	IP Address 	Network Device
		8C:C1:4A:A4:12:78	Auditors	Default >> MAB	Default >> Sprt	PermitAccess	10.20.30.40	
		E9:18:22:65:A8:42	Auditors	Default >> MAB	Default >> Sprt	PermitAccess	10.20.30.204	
		96:C0:D0:C4:DC:B9	Auditors	Default >> MAB	Default >> Sprt	PermitAccess	10.20.30.8	
		3D:2A:99:DA:22:82	Auditors	Default >> MAB	Default >> Sprt	PermitAccess	10.20.30.108	
		E9:18:22:65:A8:42		Default >> MAB	Default >> Sprt	PermitAccess		SPRT
		8C:C1:4A:A4:12:78		Default >> MAB	Default >> Sprt	PermitAccess		SPRT
		96:C0:D0:C4:DC:B9		Default >> MAB	Default >> Sprt	PermitAccess		SPRT
		3D:2A:99:DA:22:82		Default >> MAB	Default >> Sprt	PermitAccess		SPRT

SXP Devices (i)

Rows/Page 1 ⌂ ⏪ ⏩ 1 ⌵

↻ [Add](#) [Trash](#) ⌵ [Edit](#) [Assign SXP Domain](#)

<input type="checkbox"/>	Name	IP Address	Status	Peer Ro...	SXP Do...	SXP Version	Neg...	Pass...	Connected To	Duration ...
<input type="checkbox"/>	9300-09	<u>10.31.121.160</u>	<u>ON</u>	<u>LISTENER</u>	<u>cisco-live</u>	<u>V4</u>	V4	DEFA...	ise33a	00:00:57:06

All SXP Mappings ⓘ

Rows/Page 4 ▼ < 1

[↻](#) [Add SXP Domain filter](#) [Manage SXP Domain filters](#)

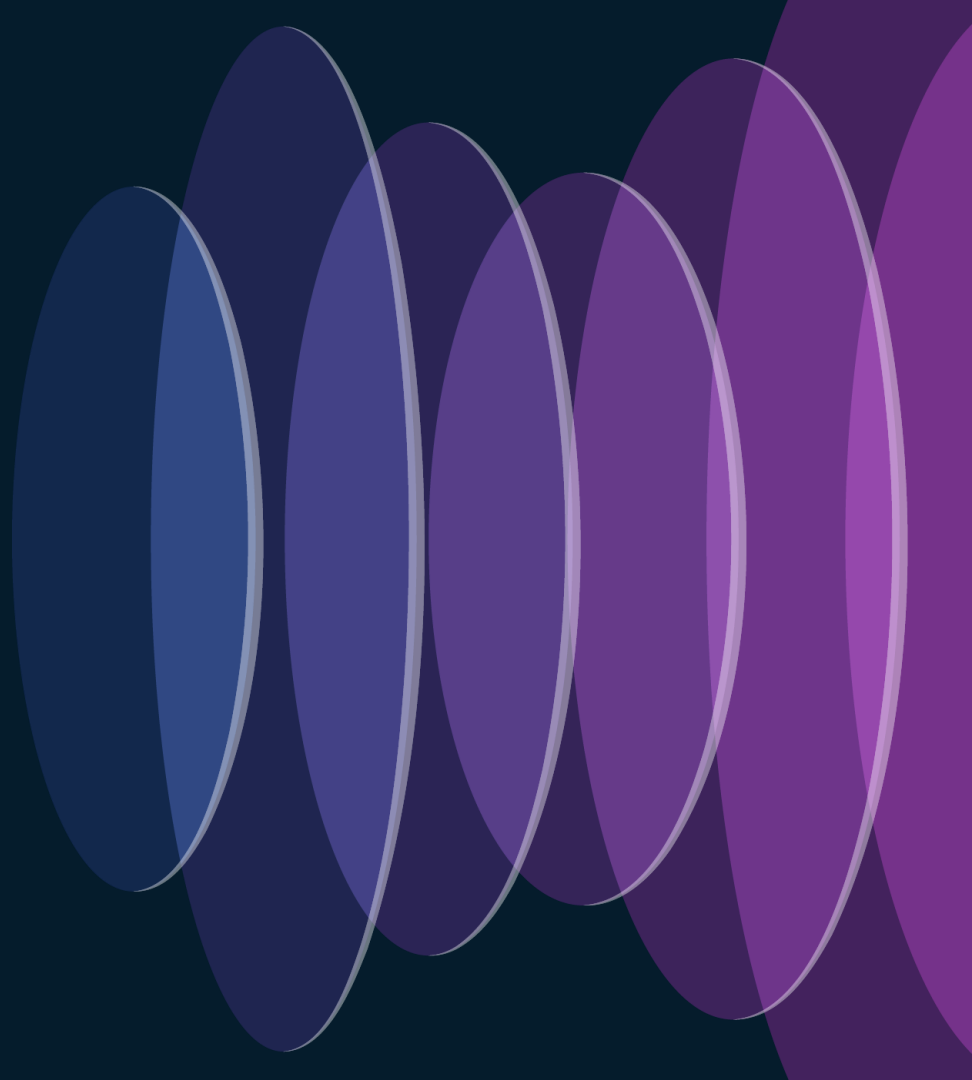
IP Address	SGT	VN	Learned From	Learned ...	SXP Domain	PSNs Involved
10.20.30.8/32	Auditors (9/0009)		10.31.126.181,10.31.126.245	Session	cisco-live	ise33a
10.20.30.40/32	Auditors (9/0009)		10.31.126.181,10.31.126.245	Session	cisco-live	ise33a
10.20.30.108/32	Auditors (9/0009)		10.31.126.181,10.31.126.245	Session	cisco-live	ise33a
10.20.30.204/32	Auditors (9/0009)		10.31.126.181,10.31.126.245	Session	cisco-live	ise33a

```
MXC.TAC.N.04-9300-09#show cts role-based sgt-map vrf cisco-live all
%IPv6 protocol is not enabled in VRF cisco-live
Active IPv4-SGT Bindings Information
```

IP Address	SGT	Source
10.20.30.8	9	SXP
10.20.30.40	9	SXP
10.20.30.108	9	SXP
10.20.30.204	9	SXP

```
IP-SGT Active Bindings Summary
=====
Total number of SXP          bindings = 4
Total number of active      bindings = 4
```

Enforcement



CTS concepts



CTS Credentials

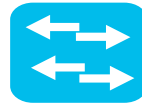
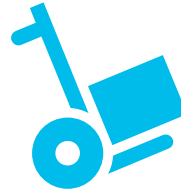


Protected-access
Credential PAC



PAC Provisioning

Environmental data



- 1 Network device security group
- 2 CTS server list
- 3 Security Group List
- 4 Refresh timers

CTS Request process

- Device discovery
- Plug n Play
- Manual Configuration



1

CTS
Credentials

Configure



Request

CTS Pac

2

```
show cts pac
AID:
2545A5CB09E8EA76E905977C39D94D7F
PAC-Info:
  PAC-type = Cisco Trustsec
  AID:
2545A5CB09E8EA76E905977C39D94D7F
..
..
```

```
#show cts environment-data
CTS Environment Data
=====
Current state = COMPLETE
-omitted--
Security Group Name Table:
  0-00:Unknown
  2-00:TrustSec_Devices
  3-00:Network_Services
  4-06:Employees
  5-00:Contractors
```

Request

CTS SGACLs

4

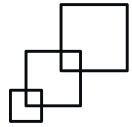
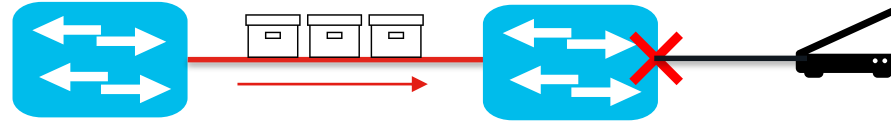
CTS Env-Data

Request

```
#show cts role-based
permissions
IPv4 Role-based
permissions default:
  Permit IP-00
IPv4 Role-based
permissions from group
16:Kris to group
8:Developers:
  Deny IP-00
..
..
```



Enforcement, considerations



SGACL/RBACL

NO source/destination IP info
ONLY permitted/denied traffic
based on protocols, ports, etc.



Switch downloads only the
SGACL associated with the IP-
SGT bindings that it has.

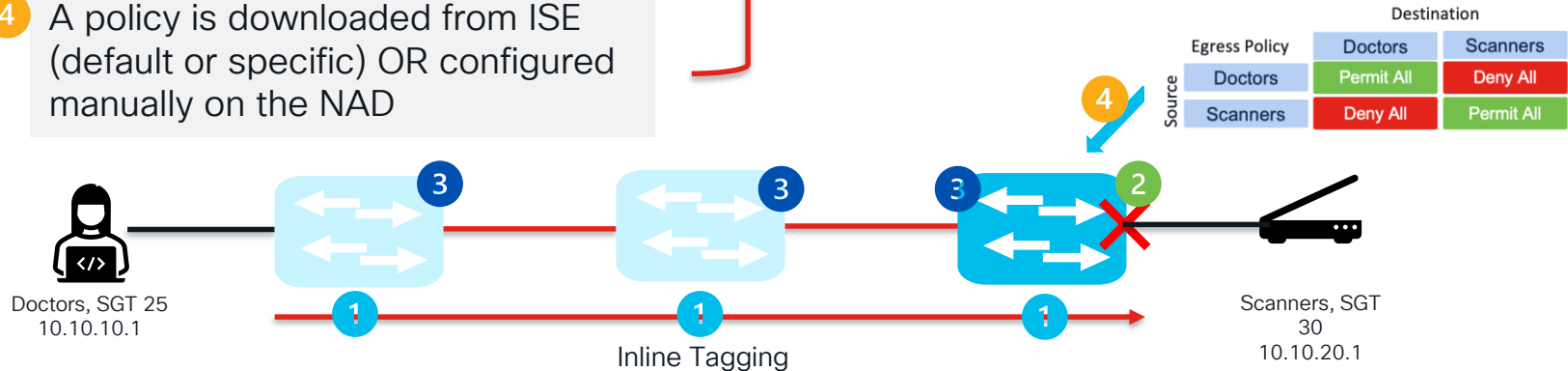


Traffic tagged with SGT 0
(unknown) will hit the default
configured action.

Where does enforcement occur?

- 1 Source IP:SGT binding
- 2 Destination IP:SGT binding
- 3 Platform and VLAN has enforcement enabled
- 4 A policy is downloaded from ISE (default or specific) OR configured manually on the NAD

“Enforcement is conducted at the primary platform along the traffic route that meets all of the following conditions”

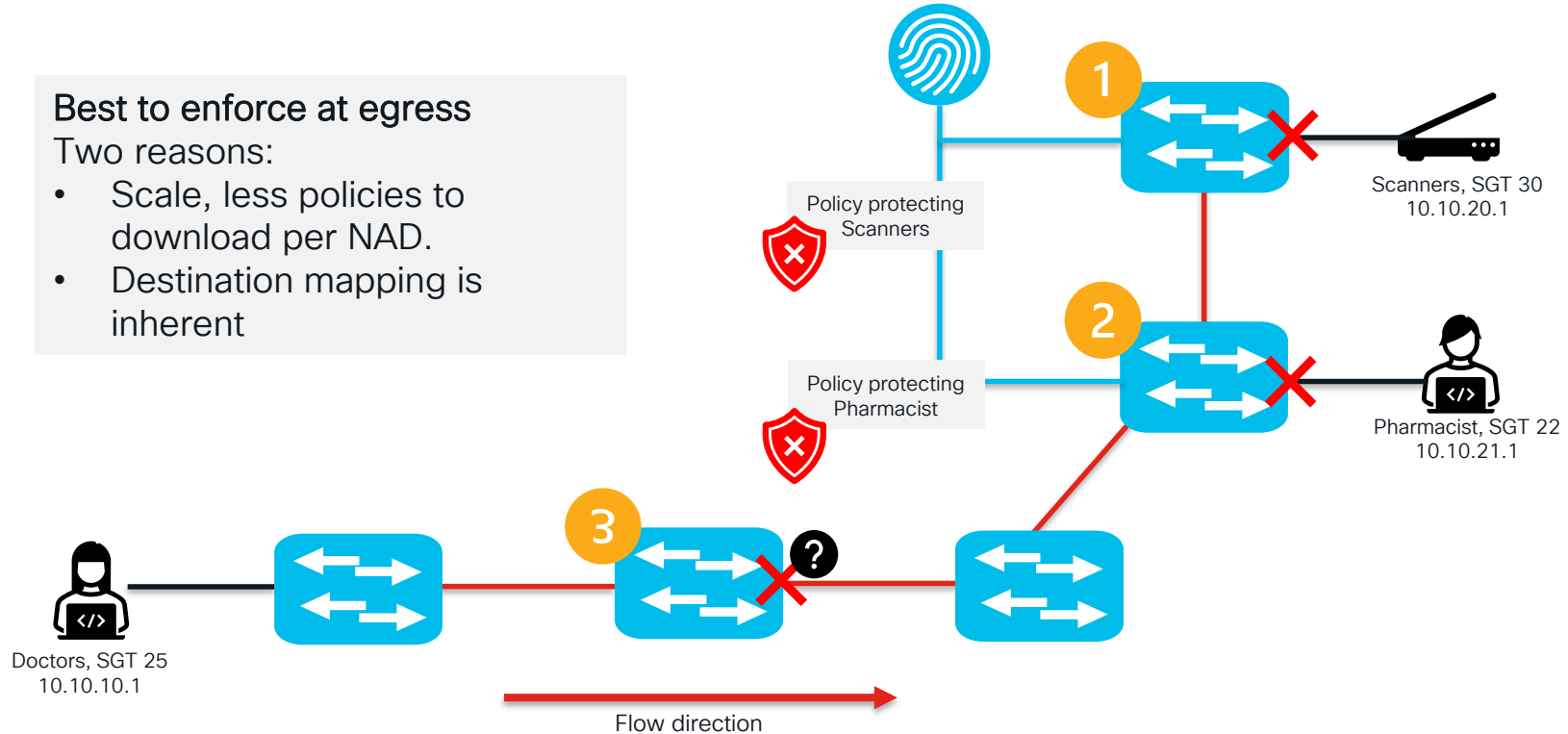


Where is best to enforce?

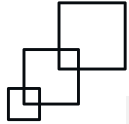
Best to enforce at egress

Two reasons:

- Scale, less policies to download per NAD.
- Destination mapping is inherent



Enforcement, troubleshooting

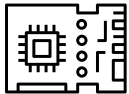


SGACL downloaded correctly

```
Switch#show cts role-based permissions
IPv4 Role-based permissions default:
    Permit IP-00

IPv4 Role-based permissions from group 30:Doctors
to group 22:Scanners:
    SGACL_01

IPv4 Role-based permissions from group 30:Doctors
to group 50:Health_servers:
    SGACL_02
```



TCAM usage

```
#show platform hardware fed active sgacl resource
usage
...
Policy Entries : 256 2 → SGACL
...
Output SGACL : 2560 9 → ACEs
```



SGACL content

```
#show access-list SGACL_01
Role-based IP access list SGACL_9151_1016-01 (downloaded)
 10 permit icmp.....1 slot in TCAM
 20 permit udp src range 5246 5247 5247.....2 slots in TCAM
 30 permit ip log.....1 slot in TCAM

#show access-list SGACL_02
Role-based IP access list SGACL_1016_9151-01 (downloaded)
 10 permit icmp
 20 permit udp dst range 5246 5247
 30 permit ip log
```

Troubleshooting tips

SGACLs downloaded correctly

#show cts role-based permissions

IPv4 Role-based permissions default:

Permit IP-00

IPv4 Role-based permissions from group 30:Doctors to group 22:Scanners:

SGACL_01

IPv4 Role-based permissions from group 30:Doctors to group 50:Health_servers:

SGACL_02

RBACL Monitor All for Dynamic Policies : FALSE

RBACL Monitor All for Configured Policies : FALSE

- NAD only downloads the bindings that it learned.
- Default action for unmatched traffic is: **Permit All**
- Monitor mode is Turned Off

Enforcement, troubleshooting



SGACL content

```
#show access-list SGACL_01
Role-based IP access list SGACL_9151_1016-01 (downloaded)
 10 permit icmp.....1 slot in TCAM
 20 permit udp src range 5246 5247 5247.....2 slots in TCAM
 30 permit ip log.....1 slot in TCAM

#show access-list SGACL_02
Role-based IP access list SGACL_1016_9151-01 (downloaded)
 10 permit icmp
 20 permit udp dst range 5246 5247
 30 permit ip log
```

TCAM Usage

```
#show platform hardware fed active sgacl resource
usage
...
Policy Entries : 256 2 → SGACL
...
Output SGACL : 2560 9 → ACEs
```

+1 Default action



More ACEs and less SGACL to improve resource utilization



Cisco Group Based Policy Platform and Capability Matrix

Enforcement, troubleshooting

Role-based counters

```
#show cts role-based counters from 30 to 22
```

```
Role-based IPv4 counters
```

From	To	SW-Denied	HW-Denied	SW-Permitted	HW-Permitted
30	22	0	1	0	22

- Ensure that counters are enabled **#cts role-based counters enabled**
- HW-Denied, HW-Permitted
 - Used in modern NADs
 - RBACL enforcement happens on the ASIC.
- SW-Denied, SW- Permitted
 - Common in NADs that lack dedicated hardware.
 - RBACL happens on CPU

Enforcement, troubleshooting

CTS Liveness Auto-test

```
#show cts server-list
```

```
CTS Server Radius Load Balance = DISABLED
```

```
Server Group Deadtime = 20 secs (default)
```

```
Global Server Liveness Automated Test Deadtime = 20 secs
```

```
Global Server Liveness Automated IDLE Time = 60 mins
```

```
Global Server Liveness Automated Test = ENABLED (default)
```

```
Installed list: CTSServerList1-0005, 2 server(s):
```

```
*Server: 10.31.126.220, port 1812, A-ID E8F71A3AE317511F27904B503414490C
```

```
Status = ALIVE
```

```
auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20  
secs
```

```
*Server: 10.31.126.222, port 1812, A-ID E8F71A3AE317511F27904B503414490C
```

```
Status = ALIVE
```

```
auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20  
secs
```

Enforcement, troubleshooting

debug radius

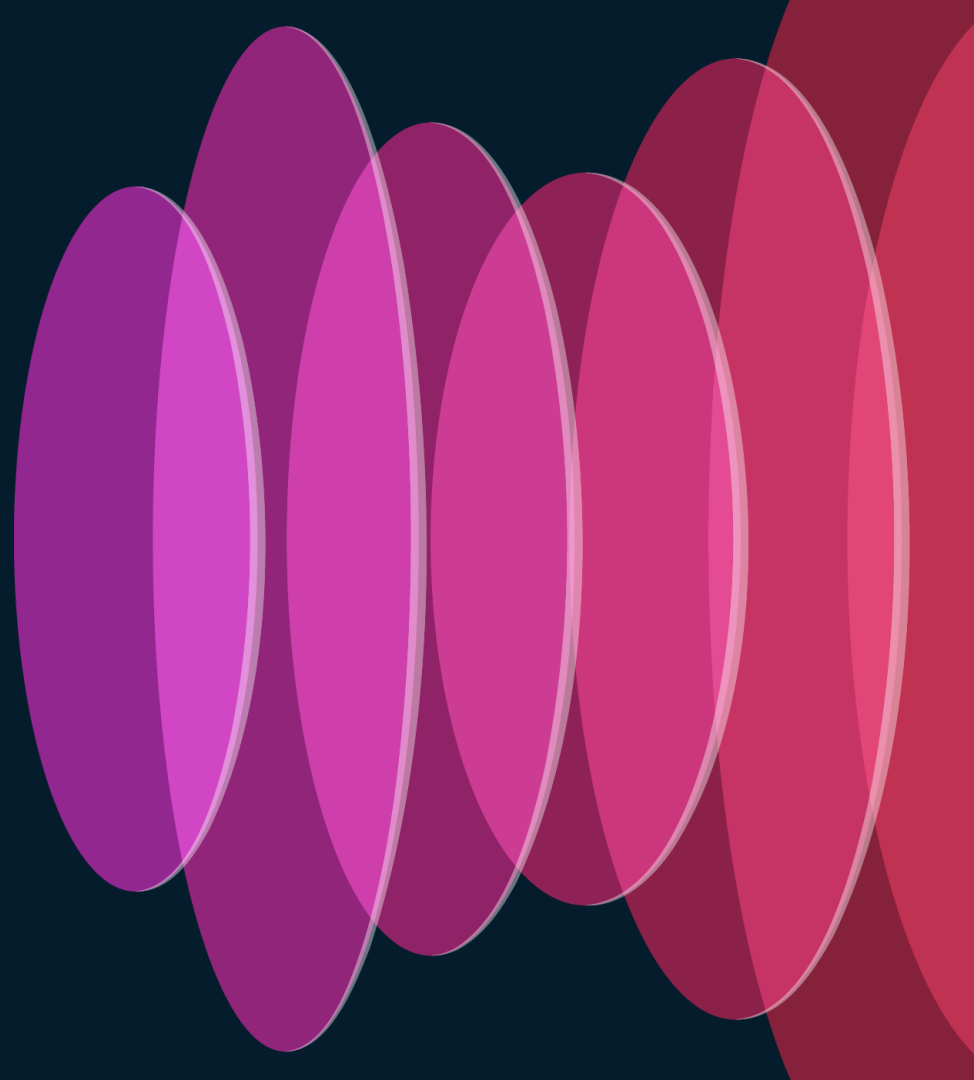
```
Mar 31 19:45:37.237: RADIUS: Vendor, Cisco [26] 211
Mar 31 19:45:37.237: RADIUS: Cisco AVpair [1] 205 "cts-pac-
opaque= "
Mar 31 19:45:37.237: RADIUS: User-Password [2] 18 *
Mar 31 19:45:37.237: RADIUS: User-Name [1] 17 "CTS-Test-
Server"
Mar 31 19:45:37.238: RADIUS: Service-Type [6] 6 Login [1]
Mar 31 19:45:37.238: RADIUS: NAS-IP-Address [4] 6 x.x.x.x
```

Radius automate-tester configuration along with CTS may impact env-data/SGACL downloads.

When the server is marked as DEAD, the switch sends radius test with user “CTS-Test-Server”

```
radius server ISE_3
address ipv4 x.x.x.x auth-port 1812 acct-port
1813
timeout 10
retransmit 3
automate-tester username RADIUS_TEST_USER
probe-on
pac key 7 <removed>
```

PxGrid Direct



PxGrid Direct in a nutshell



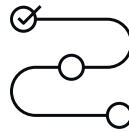
- DB entries on remote server retrieved by ISE
- You can use the fetched data in the authorization policies
- Eliminates the need to query for endpoint data during authZ

```
    ,
    "checked_in": "", {"result": [{"
      "owned_by": "joncasil",
      "operational_status": "Operational",
      "sys_updated_on": "2024-05-22 16:44:52",
      "sys_created_by": "joncasil",
      "warranty_expiration": "",
      "cpu_name": "",
      "cpu_speed": "",
      "checked_out": "",
      "maintenance_schedule": "",
      "u_segmentation_group_tag": "cts:security-group-tag=12-00",
      "managed_by": "joncasil",
      "sys_class_name": "Computer",
      "assigned_to": "joncasil@example.org",
      "department": "Marketing",
      "os": null,
      "ip_address": "10.1.16.2",
      "model_id": "Unknown",
      ...
    ]}
```

PxGrid Direct, considerations



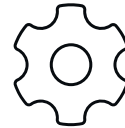
Advantage license to manage PxGrid Direct connectors



Recommended to use a maximum of 10 connectors

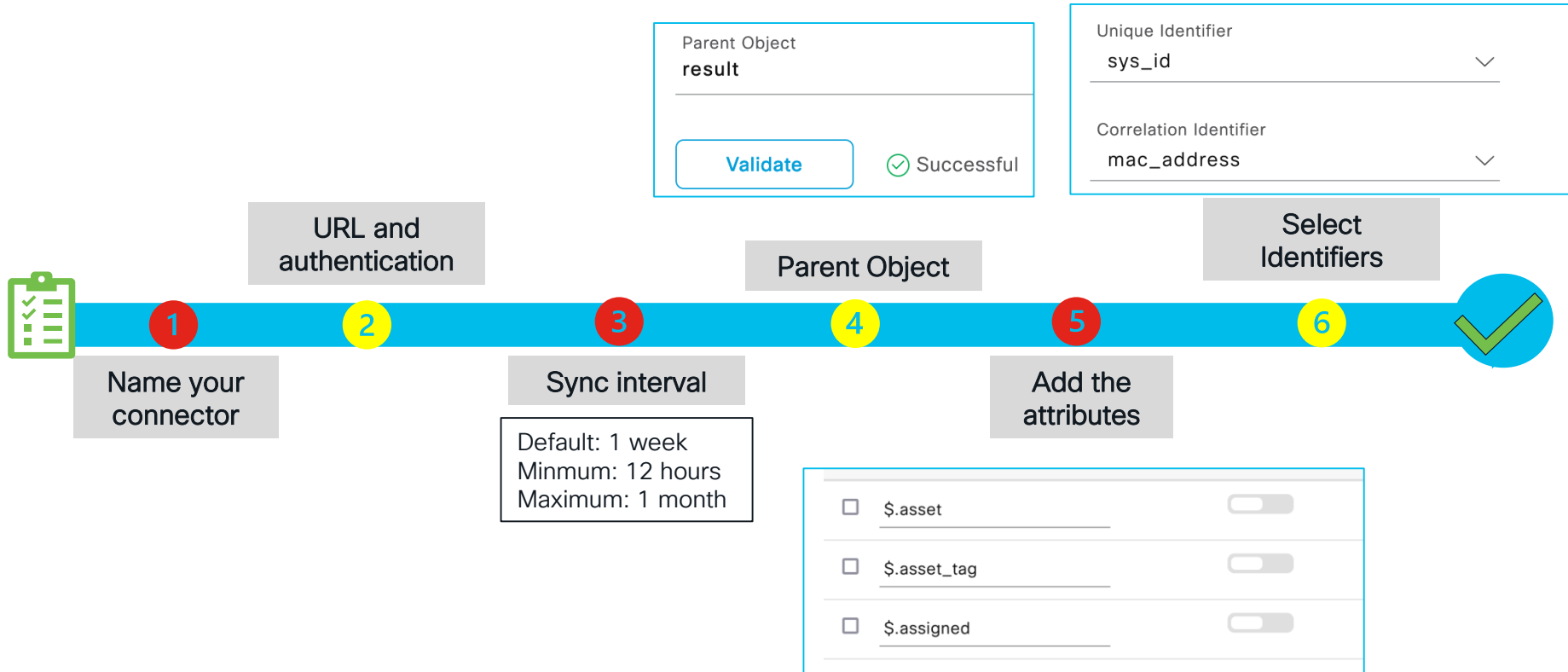


PxGrid Direct runs on the PAN and data fetched available on all PSNs



You can create/manage a connector via UI or using Open API

PxGrid Direct, configuration



PxGrid Direct Identifiers

Unique Identifier	
sys_id	▼
<hr/>	
Correlation Identifier	
mac_address	▼
<hr/>	
Version Identifier (optional)	
	▼
<hr/>	



Unique identifier is used as a tie breaker in cases where the mac address is duplicated




Correlation identifier is used as a primary key to fetch endpoint data



Version identifier is used to differentiate connector updates

Configuration summary

<input type="checkbox"/>	ⓘ Name	Scheduling	Connector T...	URL	ⓘ Total Obj...	References
<input type="checkbox"/>	Servic...	✓ Enabled	URLFETCHER	http://10.3... 	1	2



From ISE 3.2P5, 3.3P2 you can use the Sync Now feature for **on-demand** sync from PxGrid Connectors.

PxGrid Direct Dictionary

The screenshot shows the 'Dictionaries' section in the Cisco Policy Center. On the left, a navigation pane lists several categories: Posture, PROFILER, Radius, and ServiceNow. The 'ServiceNow' category is expanded and highlighted with a red box. Below it are sub-items: asset, asset_tag, and assigned. On the right, the 'View Dictionary' page for 'ServiceNow' is displayed. It shows the following details:

- Dictionary Name: ServiceNow
- Description: Dictionary for pxGrid Direct Cc
- Version: 1
- Dictionary Attribute Type: MSG_ATTR
- Dictionary: SYSTEM

Policy>Policy Elements>Dictionaries

The screenshot shows the 'Dictionary Attributes' page for the 'ServiceNow' dictionary. The breadcrumb navigation is 'Dictionaries > ServiceNow' and the page title is 'Dictionary Attributes'. A red box highlights the 'Dictionary Attributes' link in the breadcrumb. Below the title, there is a 'View' link and a table of attributes.

	Name	Internal Name	Description
<input type="checkbox"/>	asset	asset	Dictionary attribute for p...
<input type="checkbox"/>	asset_tag	asset_tag	Dictionary attribute for p...
<input type="checkbox"/>	assigned	assigned	Dictionary attribute for p...
<input type="checkbox"/>	assigned_to	assigned_to	Dictionary attribute for p...
<input type="checkbox"/>	assignment_group	assignment_group	Dictionary attribute for p...

PxGrid Direct attributes used in policy

Authorization Policy(13)

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	PxGrid Direct	ServiceNow-assigned_to EQUALS cisco.com	SNOW	Select from list	0	

AuthZ conditions can use PxGrid Direct attributes

Authz profile can assign PxGrid Direct attributes

Advanced Attributes Settings

Cisco:cisco-av-pair = u_segmentation_group_tag

Attributes Details

Access Type = ACCESS_ACCEPT

cisco-av-pair = u_segmentation_group_tag

Visibility


Authentication BYOD Compliance Compromised Endpoints Endpoint Classification Guest Vulnerable Endpoints Har


pxGrid Direct Endpoints

Connector · ServiceNow

Rows/Page 1 << < 1

This window lists the endpoint attribute data that is fetched from pxGrid Direct Connectors. Click the correlation ID for an endpoint to view or download the endpoint details.
To create a new pxGrid Director Connector or to update existing connector configurations, go to the [pxGrid Direct Connectors](#) window.



Correlation ID	Unique ID	Version ID	Connector Name
 Correlation ID	Unique ID	Version ID	Connector Name
DE:AD:BE:EF:12:34	0009ef70dbc01101f0f174b13961997		ServiceNow

Details

0009ef70dbc01101f0f174b13961997

install_date:

install_status: SNtoDataMartJon.Casil

internet_facing: true

invoice_number:

ip_address: 10.31.126.183

justification:

last_discovered:

lease_id:

life_cycle_stage:

Context Visibility > Endpoints > pxGrid Direct Endpoints

PxGrid Direct, troubleshooting



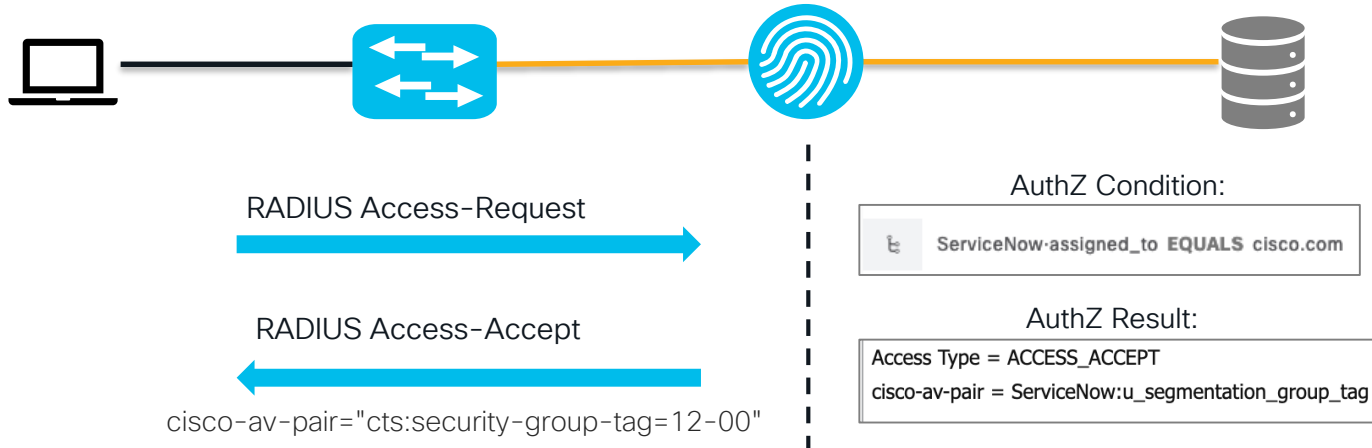
```
#show logging application  
pxgriddirect-service.log
```

Contains information related to whether fetched endpoint data has been received and saved to the Cisco ISE database.

```
#show logging application  
pxgriddirect-connector.log
```

Contains information that indicate whether a pxGrid Directed connector is successfully added to Cisco ISE.

Assign SGT with PxGrid Direct



Attribute previously imported from external DB

```
sys_updated_by: "joncasil"  
sys_updated_on: "2024-03-11 19:44:52"  
u_segmentation_group_tag: "cts:security-group-tag=0020-00"
```

Considerations



DO assign the SGT from the authZ profile
DO NOT assign the SGT from the policy



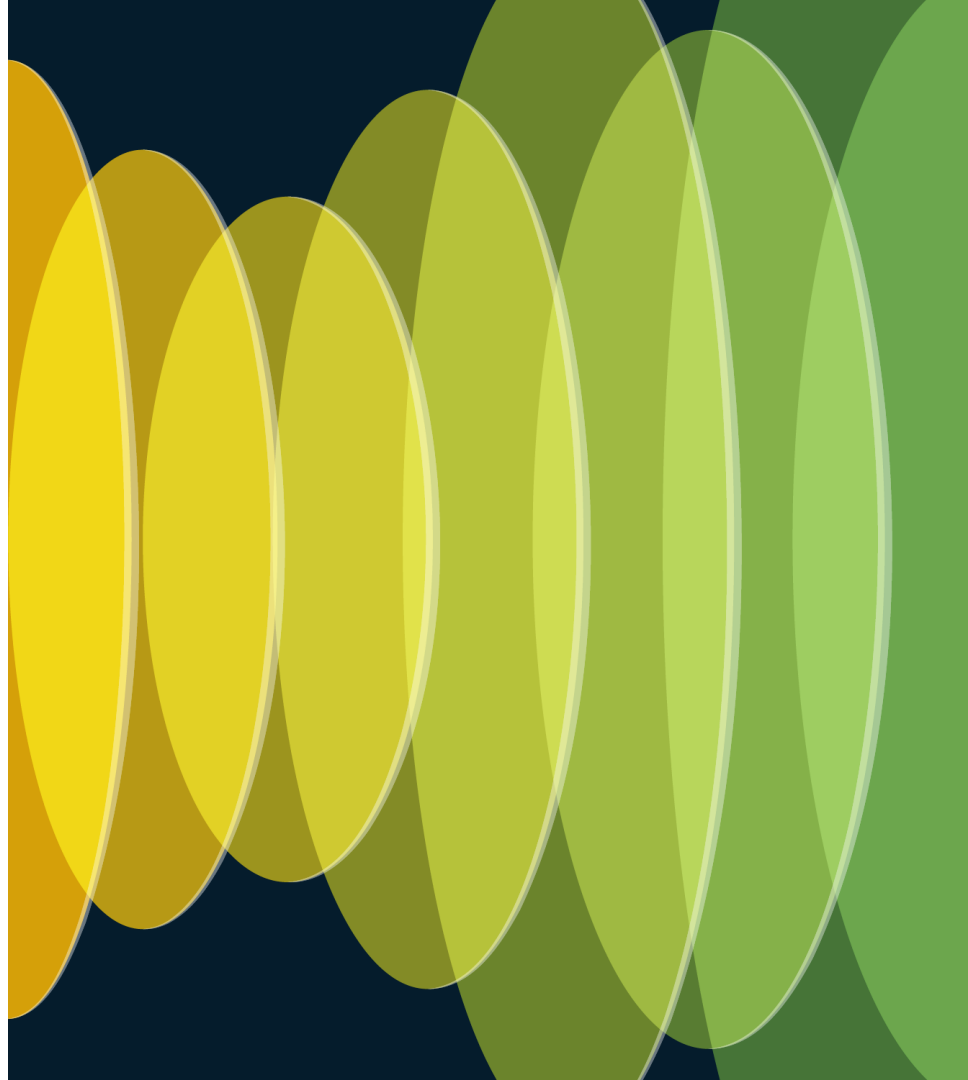
Radius Live log

22037	Authentication Passed	1
15036	Evaluating Authorization Policy	0
15048	Queried PIP - ServiceNow.assigned_to	46
15016	Selected Authorization Profile - SNOW	9
15048	Queried PIP - Network Access.EndPointMACAddress	19
15048	Queried PIP - ServiceNow.u_segmentation_group_tag	4
24209	Looking up Endpoint in Internal Endpoints IDStore - DE:AD:BE:EF:12:34	5
24211	Found Endpoint in Internal Endpoints IDStore	5
11002	Returned RADIUS Access-Accept	

Result	
UserName	DE:AD:BE:EF:12:34
User-Name	DE-AD-BE-EF-12-34
Class	CACS:0a1f7eb5qBB/ uxMVp_Oi8l6kZeWwDIbdnCuNotKtPtTQvSh6DN4:ise33a/ 502160790/16
cisco-av-pair	cts:security-group-tag=0020-00

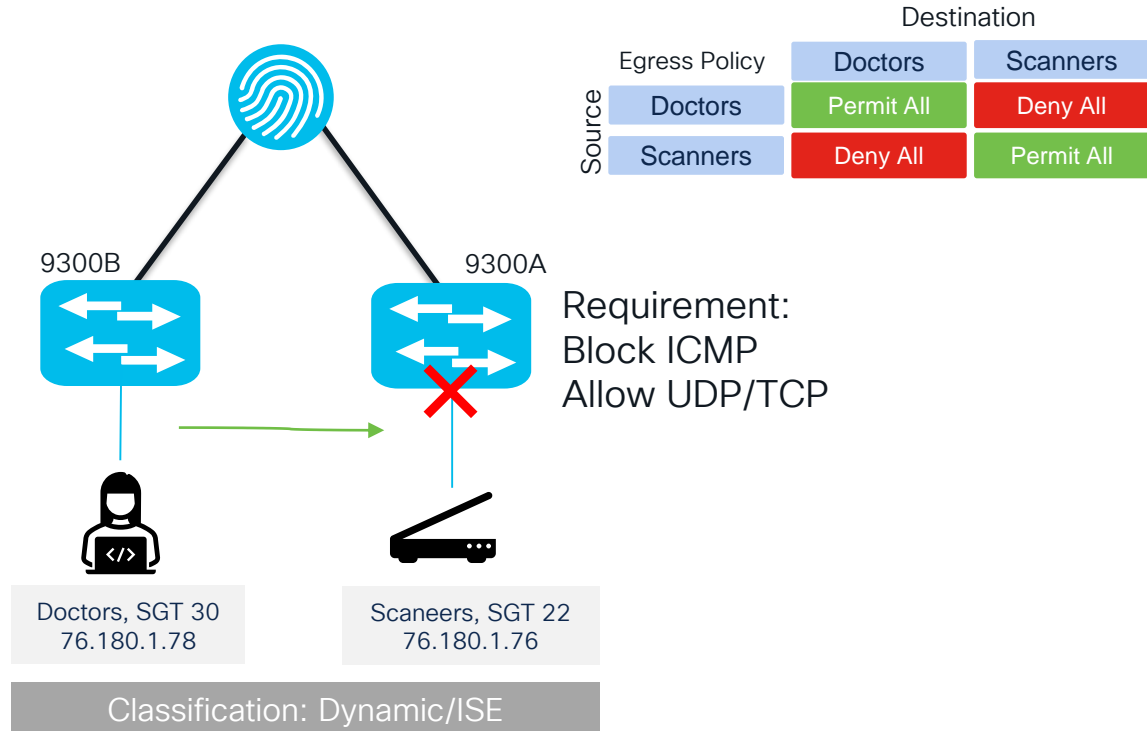
Demo

CISCO *Live!*



Use case

SGT	
Doctors	30
Scanners	22



Parent Object

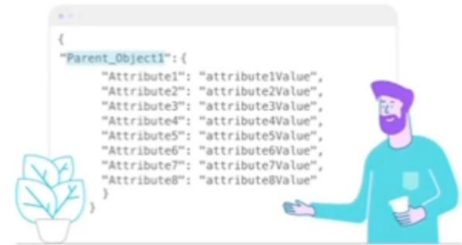
Configure the JSON data object that must be used to search for the rest of the attributes. You can read more information and example at [Page Level Help](#).

Parent Object
result

✓ Successful

```

"asset": "unknown",
"asset_tag": "",
"assigned": "",
"assigned_to": "joncasil@cluslab.com",
"assignment_group": "",
"attestation_score": "",
"attested": "false",
"attested_by": "",
"attested_date": "",
"attributes": "",
"can_print": "false",
"category": "Hardware",
"cd_rom": "false",
"cd_speed": "",
"change_control": "",
"chassis_type": null,
"checked_in": "",
"checked_out": "",
    
```



- Bookmarks
- Dashboard
- Context Visibility
- Operations
- Policy
- Administration**
- Work Centers
- Interactive Features

- Welcome
- Connector Definition
- URL
- Schedule
- Parent Object
- Attributes
- Identifiers
- 8 Summary**

Summary

Connector Definition [Edit](#)

Name: ServiceNow
Connector type: URLFETCHER

URL [Edit](#)

URL: http://10.31.126.232:5000/endpoints
Authentication: Successful

Set Up Synchronization Schedule [Edit](#)

SCHEDULE FULL SYNC
Interval: 1 WEEKS
Start Date: 2024-05-24
Start Time: 04:30:00

- Bookmarks
- Dashboard
- Context Visibility
- Operations
- Policy
- Administration**
- Work Centers
- Interactive Features

- Welcome
- Connector Definition
- URL
- Schedule
- Parent Object
- Attributes
- Identifiers
- 8 Summary**

Summary

Connector Definition [Edit](#)

Name: ServiceNow
Connector type: URLFETCHER

URL [Edit](#)

URL: http://10.31.126.232:5000/endpoints
Authentication: Successful

Set Up Synchronization Schedule [Edit](#)

SCHEDULE FULL SYNC
Interval: 1 WEEKS
Start Date: 2024-05-24
Start Time: 04:30:00

Bookmarks | Dashboard | Context Visibility | Operations | **Policy** | Administration | Work Centers | Interactive Features

Dictionarys | Conditions | Results

System Dictionarys

Selected 0 Total 51

View | All

Name	Description
<input type="checkbox"/> ACIDEX	Profiler ACIDEX dictionary
<input type="checkbox"/> ACTIVEDIRECTORY_PROBE	Profiler ACTIVEDIRECTORY_PROBE dictionary
<input type="checkbox"/> APIC	Dictionary for APIC
<input type="checkbox"/> CDP	Profiler CDP dictionary
<input type="checkbox"/> CERTIFICATE	Cisco Certificate Dictionary
<input type="checkbox"/> CUSTOMATTRIBUTE	CustomAttribute Dictionary
<input type="checkbox"/> CWA	Cisco CWA Dictionary
<input type="checkbox"/> CiscoPEP	Cisco PEP Dictionary
<input type="checkbox"/> DEVICE	Cisco Device Dictionary
<input type="checkbox"/> DHCP	Profiler DHCP dictionary
<input type="checkbox"/> ENDPOINTPURGE	Profiler ENDPOINTPURGE dictionary
<input type="checkbox"/> EPS	EPS Dictionary

Dictionarys

network Condition

NMAP

NMAPExtension

Normalised Radius

PassiveID

Posture

PROFILER

Radius

ServiceNow

- asset
- asset_tag
- assigned
- assigned_to
- assignment_group
- attestation_score
- attested

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

▼ Authorization Policy(14)

Status	Rule Name	Conditions	Results			Hits	Actions
			Profiles	Security Groups			
+	Search						
+	<u>ServiceNow - Devices</u>	ServiceNow-assigned_to CONTAINS cluslab.com	ScannersAccess	Select from list	4		
+	<u>Doctors</u>	Network Access-Device IP Address EQUALS 10.31.127.124	PermitAccess	Doctors	5		
+	<u>Wireless Block List Default</u>	AND Wireless_Access IdentityGroup-Name EQUALS Endpoint Identity Groups:Blocked List	Block_Wireless_Access	Select from list	0		
+	<u>Profiled Cisco IP Phones</u>	IdentityGroup-Name EQUALS Endpoint Identity Groups:Profiled:Cisco-IP-Phone	Cisco_IP_Phones	Select from list	0		
+	<u>Profiled Non Cisco IP Phones</u>	Non_Cisco_Profiled_Phones	Non_Cisco_IP_Phones	Select from list	0		
+	<u>Unknown Comolance Redir</u>	Network_Access_Authentication_Passed	Cisco_Tomorrow_Colored	Select from list	0		

- Bookmarks
- Dashboard
- Context Visibility
- Operations
- Policy**
- Administration
- Work Centers
- Interactive Features

- Dictionarys
- Conditions
- Results**
- Authentication
- Authorization
 - Authorization Profiles
 - Downloadable ACLs
- Profiling
- Posture
- Client Provisioning

Common tasks

- Voice Domain Permission
- Web Redirection (CWA, MDM, NSP, CPP)
- Auto Smart Port

Advanced Attributes Settings

Cisco:cisco-av-pair = ServiceNow:u_segmentati...

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = ServiceNow:u_segmentation_group_tag

Overview

Event	5200 Authentication succeeded
Username	8C:16:45:11:23:3A
Endpoint Id	8C:16:45:11:23:3A ⓘ
Endpoint Profile	Unknown
Authentication Policy	Default >> MAB
Authorization Policy	Default >> ServiceNow - Devices
Authorization Result	ScannersAccess

Authentication Details

Source Timestamp	2024-05-24 04:17:26.315
Received Timestamp	2024-05-24 04:17:26.315
Policy Server	ise33a
Event	5200 Authentication succeeded
Username	8C:16:45:11:23:3A
User Type	Host
Endpoint Id	8C:16:45:11:23:3A
Calling Station Id	8C-16-45-11-23-3A

Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request	
11017	RADIUS created a new session	0
11027	Detected Host Lookup UseCase (Service-Type = Call Check (10))	1
15049	Evaluating Policy Group	0
15008	Evaluating Service Selection Policy	0
15041	Evaluating Identity Policy	4
15048	Queried PIP - Normalised Radius.RadiusFlowType	1
15013	Selected Identity Source - Internal Endpoints	16
24209	Looking up Endpoint in Internal Endpoints IDStore - 8C:16:45:11:23:3A	0
24211	Found Endpoint in Internal Endpoints IDStore	2
22037	Authentication Passed	0
15036	Evaluating Authorization Policy	0
15048	Queried PIP - ServiceNow.assigned_to	39
15016	Selected Authorization Profile - ScannersAccess	4
15048	Queried PIP - Network Access.EndPointMACAddress	21
15048	Queried PIP - ServiceNow.u_segmentation_group_tag	2
24209	Looking up Endpoint in Internal Endpoints IDStore - 8C:16:45:11:23:3A	2
24211	Found Endpoint in Internal Endpoints IDStore	0
11002	Returned RADIUS Access-Accept	1

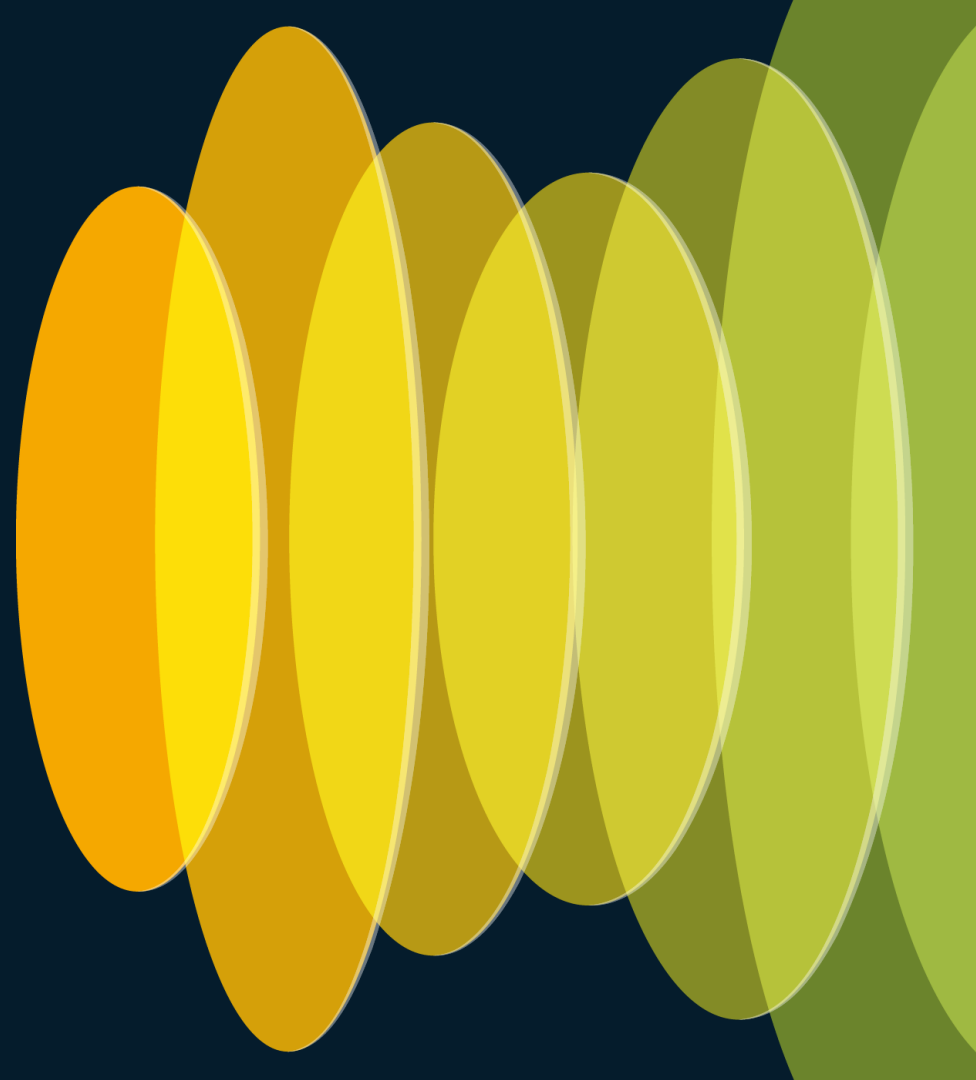
Result

UserName	8C:16:45:11:23:3A
User-Name	8C-16-45-11-23-3A
Class	CACS:867F1F0A0000001BA8D0FDB1:ise33a/504489529/174
cisco-av-pair	cts:security-group-tag=0016-02
cisco-av-pair	profile-name=Unknown
LicenseTypes	Essential license consumed.

Session Events

2024-05-24 04:17:28.237	RADIUS Accounting watchdog update
2024-05-24 04:17:26.33	RADIUS Accounting start request
2024-05-24 04:17:26.315	Authentication succeeded

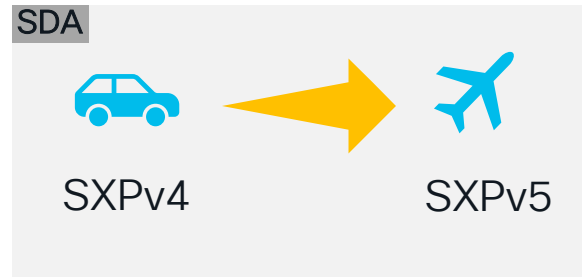
Wrap up time



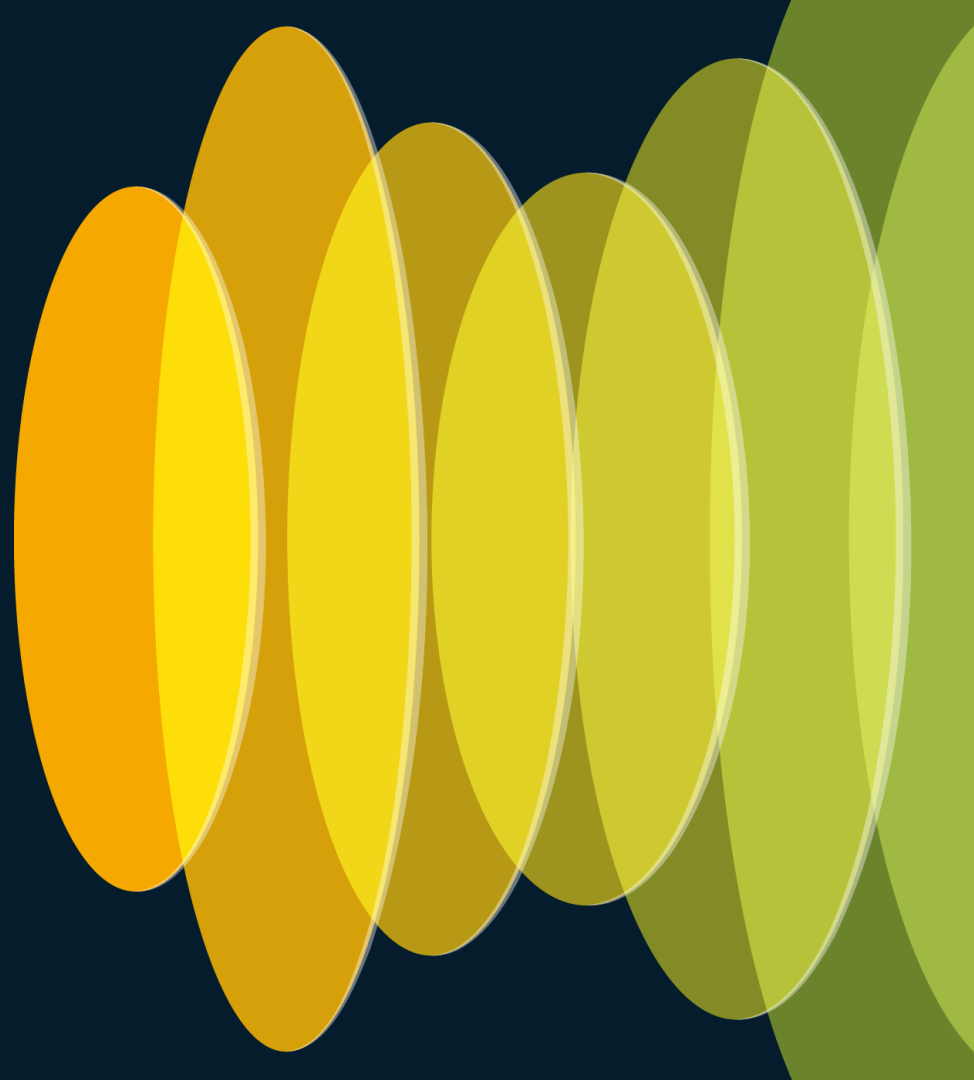
Key Takeaways

- Making Cisco TrustSec easy to manage and deploy.
- SXPv5 leverages VRF aware communication, enabling a single SXP connection to handle all VNs.
- PxGrid Direct provides flexibility and accuracy to your segmentation strategy leveraging information from CMDBS.
 - PxGrid Direct eliminates the need to query for endpoint attribute data each time that requires authorization.

The path forward



Q&A



Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.



Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.



Level up and earn **exclusive prizes!**

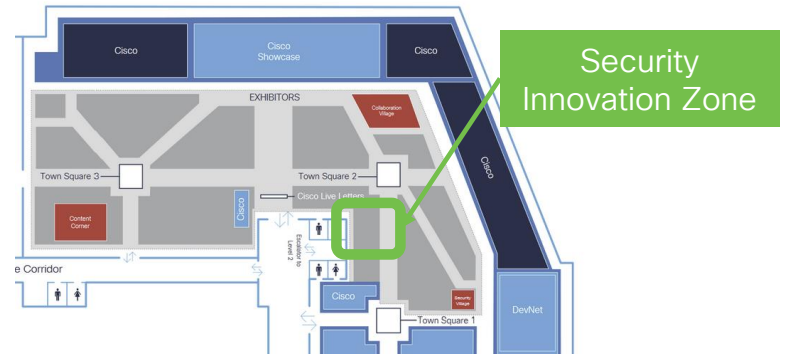


Complete your surveys in the **Cisco Live mobile app.**

Continue your education

CISCO *Live!*

- Visit us at the Security Innovation Zone for in-depth demos and workshops ([Booth #4435](#))





The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive