The bridge to possible

Cross-Domain Integration: Troubleshooting Cisco SD-Access - SD-WAN Integration

Mariusz Kaźmierski, Principal Engineer

Cisco Webex App

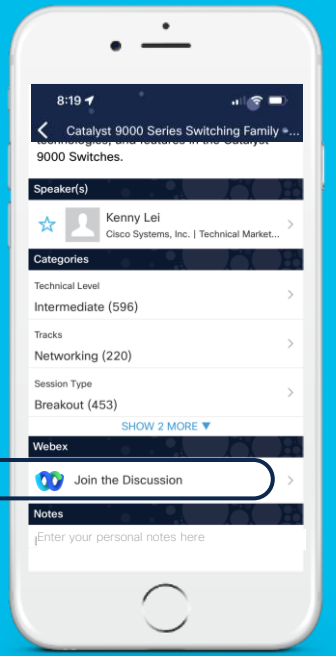
Questions?

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 until February 24, 2023.



Agenda

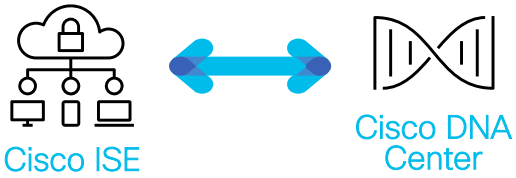
- SD-Access / SD-WAN: Basics
- Cross-Domain: Supported Designs
- Independent Domain
- Integrated Domain
- Network Troubleshooting
- Summary

SD-Access / SD-WAN: Basics

cisco Live!

SD-Access (SDA) - basics

Software



Cisco DNA Center

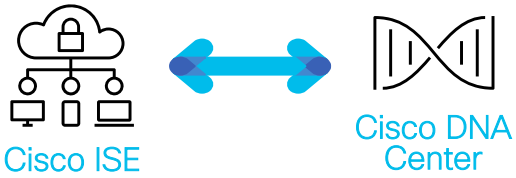
Orchestrator responsible for intent-based automation and assurance in Campus Network.

Cisco Identity Services Engine (ISE)

Engine that provides a dynamic end-point to SGT group mapping and policy definition.

SD-Access (SDA) - basics

Software



Cisco DNA Center

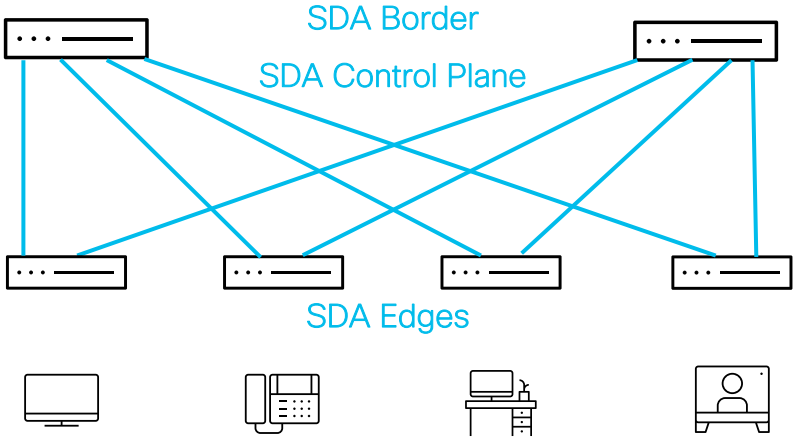
Orchestrator responsible for intent-based automation and assurance in Campus Network.

Cisco Identity Services Engine (ISE)

Engine that provides a dynamic end-point to SGT group mapping and policy definition.

SDA Fabric

VXLAN / LISP



SDA Border

Fabric device that connects SDA Fabric with the external network.

SDA Control Plane

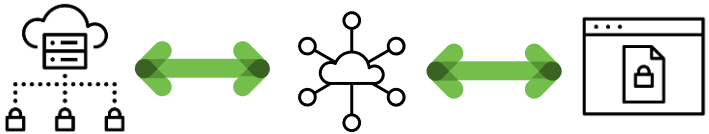
Fabric device that governs control-plane operations in the fabric.

SDA Edge

Fabric device to which end-points are connected to.

SD-WAN - basics

Software



vManage

management-plane and single pane of glass for day0, day1 and day2 operations in SD-WAN.

vBond

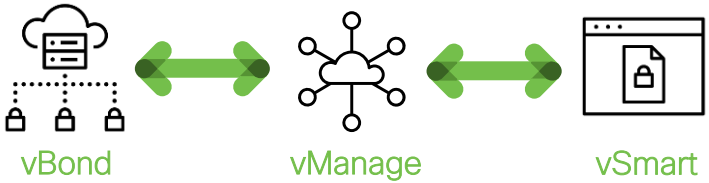
orchestration-plane responsible for on-boarding (Zero Touch Provisioning) new devices into SD-WAN fabric.

vSmart

control-plane responsible for applying and enforcing configured policies in SD-WAN fabric.

SD-WAN - basics

Software



vManage

management-plane and single pane of glass for day0, day1 and day2 operations in SD-WAN.

vBond

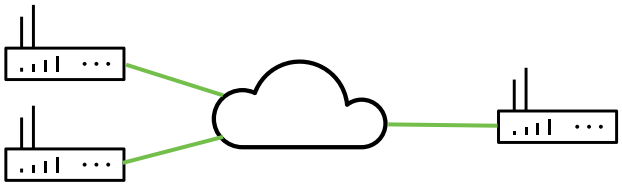
orchestration-plane responsible for on-boarding (Zero Touch Provisioning) new devices into SD-WAN fabric.

vSmart

control-plane responsible for applying and enforcing configured policies in SD-WAN fabric.

SD-WAN Fabric

IPSEC / OMP



cEdge

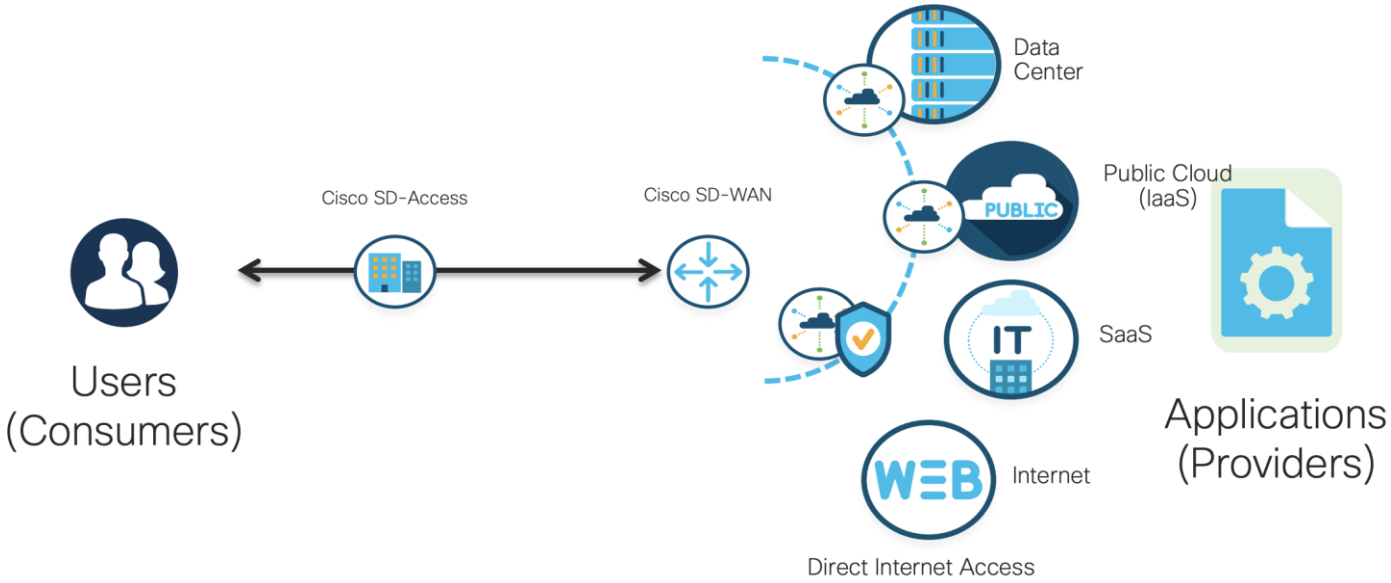
data plane device that forwards packets based on decisions received from the control plane (vSmarts).

SD-Access – SD-WAN: Comparison

Function	SD-Access	SD-WAN
Management	Cisco DNA Center	vBond – UI vManage – NMS
Control Plane	LISP	vSmart (OMP)
Data Plane Underlay	Based on RLOC	Based in TLOC
Data Plane Overlay	VXLAN	IPSec

Cross-Domain: Supported Designs

Integration Goals – WHY?



Integration Goals – WHY?

1) **Ensure** micro- and macro-segmentation across the whole enterprise.

2) **Use** consistent end-to-end group-based policies.

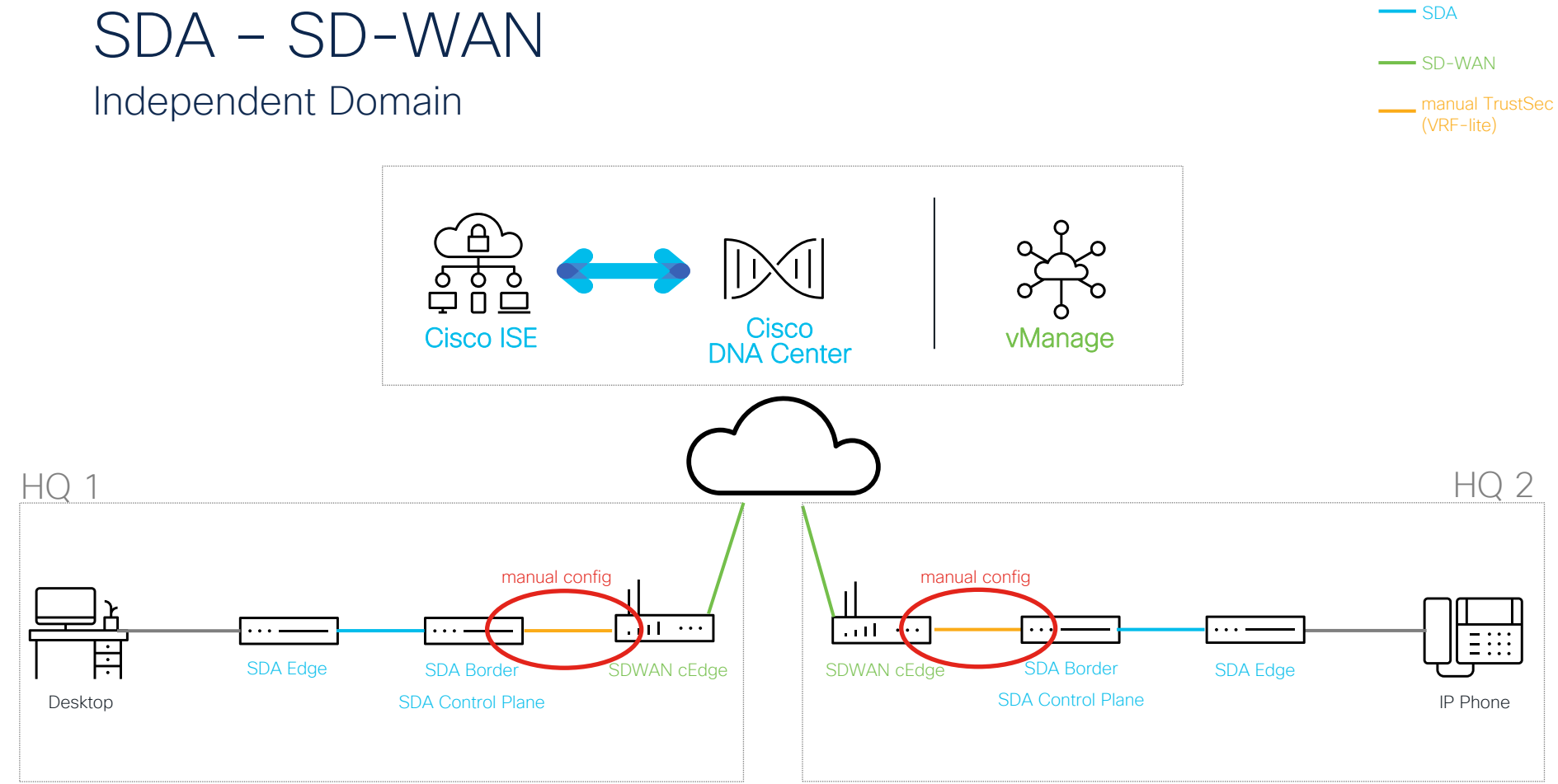
3) **Leverage** intelligent routing between different branch offices.

4) **Automate** new site deployments.

5) **Monitor** network via single pane of glass (integrated domain).

SDA – SD-WAN

Independent Domain

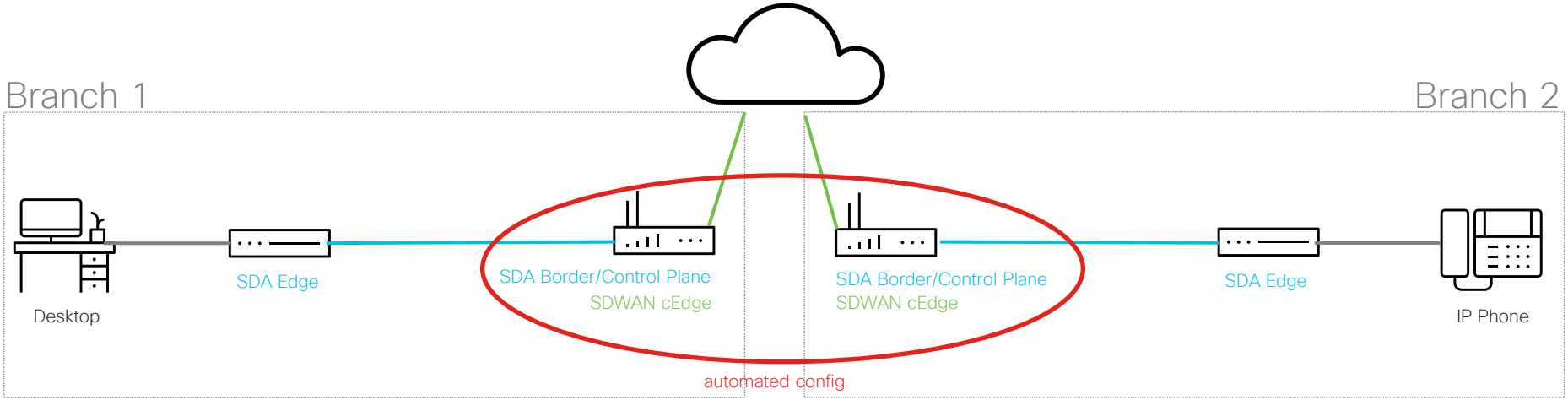


SDA – SD-WAN

Integrated Domain

SDA

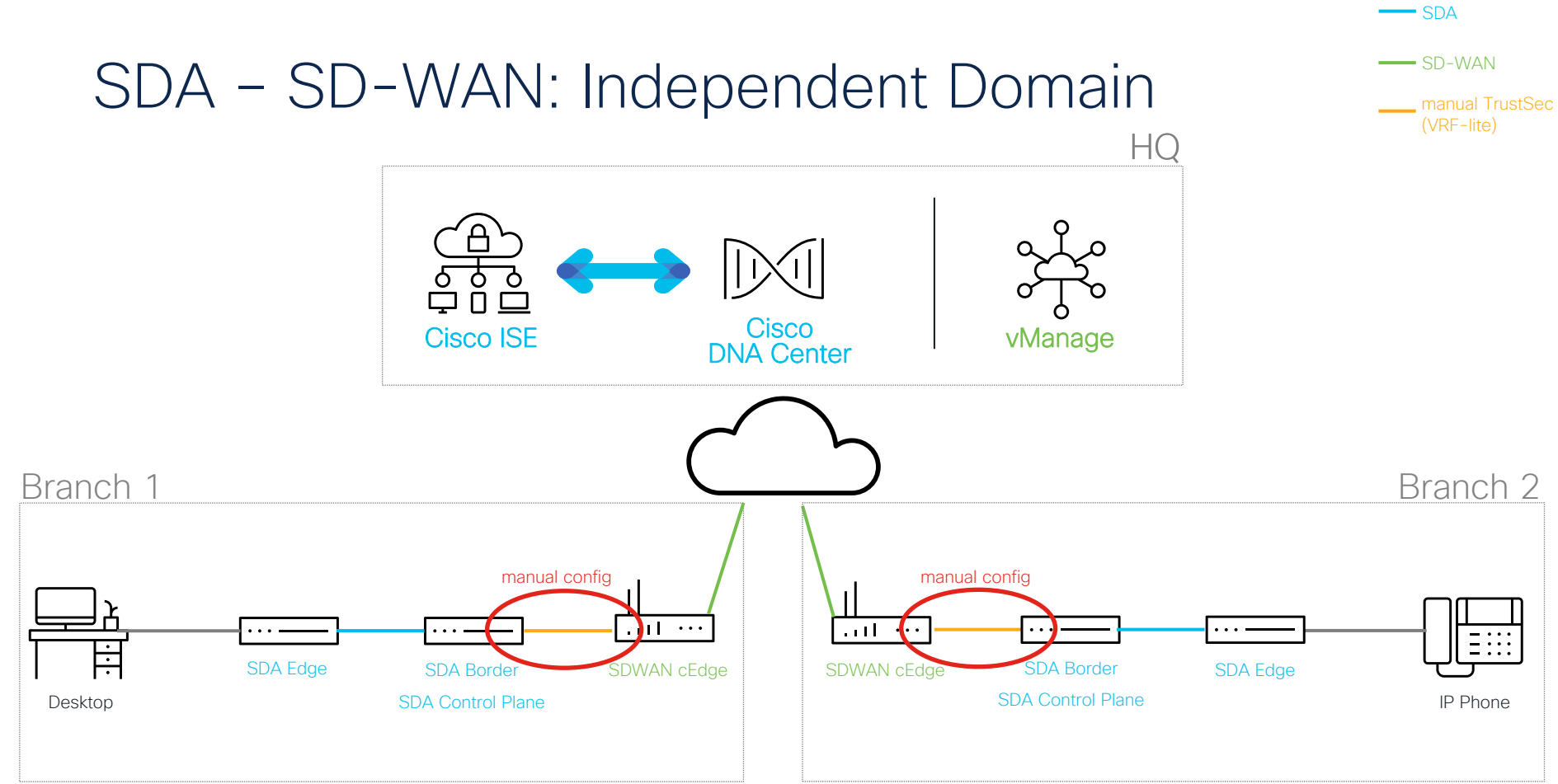
SD-WAN



Independent Domain

Independent Domain
Introduction

SDA – SD-WAN: Independent Domain



SDA – SD-WAN: Independent Domain

Interoperability:

- SD-WAN cEdges perform only SD-WAN functionality,
- SD-WAN cEdges are managed and provisioned by SD-WAN controllers,
- SDA devices perform only SDA functionality,
- SDA devices are managed and provisioned by Cisco DNA Center,
- Security details (SGT values) are carried over between both solutions in data-plane (Ethernet / CMD frame).

SDA – SD-WAN: Independent Domain

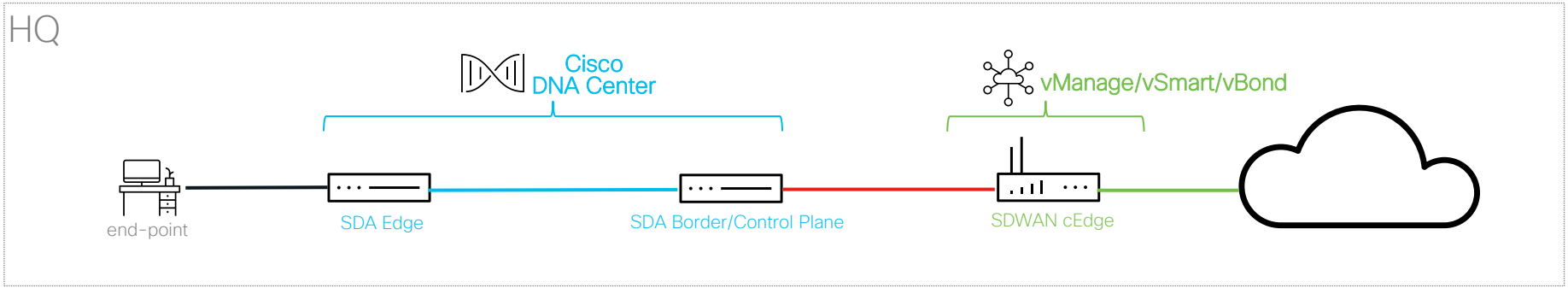
Main characteristics:

- very flexible as both solutions are loosely coupled together & can be managed independently,
- there are no strict software version requirements (strict compatibility matrix),
- It can be implemented on new or existing SDA site,
- it requires two devices (one for SDA, one for SD-WAN),
- It requires additional configuration (CMD / VRF-Lite) to exchange security tags.

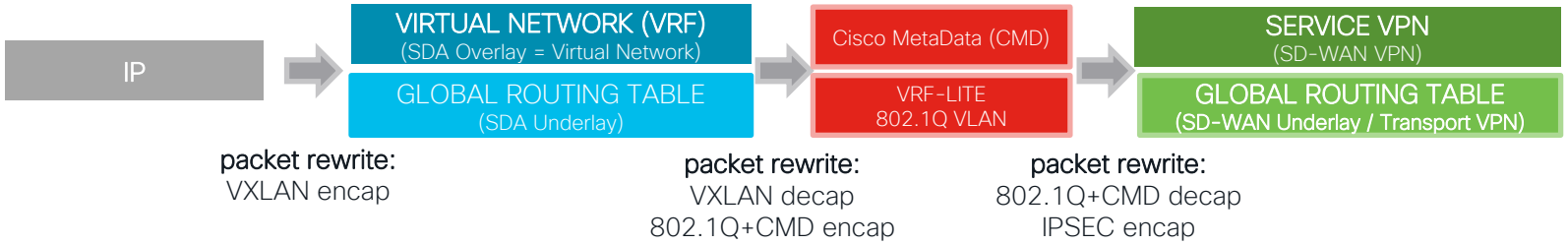
Common Use Case:

Mainly used in HQ / large sites where complex traffic rules are often needed.

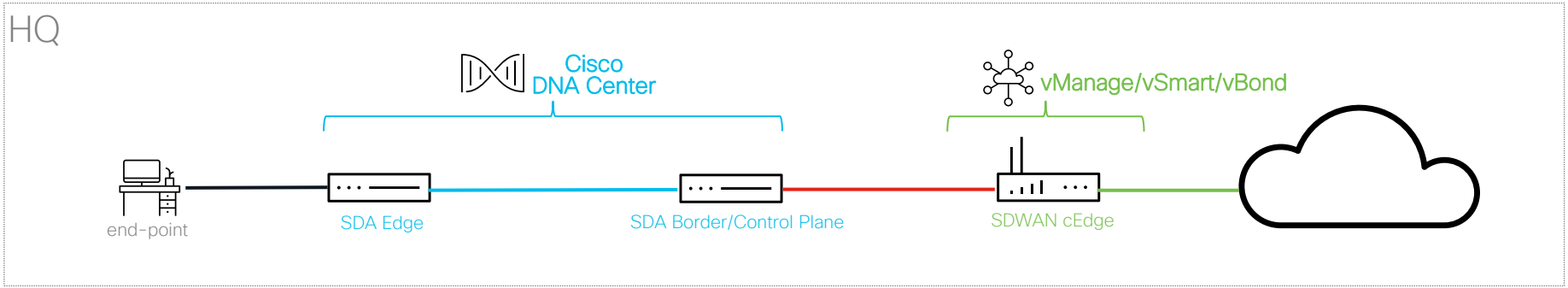
Independent Domain



DATA-PLANE

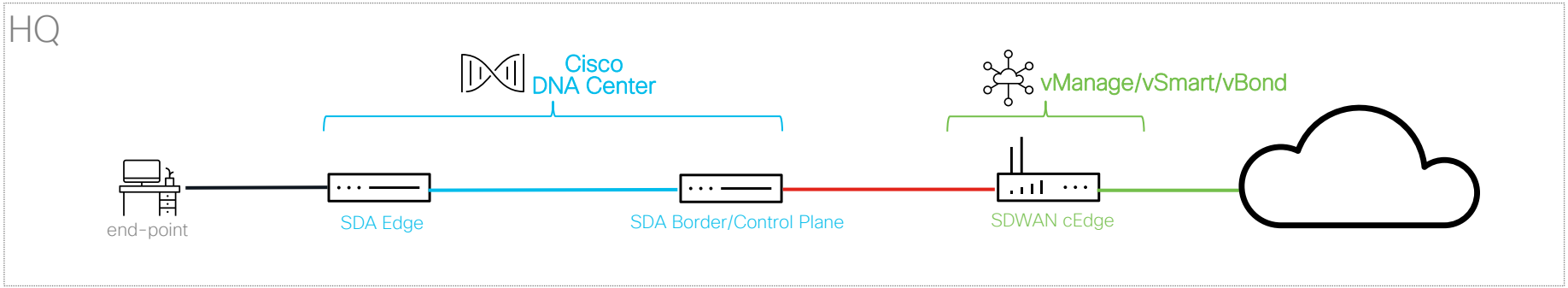


Independent Domain



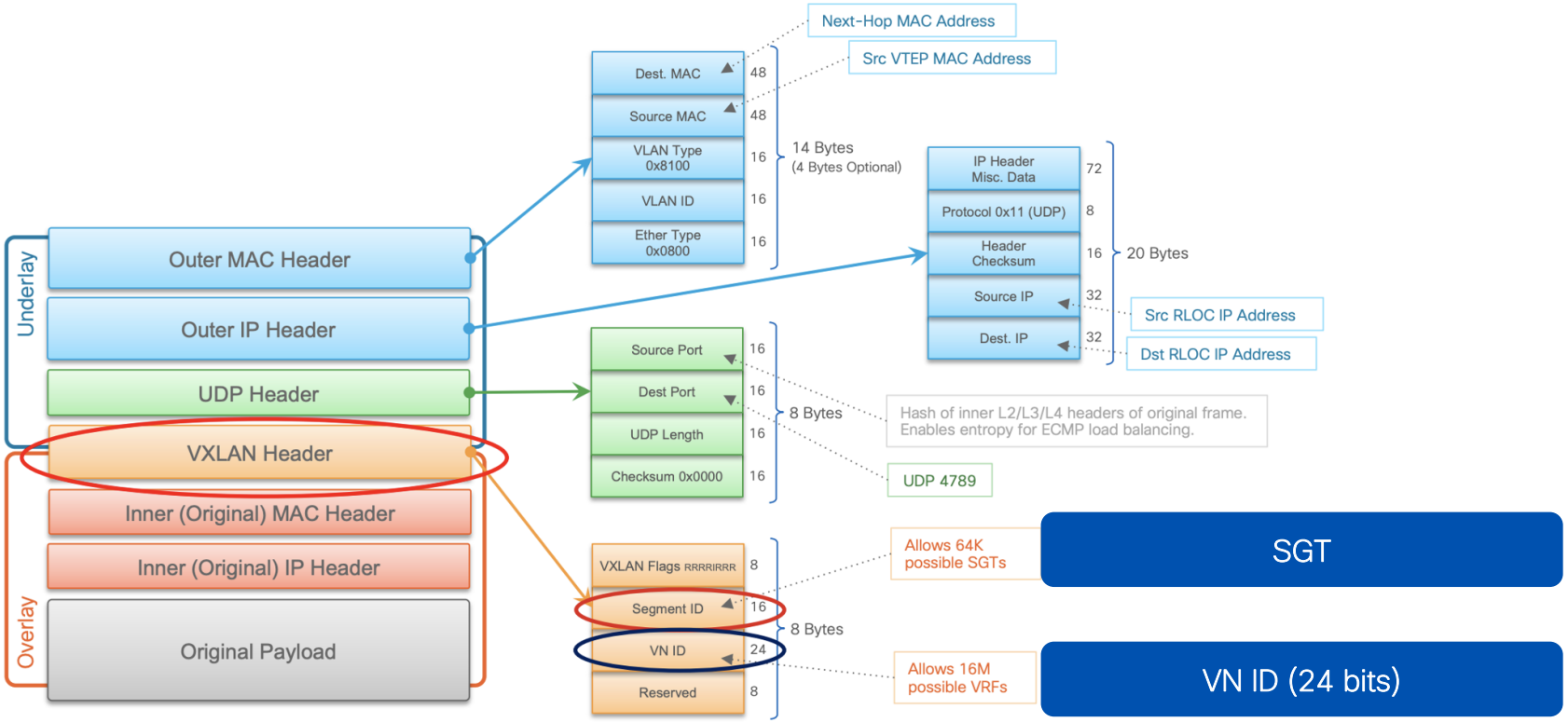
CONTROL-PLANE (overlay)

Independent Domain

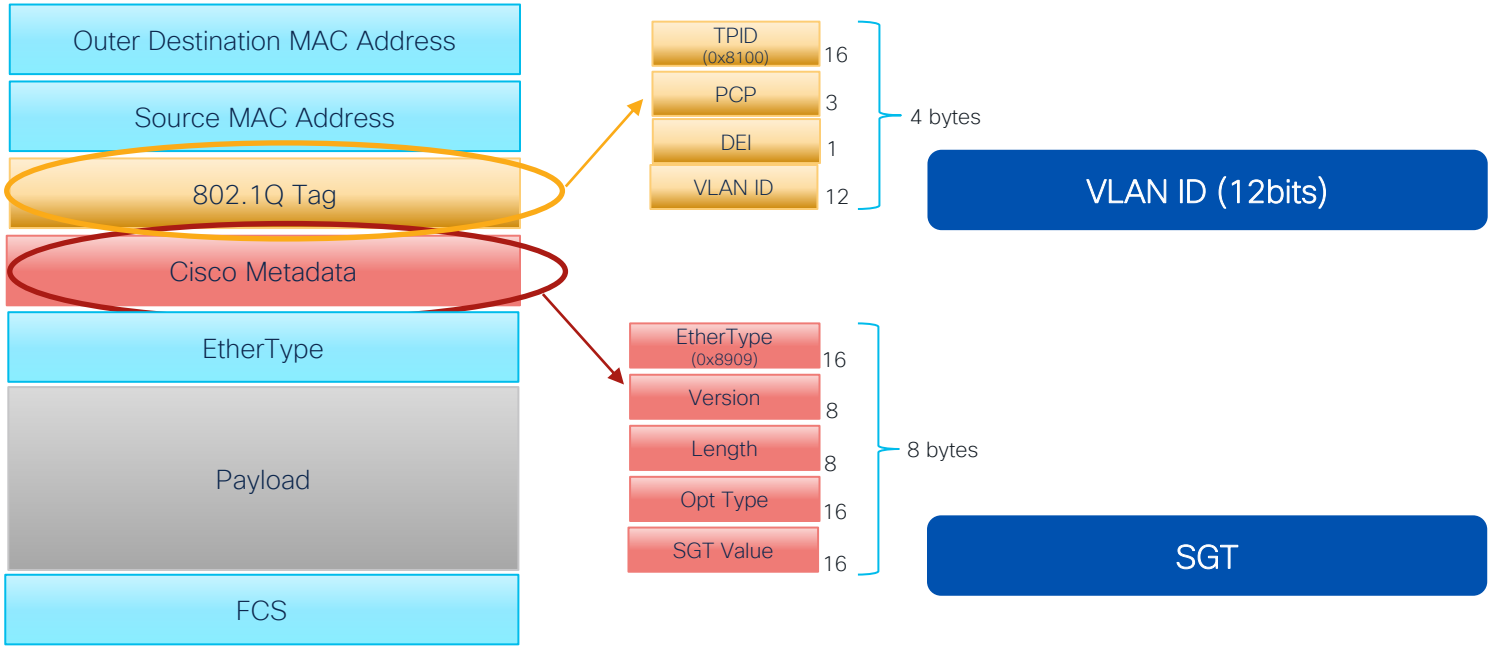


SECURITY-PLANE

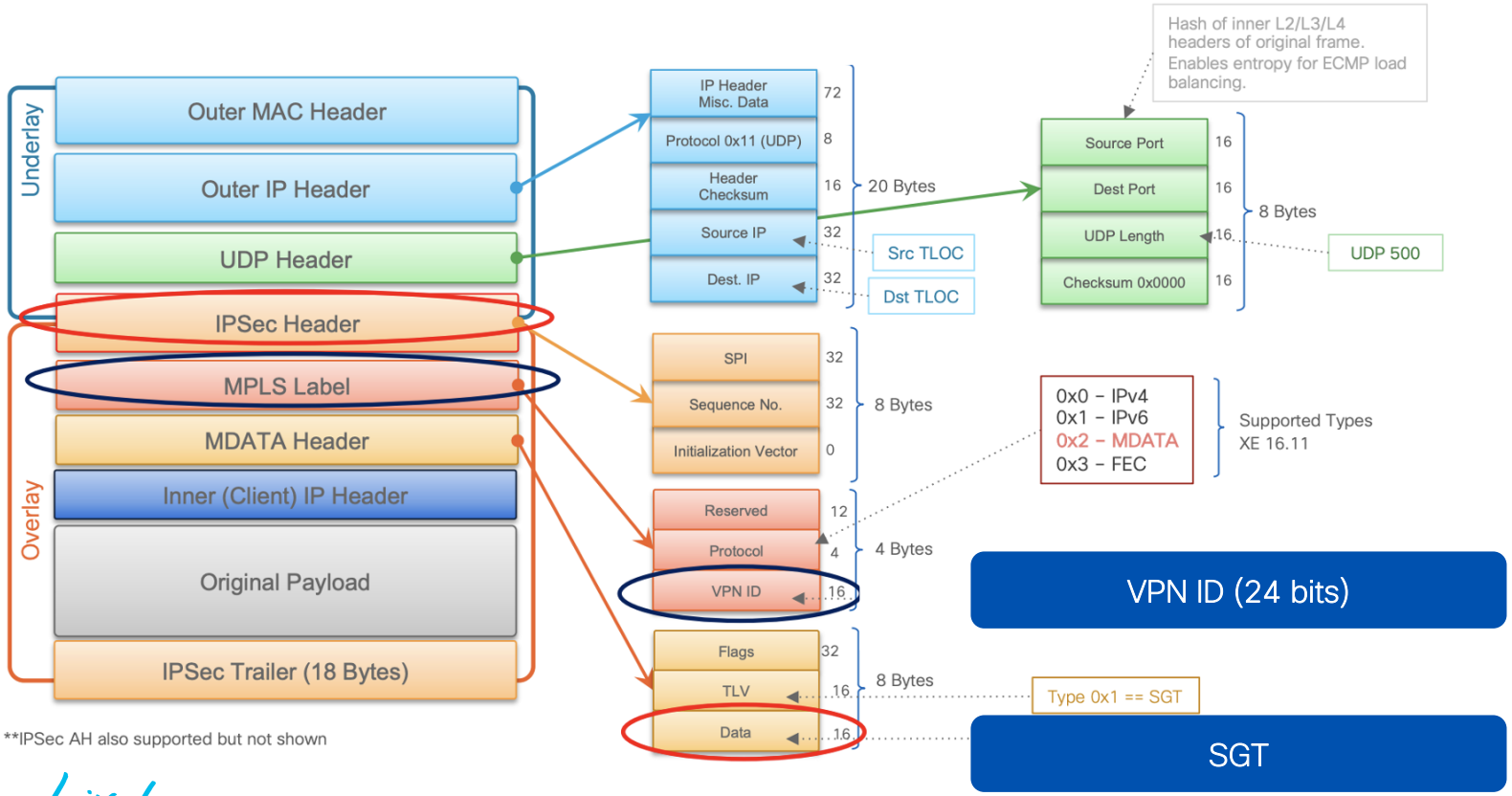
SDA: VXLAN Encapsulation



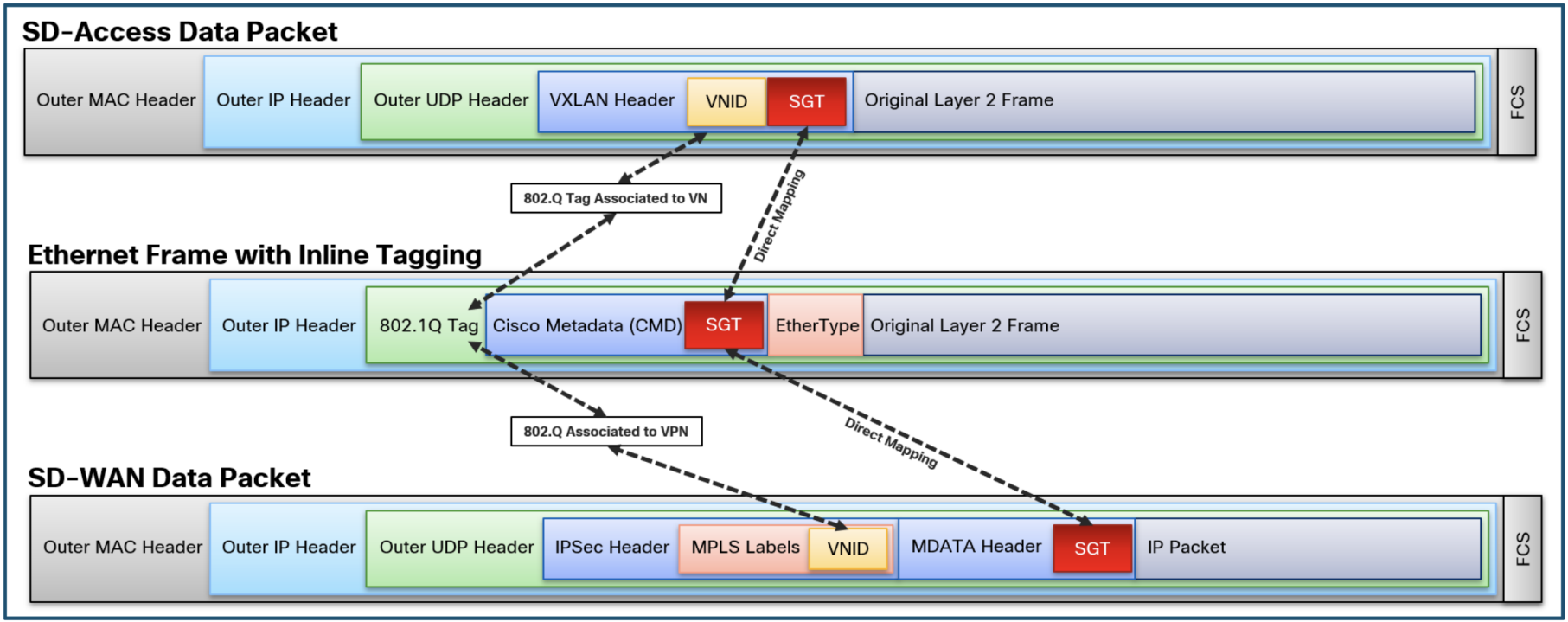
Ethernet Cisco Metadata (CMD)



SD-WAN: IPSec Encapsulation



Putting all together…



Independent Domain
Basic Deployment

Deployment Prerequisites

SD-WAN:

- Cisco SD-WAN Controllers (vManage, vBond, and vSmart) are deployed with valid certificates,

- Independent Domain supported Cisco WAN Edge devices are onboarded and active.

SDA:

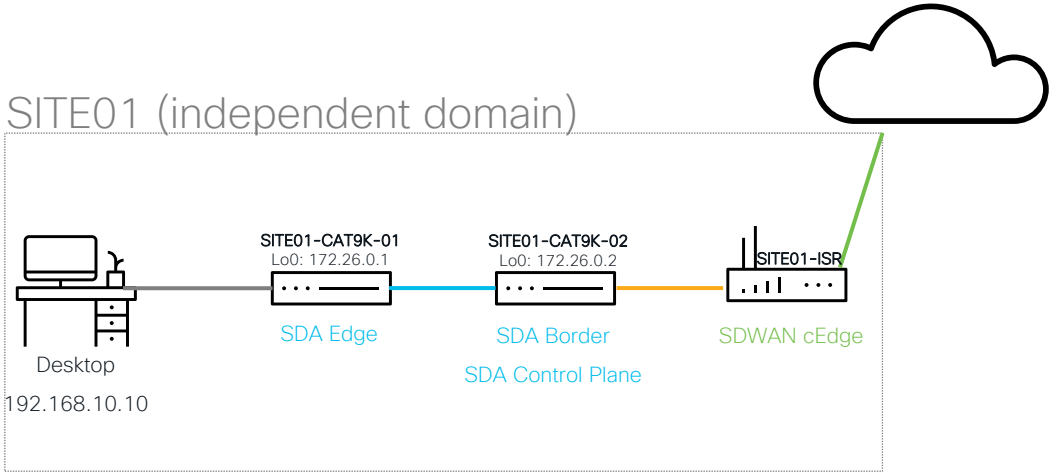
- Cisco DNA Center is installed and integrated with the Identity Services Engine,

- The Design Application in Cisco DNA Center is appropriately configured for the deployment,

- The SD-Access fabric is deployed. The border nodes are connected to the SD-WAN eEdge routers and have IP reachability to Cisco DNA Center.

SDA – SD-WAN: Setup

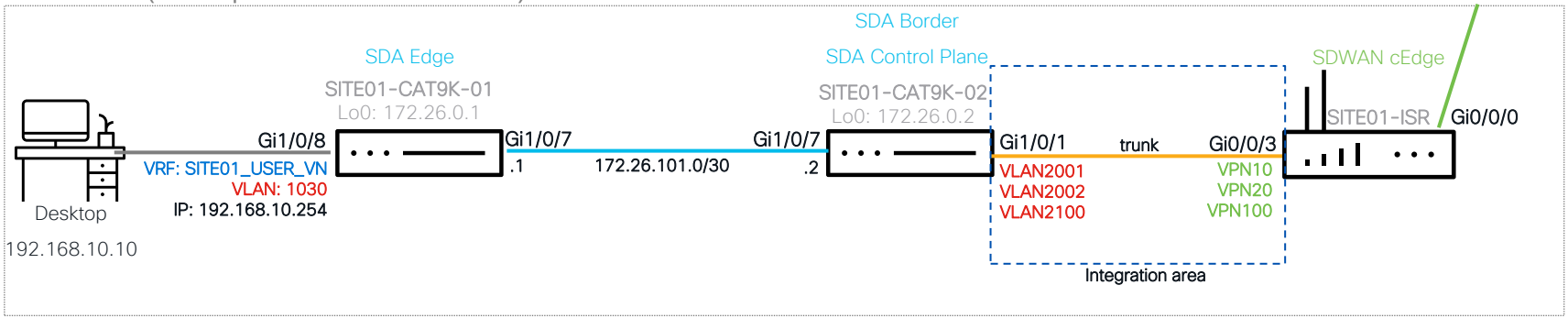
SDA
SD-WAN
manual TrustSec (VRF-lite)



SDA – SD-WAN: Setup

SDA
SD-WAN
manual TrustSec (VRF-lite)

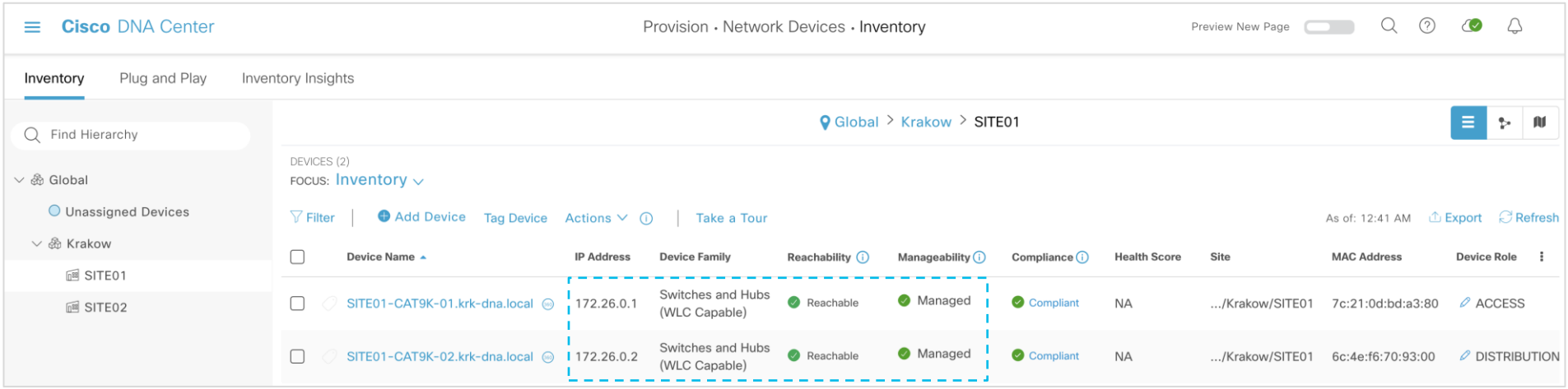
SITE01 (independent domain)



SDA IP Transit & mapping to SD-WAN VPNs:

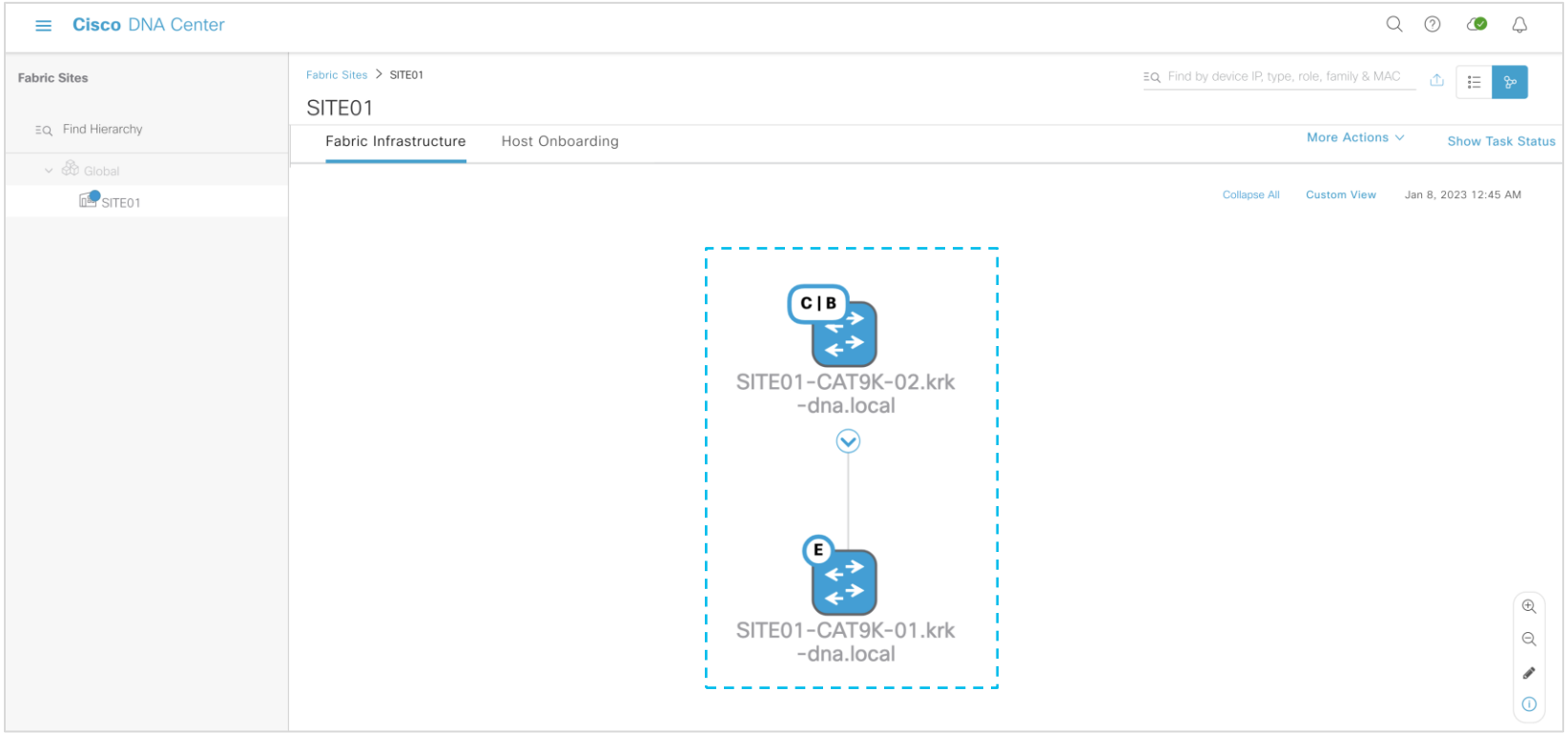
VN: SITE01_USER_VN	SVI/VLAN: 2001	IP: 172.26.100.0/30	VPN: 10
VN: SITE01_DEVICE_VN	SVI/VLAN: 2002	IP: 172.26.100.4/30	VPN: 20
VN: INFRA_VN	SVI/VLAN: 2100	IP: 172.26.100.8/30	VPN: 100

SDA: pre-integration state



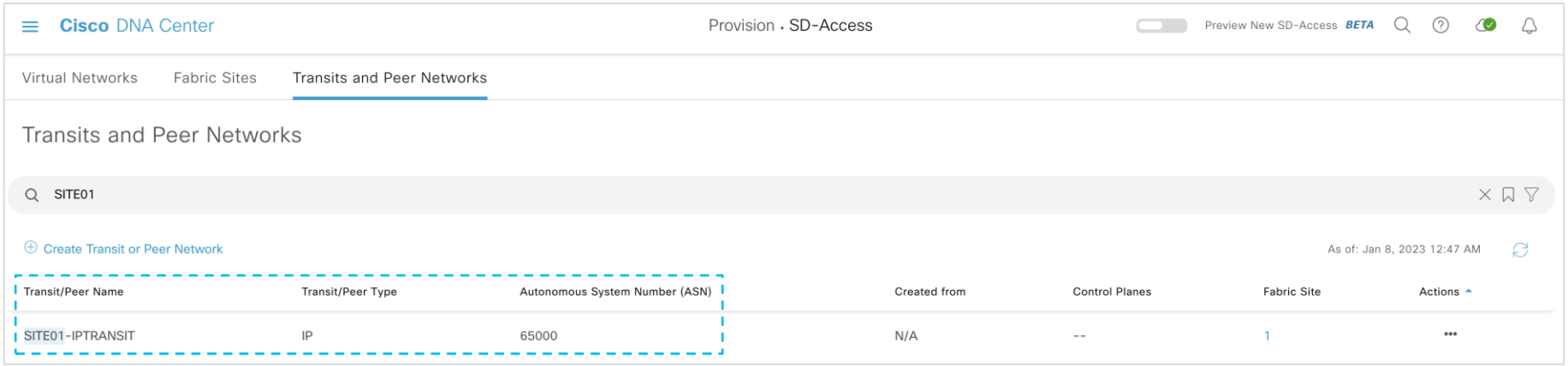
2 x Cat9k added to Cisco DNA Center inventory & provisioned

SDA: pre-integration state state



2 x Cat9k configured as SDA Edge and SDA Control/Border Node

SDA: pre-integration state



IP TRANSIT configured on SDA Border
(configured BGP AS Number = 65000 must match AS number configured on SD-WAN)

SDA: pre-integration state

SITE01-CAT9K-02.krk-dna.local

Border Information

Border Type	EXTERNAL
Internal Domain Protocol Number	65100

Border Handoff

GigabitEthernet1/0/1

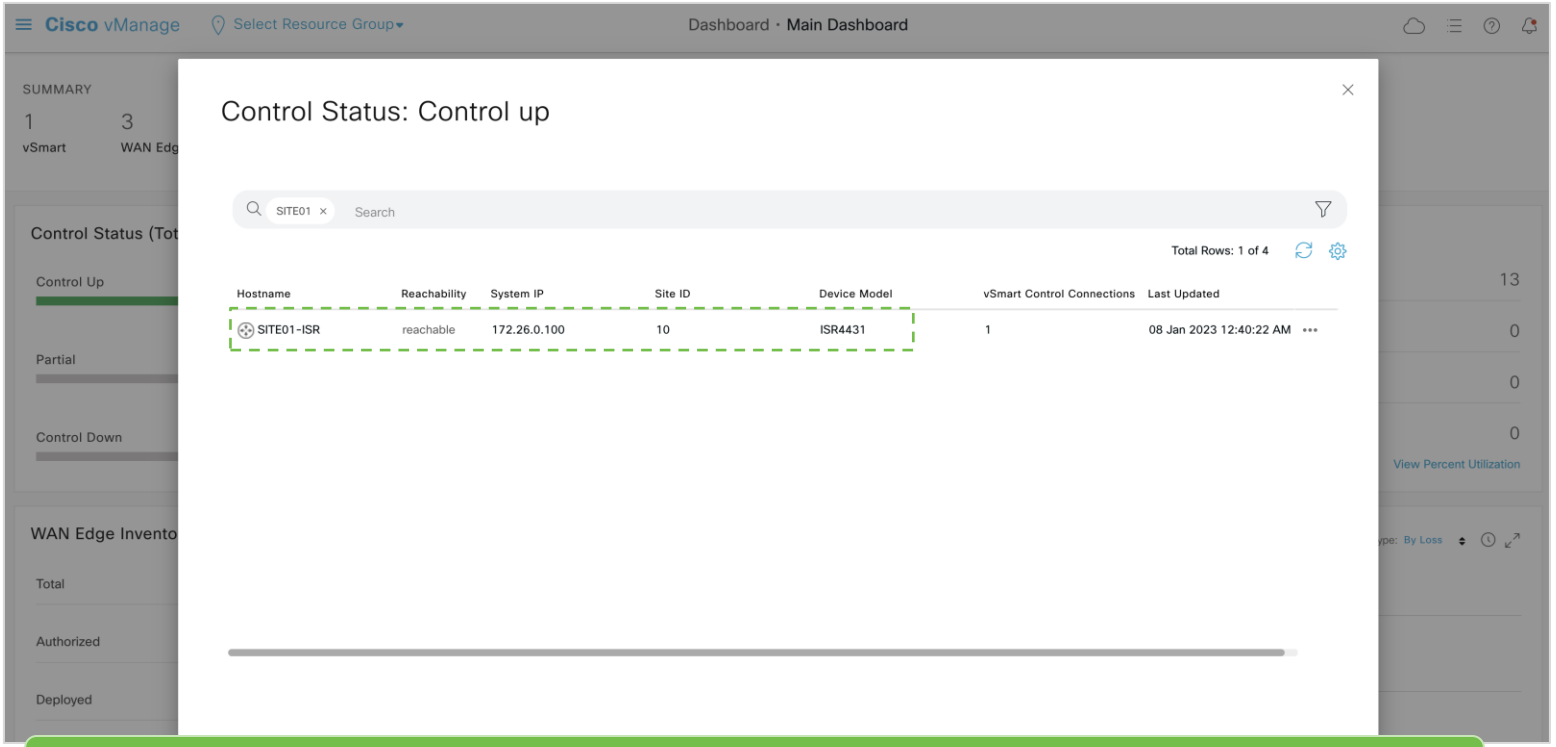
Layer3

External Domain Protocol	65000

Virtual Network	Vlan	Local IP	Remote IP
INFRA_VN-Global/Krakow/SITE01	2100	172.26.100.9/30 |	172.26.100.10/30 |
SITE01_USER_VN-Global/Krakow/SITE01	2001	172.26.100.1/30 |	172.26.100.2/30 |
SITE01_DEVICE_VN-Global/Krakow/SITE01	2002	172.26.100.5/30 |	172.26.100.6/30 |

Border Handoff configured for INFRA_VN, as well as for all other VNs (USER_VN & DEVICE_VN)

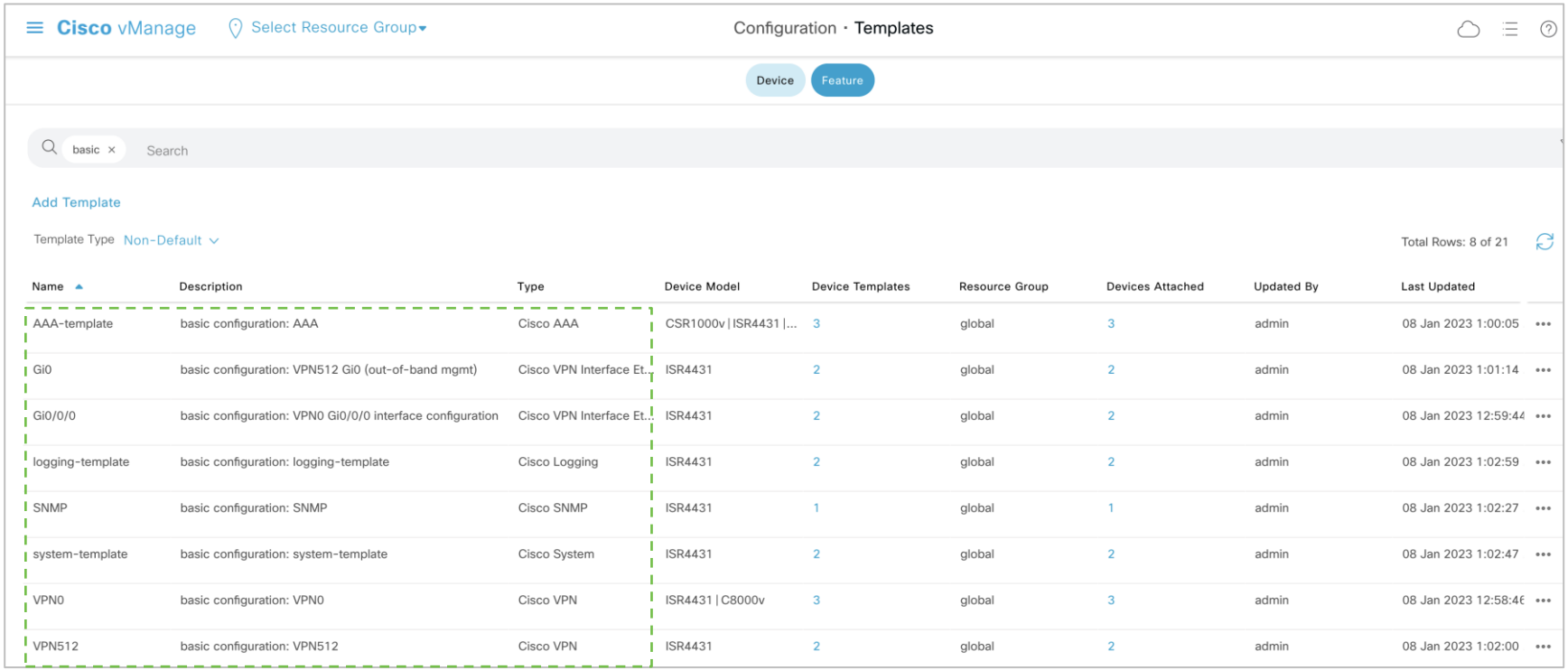
SD-WAN: pre-integration state



cEdge configured and connected to SD-WAN controllers.

SD-WAN: pre-integration state

standard SD-WAN process



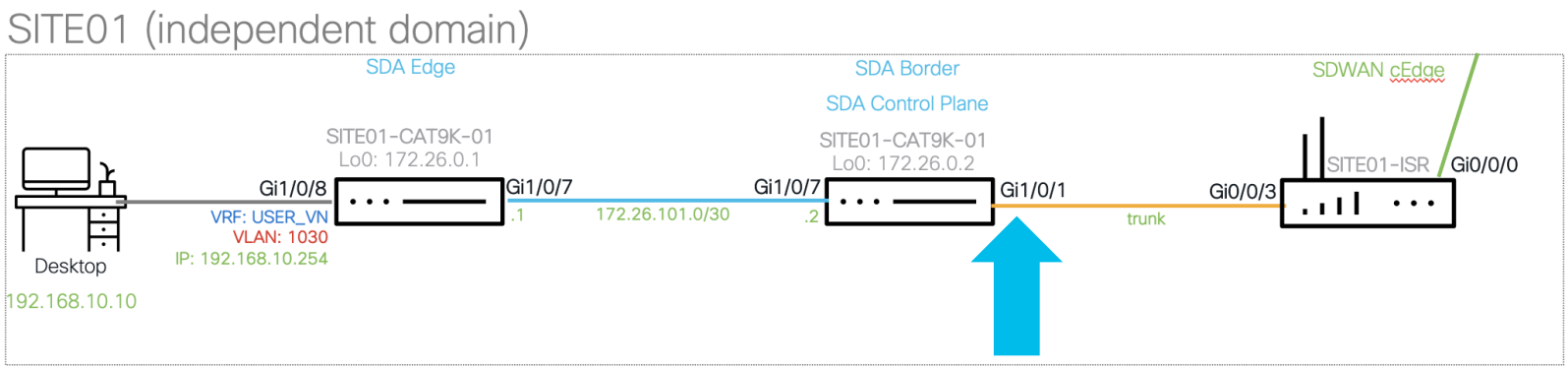
Name	Description	Type	Device Model	Device Templates	Resource Group	Devices Attached	Updated By	Last Updated
AAA-template	basic configuration: AAA	Cisco AAA	CSR1000v | ISR4431 |...	3	global	3	admin	08 Jan 2023 1:00:05
Gi0	basic configuration: VPN512 Gi0 (out-of-band mgmt)	Cisco VPN Interface Et...	ISR4431	2	global	2	admin	08 Jan 2023 1:01:14
Gi0/0/0	basic configuration: VPN0 Gi0/0/0 interface configuration	Cisco VPN Interface Et...	ISR4431	2	global	2	admin	08 Jan 2023 12:59:44
logging-template	basic configuration: logging-template	Cisco Logging	ISR4431	2	global	2	admin	08 Jan 2023 1:02:59
SNMP	basic configuration: SNMP	Cisco SNMP	ISR4431	1	global	1	admin	08 Jan 2023 1:02:27
system-template	basic configuration: system-template	Cisco System	ISR4431	2	global	2	admin	08 Jan 2023 1:02:47
VPN0	basic configuration: VPN0	Cisco VPN	ISR4431 | C8000v	3	global	3	admin	08 Jan 2023 12:58:46
VPN512	basic configuration: VPN512	Cisco VPN	ISR4431	2	global	2	admin	08 Jan 2023 1:02:00

Basic Templates created for:
- VPN0 (transport VPN) & VPN512 (management)
- Physical interfaces (Gi0/0/0 & Gi0)
- Other basic services (AAA, logging, SNMP, system, …)

Independent Domain
Integration

SDA: integration process

TrustSec configuration

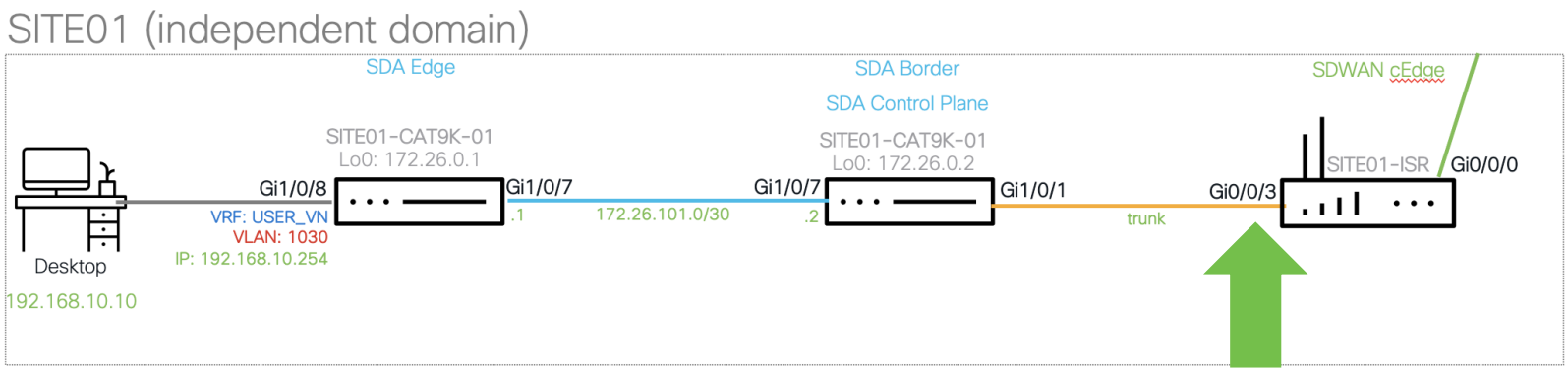



```
interface GigabitEthernet1/0/1
 switchport mode trunk
 cts manual
  policy static sgt 2 trusted
end
```

TrustSec must be enabled on SDA Border Handoff interface. During enablement, interface will flap!
SGT=2 (TrustSec_Devices)

SD-WAN: integration process

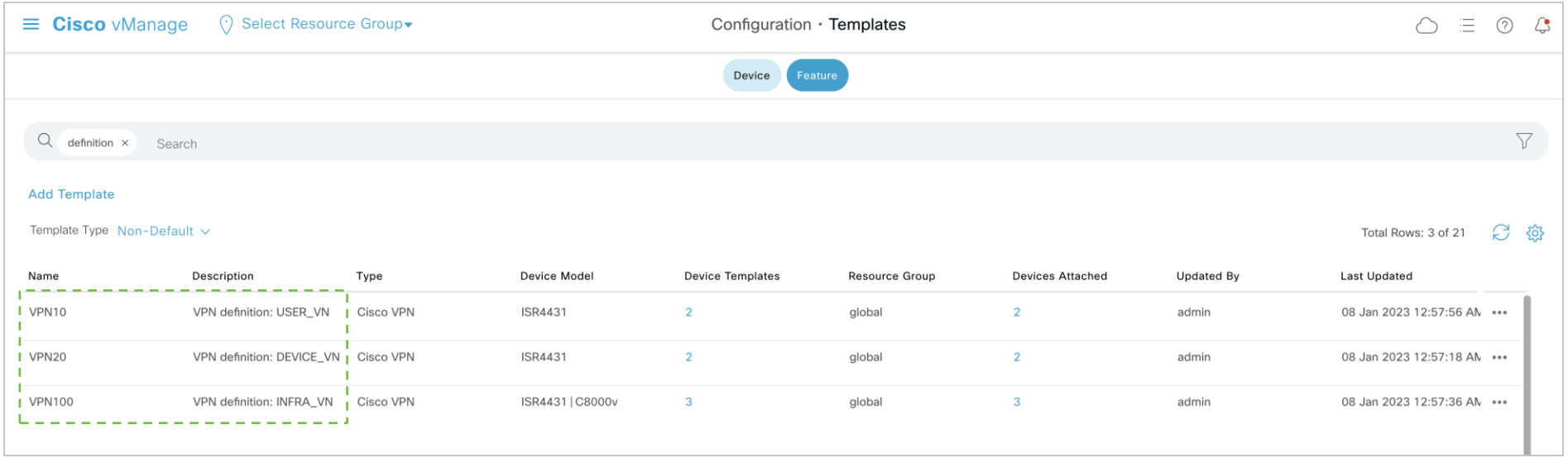
BGP & TrustSec configuration



Service VPNs, BGP and TrustSec templates must be added from SD-WAN perspective on interface towards SDA. During TrustSec enablement interface will flap!

SD-WAN: integration process

SD-WAN VPN templates for SDA Virtual Networks (VNs)

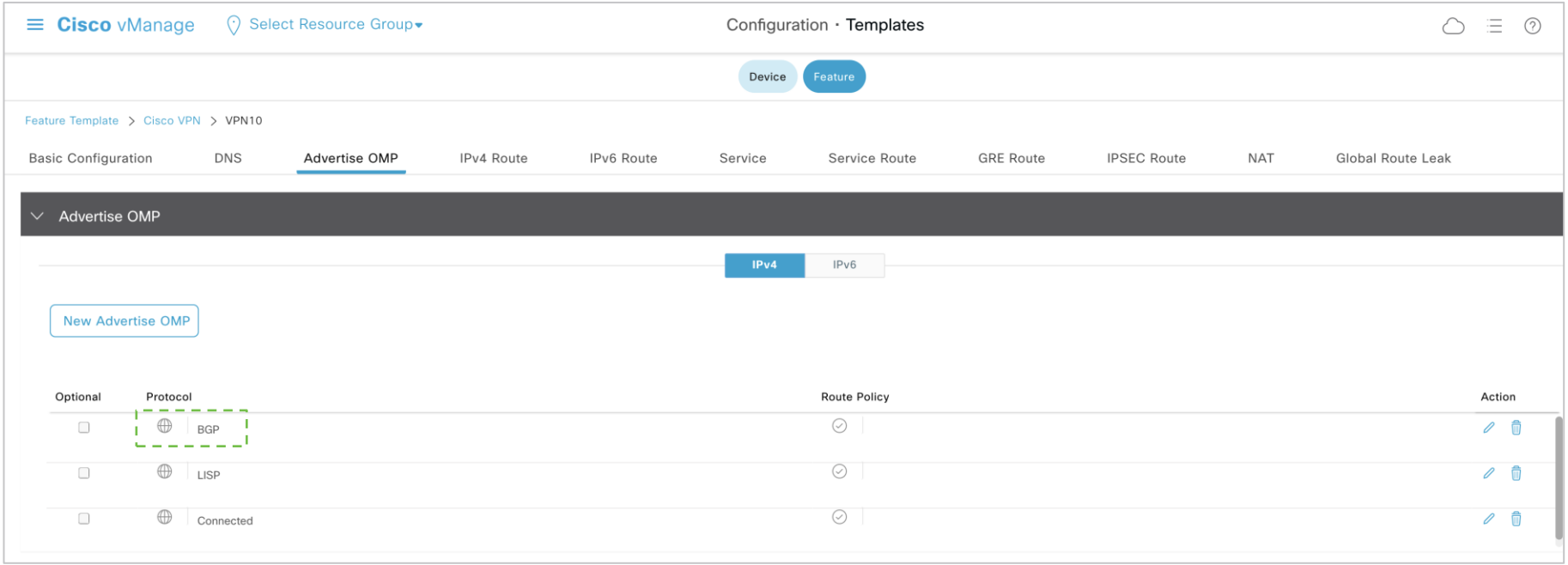


Name	Description	Type	Device Model	Device Templates	Resource Group	Devices Attached	Updated By	Last Updated
VPN10	VPN definition: USER_VN	Cisco VPN	ISR4431	2	global	2	admin	08 Jan 2023 12:57:56 AM
VPN20	VPN definition: DEVICE_VN	Cisco VPN	ISR4431	2	global	2	admin	08 Jan 2023 12:57:18 AM
VPN100	VPN definition: INFRA_VN	Cisco VPN	ISR4431 | C8000v	3	global	3	admin	08 Jan 2023 12:57:36 AM

Service VPN templates created for:
- SDA Overlay (USER_VN & DEVICE_VN)
- SDA Underlay (INFRA_VN)

SD-WAN: integration state

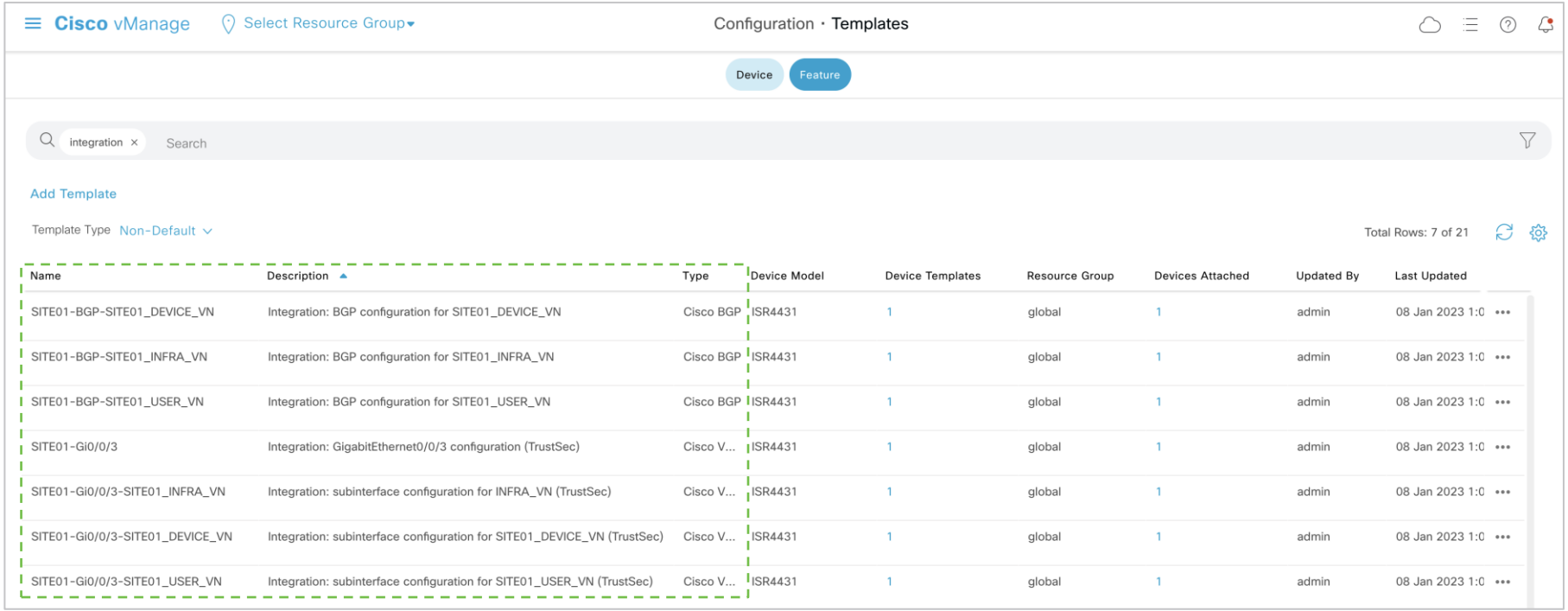
Routing redistribution



OMP-BGP Advertisement must be enabled for all Service VPNs.

SD-WAN: integration state

BGP & TrustSec configuration

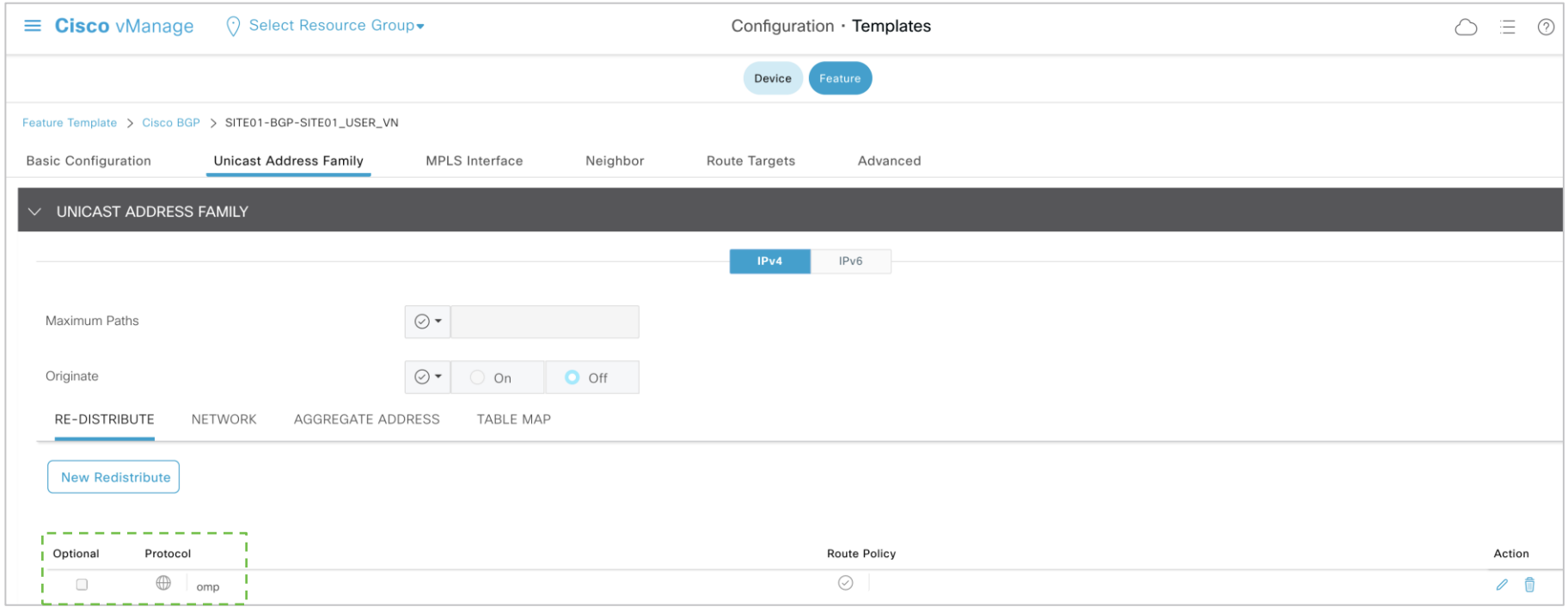


Name	Description	Type	Device Model	Device Templates	Resource Group	Devices Attached	Updated By	Last Updated
SITE01-BGP-SITE01_DEVICE_VN	Integration: BGP configuration for SITE01_DEVICE_VN	Cisco BGP	ISR4431	1	global	1	admin	08 Jan 2023 1:0
SITE01-BGP-SITE01_INFRA_VN	Integration: BGP configuration for SITE01_INFRA_VN	Cisco BGP	ISR4431	1	global	1	admin	08 Jan 2023 1:0
SITE01-BGP-SITE01_USER_VN	Integration: BGP configuration for SITE01_USER_VN	Cisco BGP	ISR4431	1	global	1	admin	08 Jan 2023 1:0
SITE01-Gi0/0/3	Integration: GigabitEthernet0/0/3 configuration (TrustSec)	Cisco V...	ISR4431	1	global	1	admin	08 Jan 2023 1:0
SITE01-Gi0/0/3-SITE01_INFRA_VN	Integration: subinterface configuration for INFRA_VN (TrustSec)	Cisco V...	ISR4431	1	global	1	admin	08 Jan 2023 1:0
SITE01-Gi0/0/3-SITE01_DEVICE_VN	Integration: subinterface configuration for SITE01_DEVICE_VN (TrustSec)	Cisco V...	ISR4431	1	global	1	admin	08 Jan 2023 1:0
SITE01-Gi0/0/3-SITE01_USER_VN	Integration: subinterface configuration for SITE01_USER_VN (TrustSec)	Cisco V...	ISR4431	1	global	1	admin	08 Jan 2023 1:0

BGP and TrustSec templates deployed on SITE01-ISR cEdge.

SD-WAN: integration state

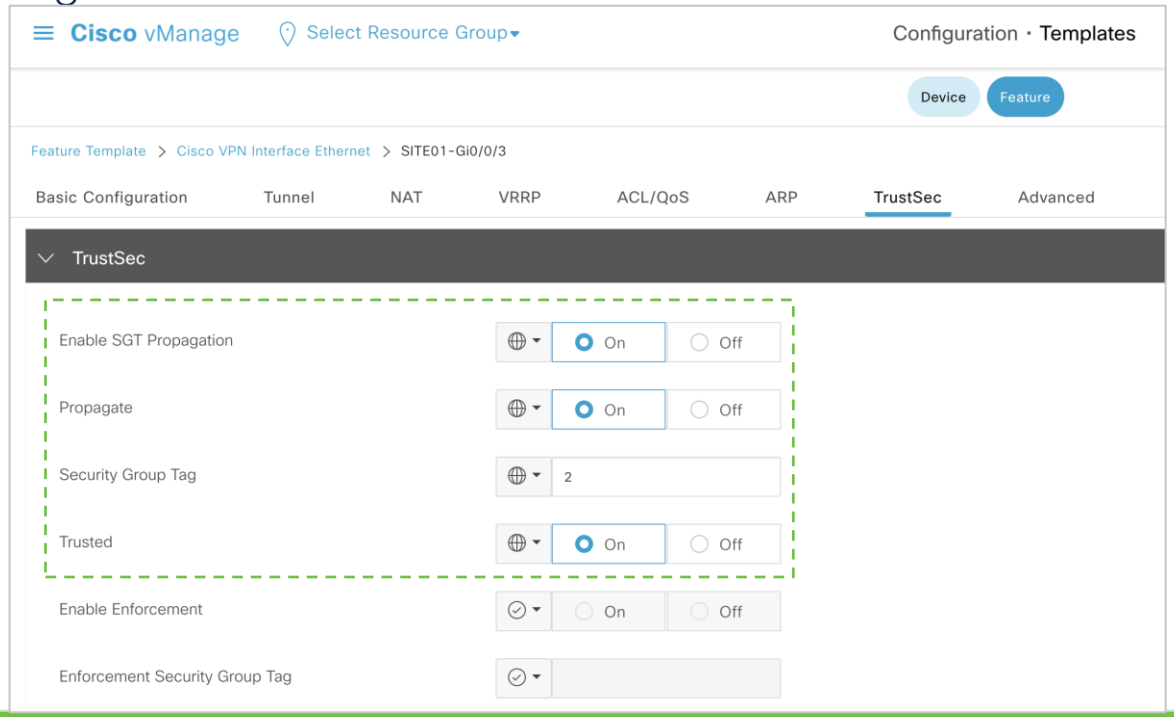
BGP configuration



OMP to BGP redistribution enabled.

SD-WAN: integration state

TrustSec configuration



TrustSec configuration on the interface (SGT=2 -> TrustSec_Devices)

Independent Domain
Validation

SDA - SD-WAN: integration validation

```
SITE01-CAT9K-02#sh ip bgp summary | b Neighbor
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.26.100.10   4        65000      80      81       49    0    0 01:07:36        4

SITE01-CAT9K-02#sh ip bgp vpnv4 vrf SITE01_USER_VN summary | b Neighbor
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.26.100.2    4        65000     364     365       61    0    0 05:27:01        2

SITE01-CAT9K-02#sh ip bgp vpnv4 vrf SITE01_DEVICE_VN summary | b Neighbor
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.26.100.6    4        65000     363     365       61    0    0 05:27:08        0
```

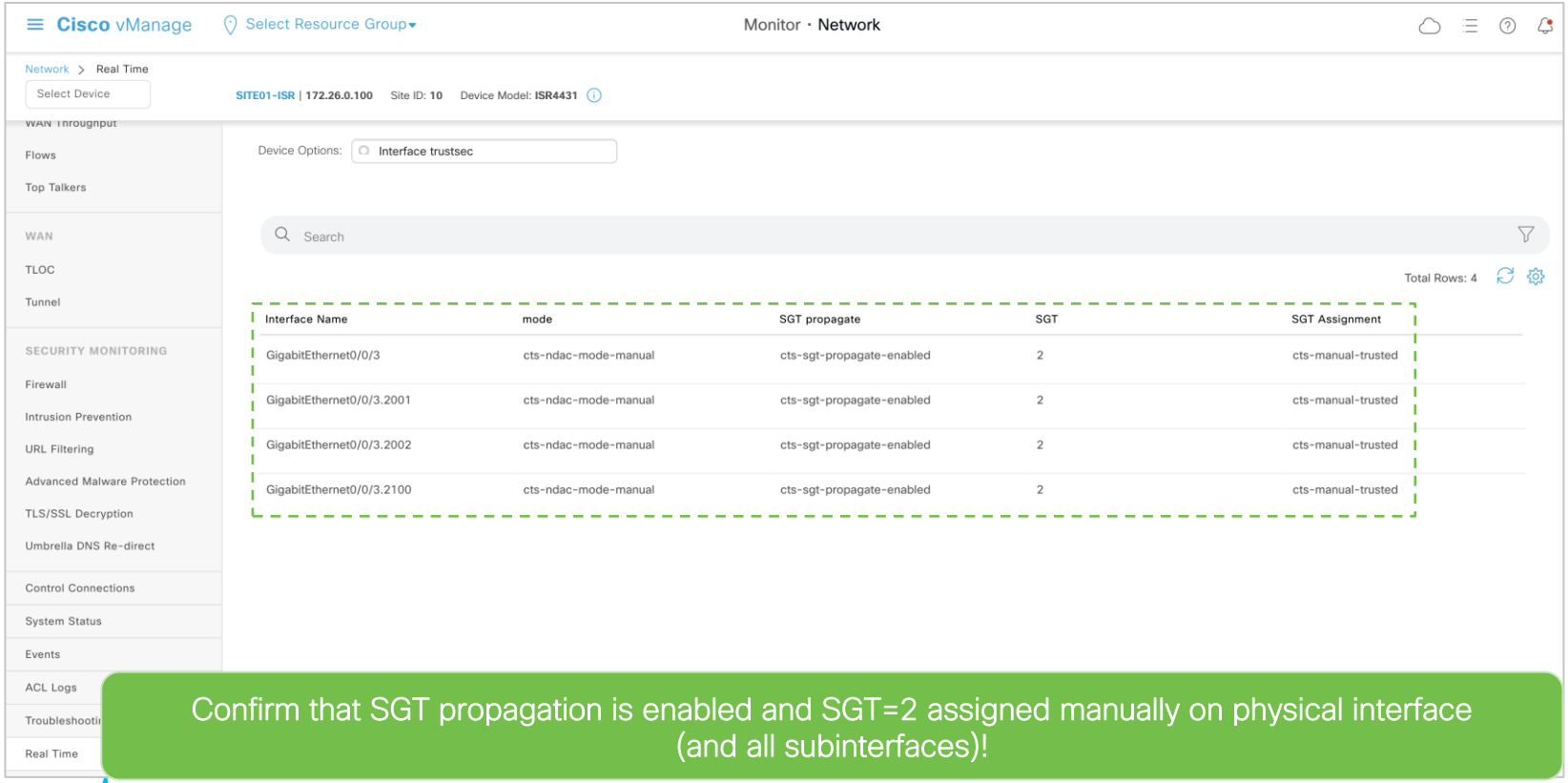
Make sure that IP Transit is working as expected, all BGP sessions are established and all necessary prefixes are exchaged for end-to-end reachability.

SDA - SD-WAN: integration validation

```
SITE01-CAT9K-02#sh cts interface brief
Global Dot1x feature is Disabled
Interface GigabitEthernet1/0/1:
    CTS is enabled, mode:    MANUAL
    IFC state:               OPEN
    Interface Active for      1d00h
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: ""
    Authorization Status:    SUCCEEDED
        Peer SGT:            2:TrustSec_Devices
        Peer SGT assignment: Trusted
    SAP Status:              NOT APPLICABLE
    Propagate SGT:           Enabled
    Cache Info:
        Expiration            : N/A
        Cache applied to link : NONE


    L3 IPM:   disabled.
```

Make sure that CTS is enabled on SDA Border Handoff.

SD-WAN: integration validation



Confirm that SGT propagation is enabled and SGT=2 assigned manually on physical interface (and all subinterfaces)!

Integrated Domain

Integrated Domain
Basic Deployment

cisco Live!

SDA – SD-WAN: Integrated Domain

Interoperability:

- SD-WAN cEdges perform both SD-WAN & SDA (border & control-plane) functionality,
- SD-WAN cEdges are provisioned by SD-WAN controllers but also managed and visible in Cisco DNA Center,
- SDA border device work also as SD-WAN cEdge device,
- SDA devices are managed and provisioned (directly / indirectly) by Cisco DNA Center,
- Security details (SGT values) are carried over between both solutions directly (VXLAN – IPSec)

SDA – SD-WAN: Integrated Domain

Main characteristics:

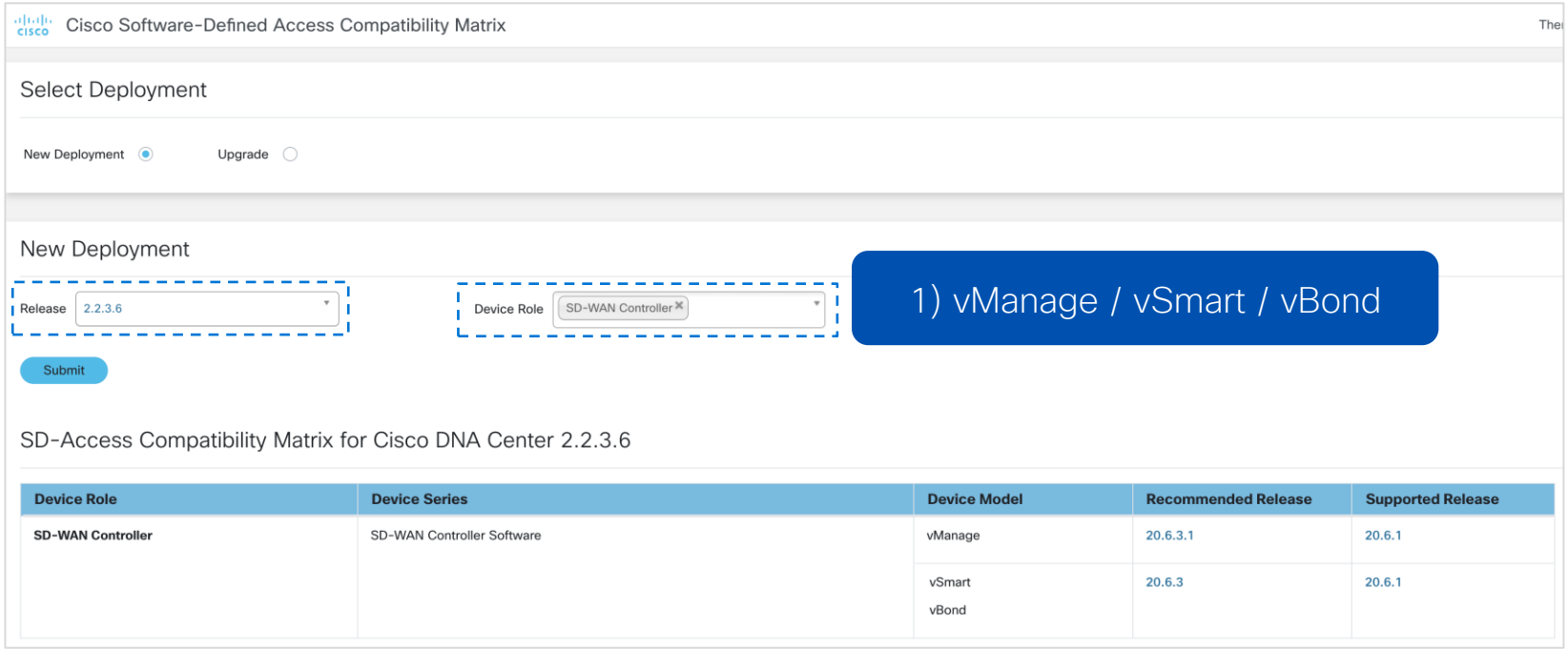
- both solutions are tightly coupled together & managed by single team,
- there are strict software version requirements (compatibility matrix),
- there is a single pane of glass to look holistically at the health state of the whole solution,
- it requires one device (for SD-WAN cEdge and SDA border & control-node),
- It must be a new SDA site.
- It has several deployment limitations and currently does not support:
  Cisco DNA Center / SDA: Multicast, IPv6, Layer 2 flooding, Layer 2 Border handoff, SD-Access Transit and Multisite Remote Border;
  IOS-XE / SD-WAN: LISP PubSub on cEdge

Common Use Case:

Mainly used in branches and small sites (CAPEX / OPEX reduction).

make sure to use compatible & tested software combinations!

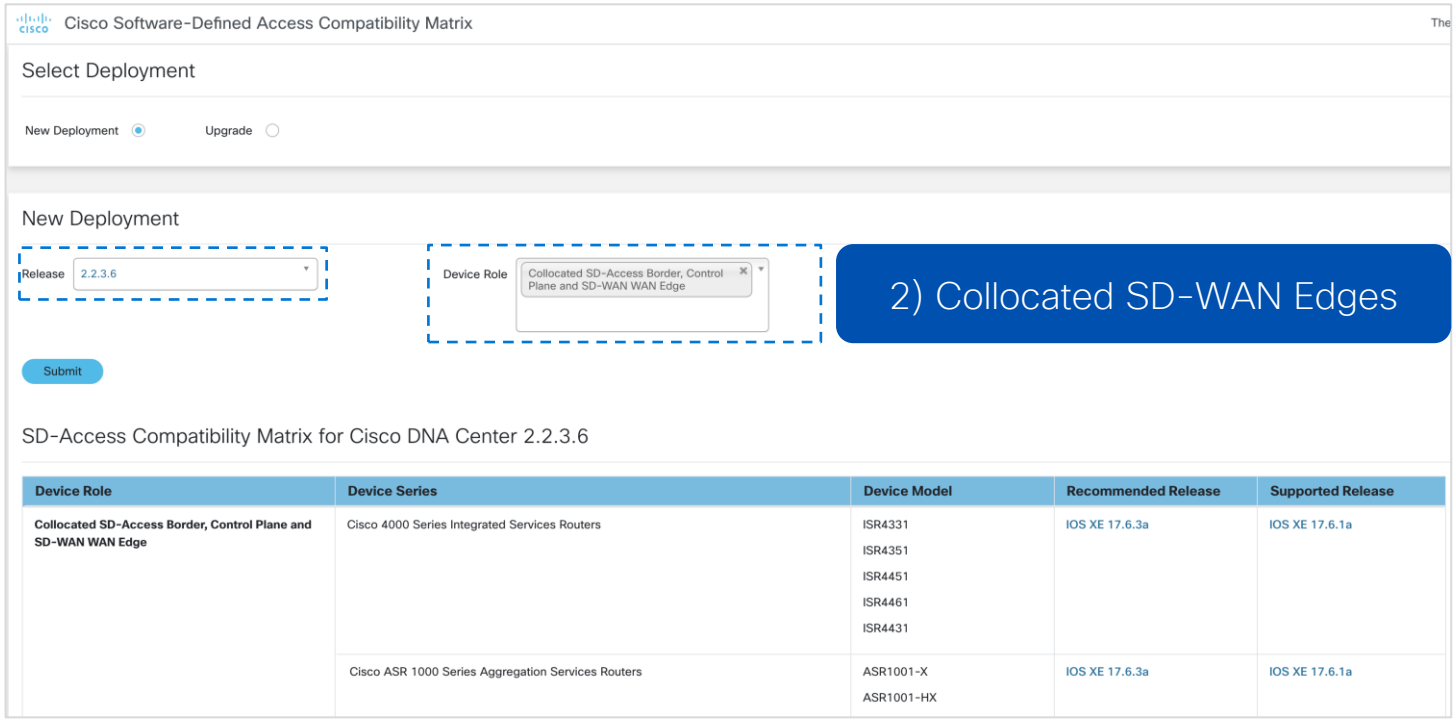
Compatibility Matrix – integrated domain



SDA-SDWAN Compatibility Matrix

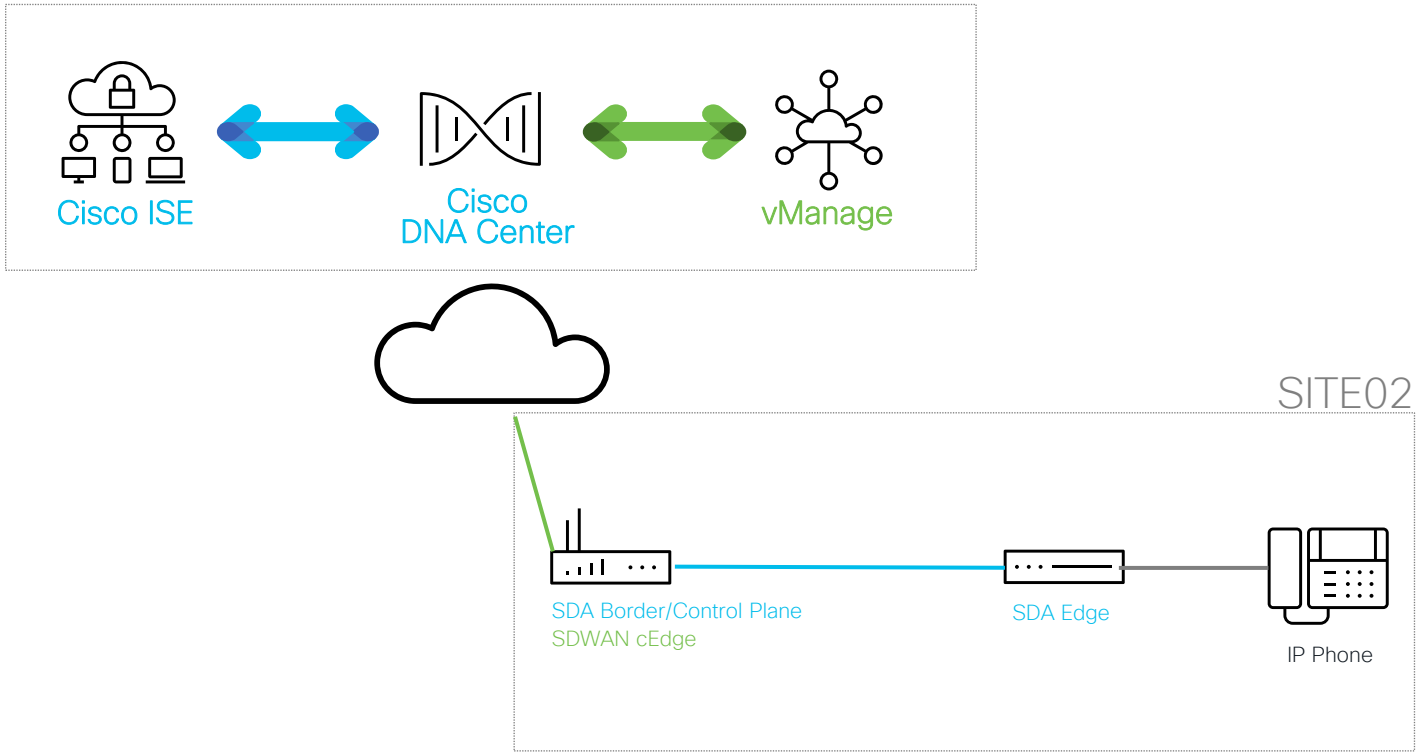
make sure to use compatible & tested software combinations!

Compatibility Matrix – integrated domain



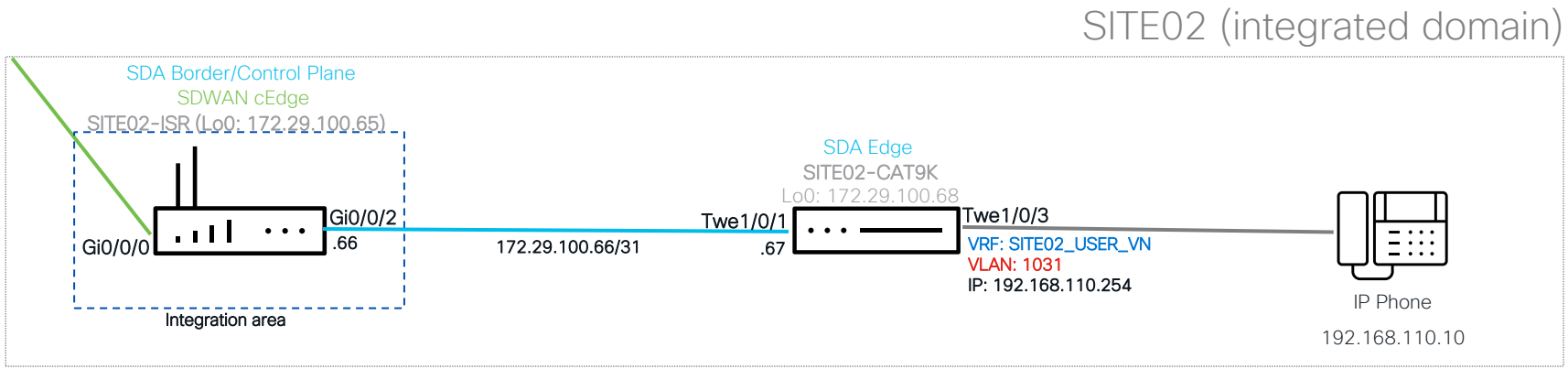
SDA-SDWAN Compatibility Matrix

SDA – SD-WAN: Integrated Domain



SDA
SD-WAN

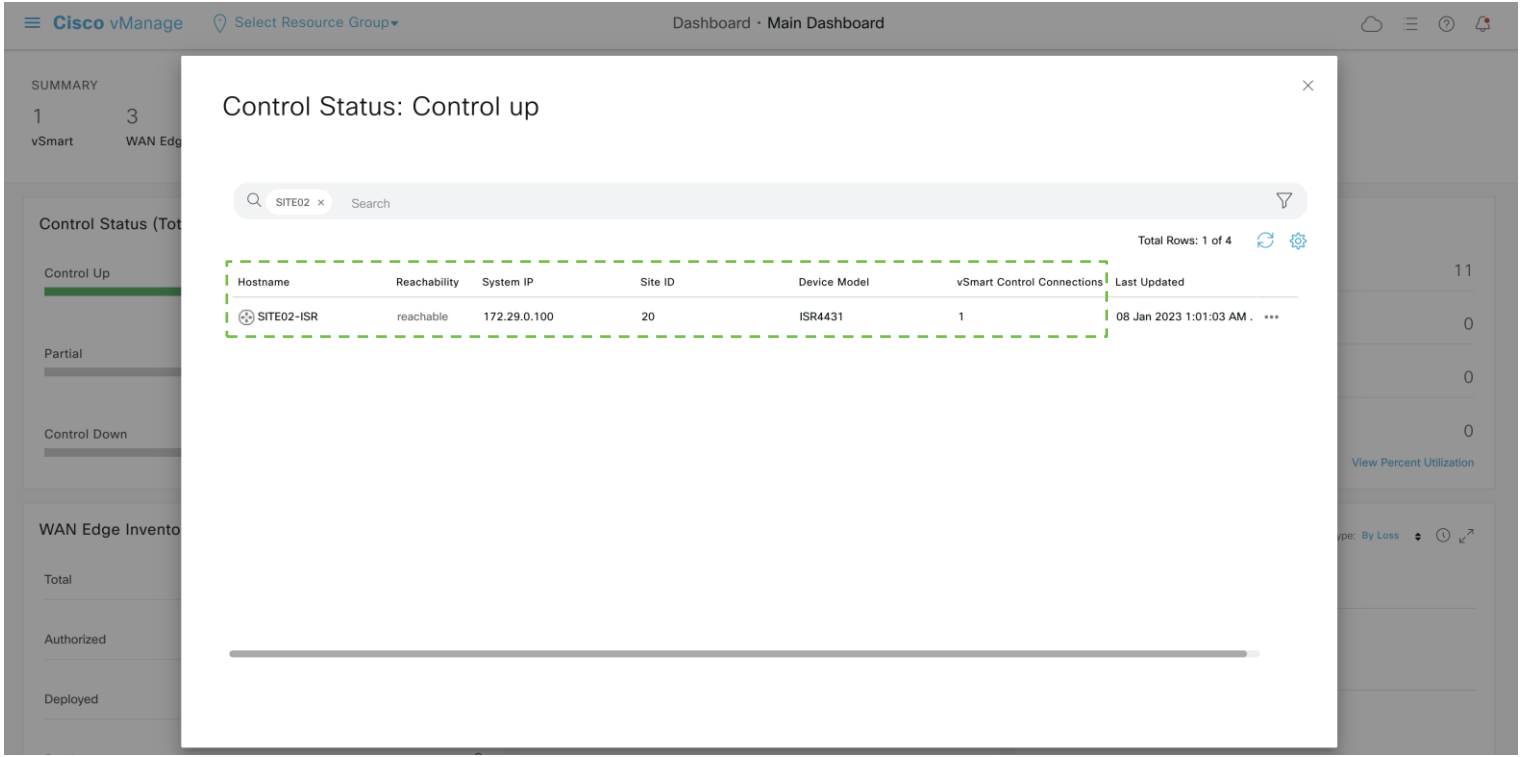
SDA – SD-WAN: Setup



Only new SDA sites are supported (no brownfield).

SDA Edge is provisioned automatically through LAN Automation process.

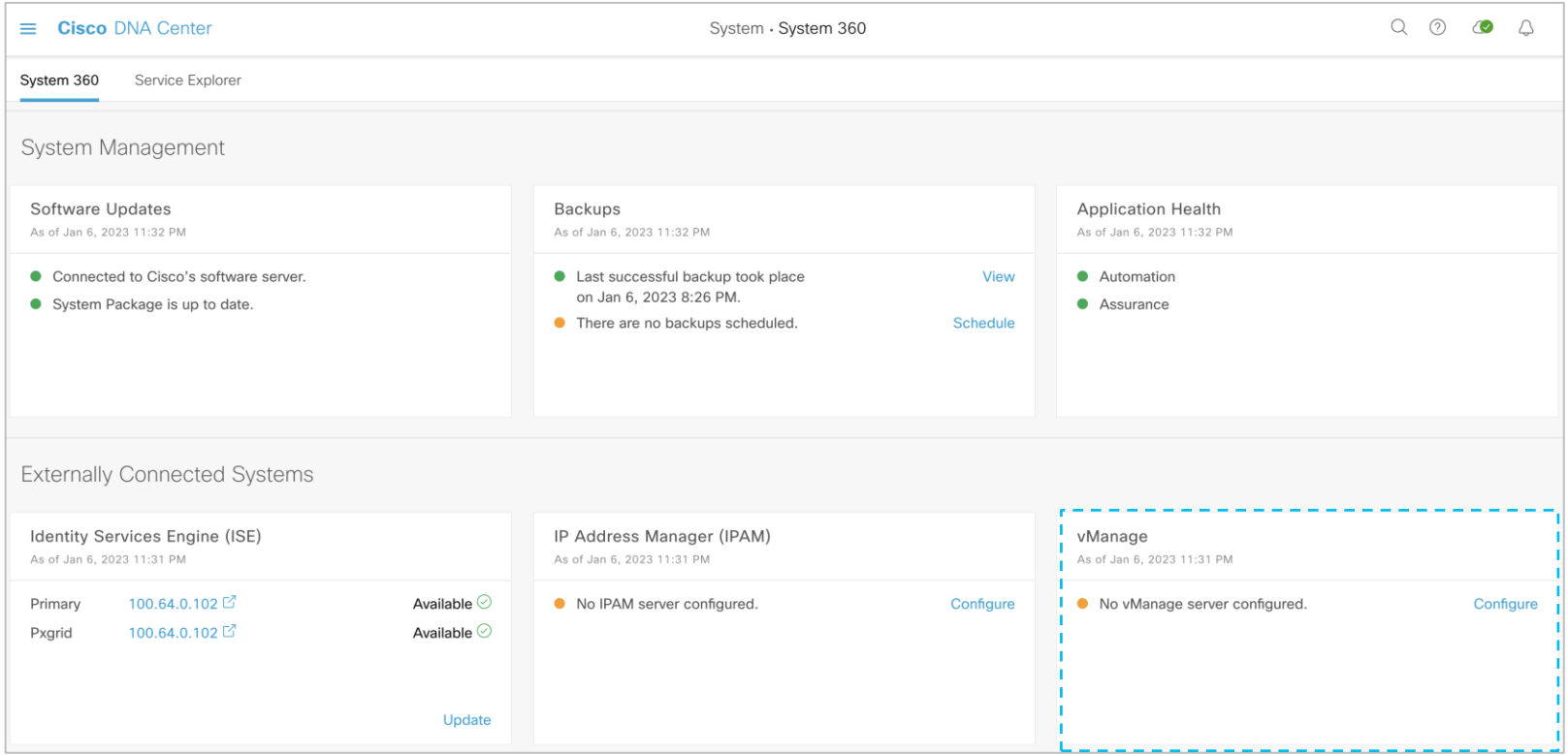
SD-WAN: pre-integration state



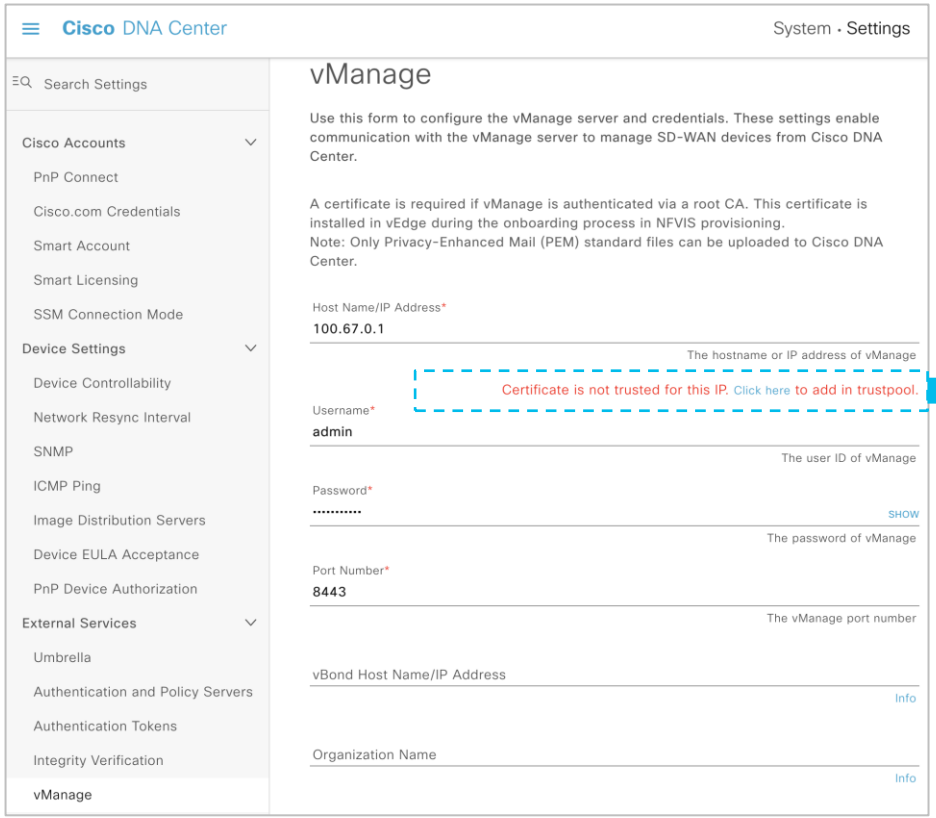
Integrated Domain
Integration

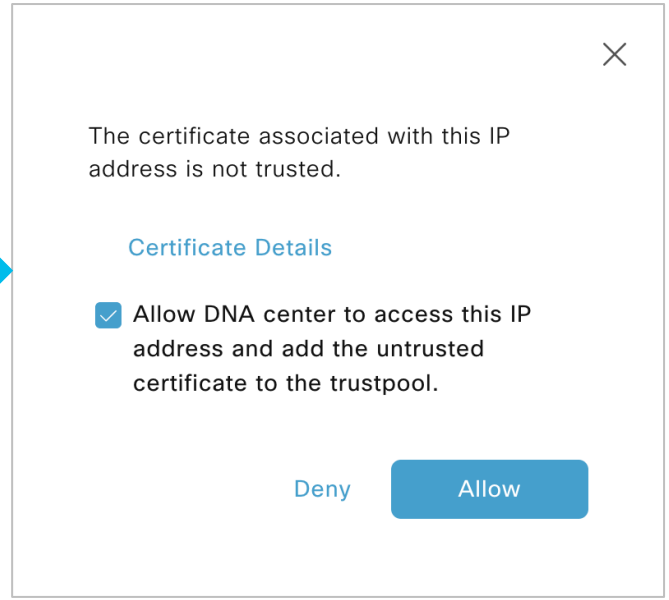
cisco Live!

SDA – SD-WAN: Controller Integration

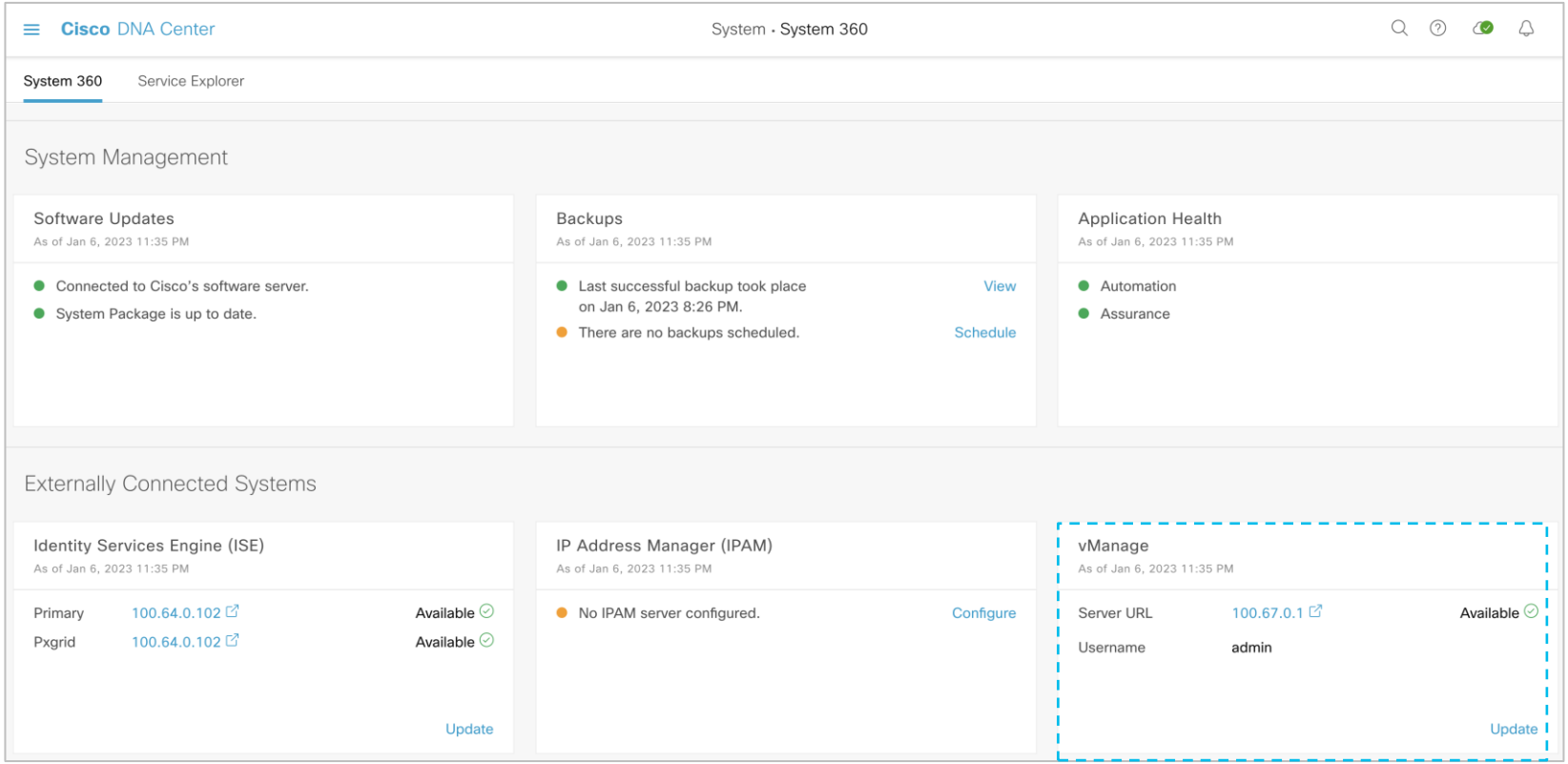


SDA – SD-WAN: Controller Integration

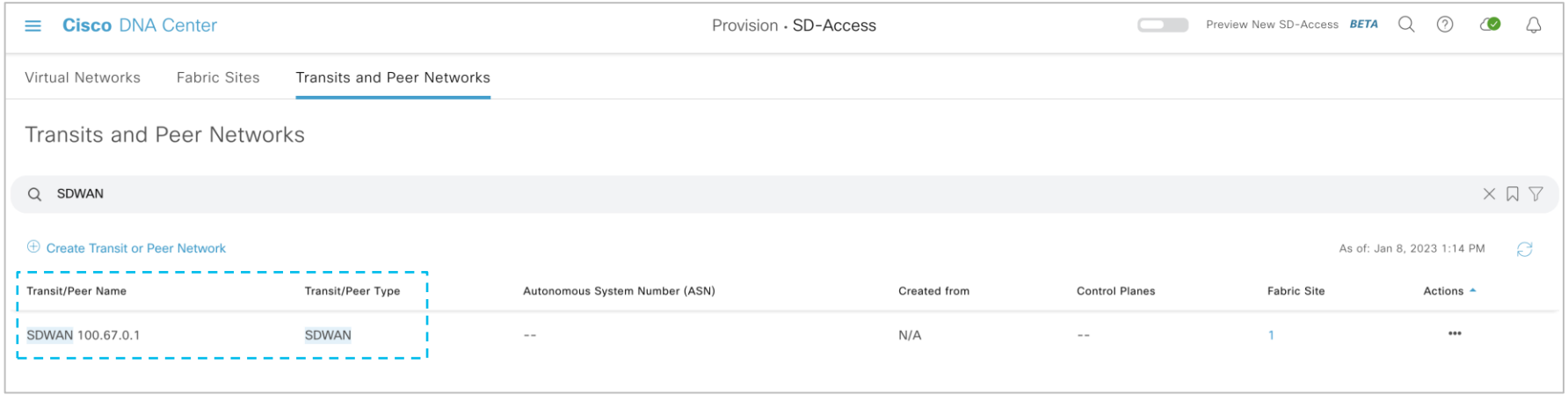




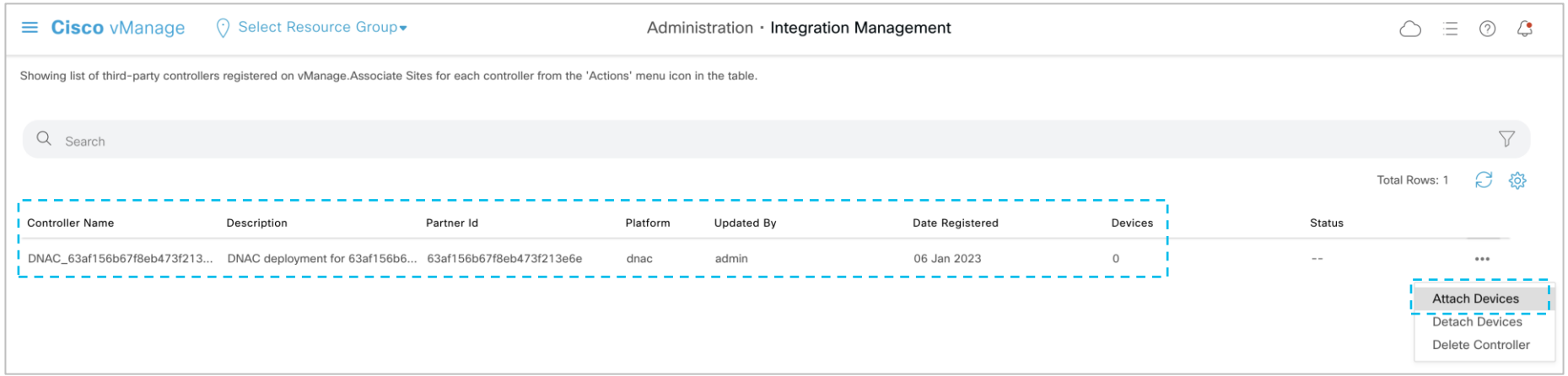
SDA – SD-WAN: Controller Integration



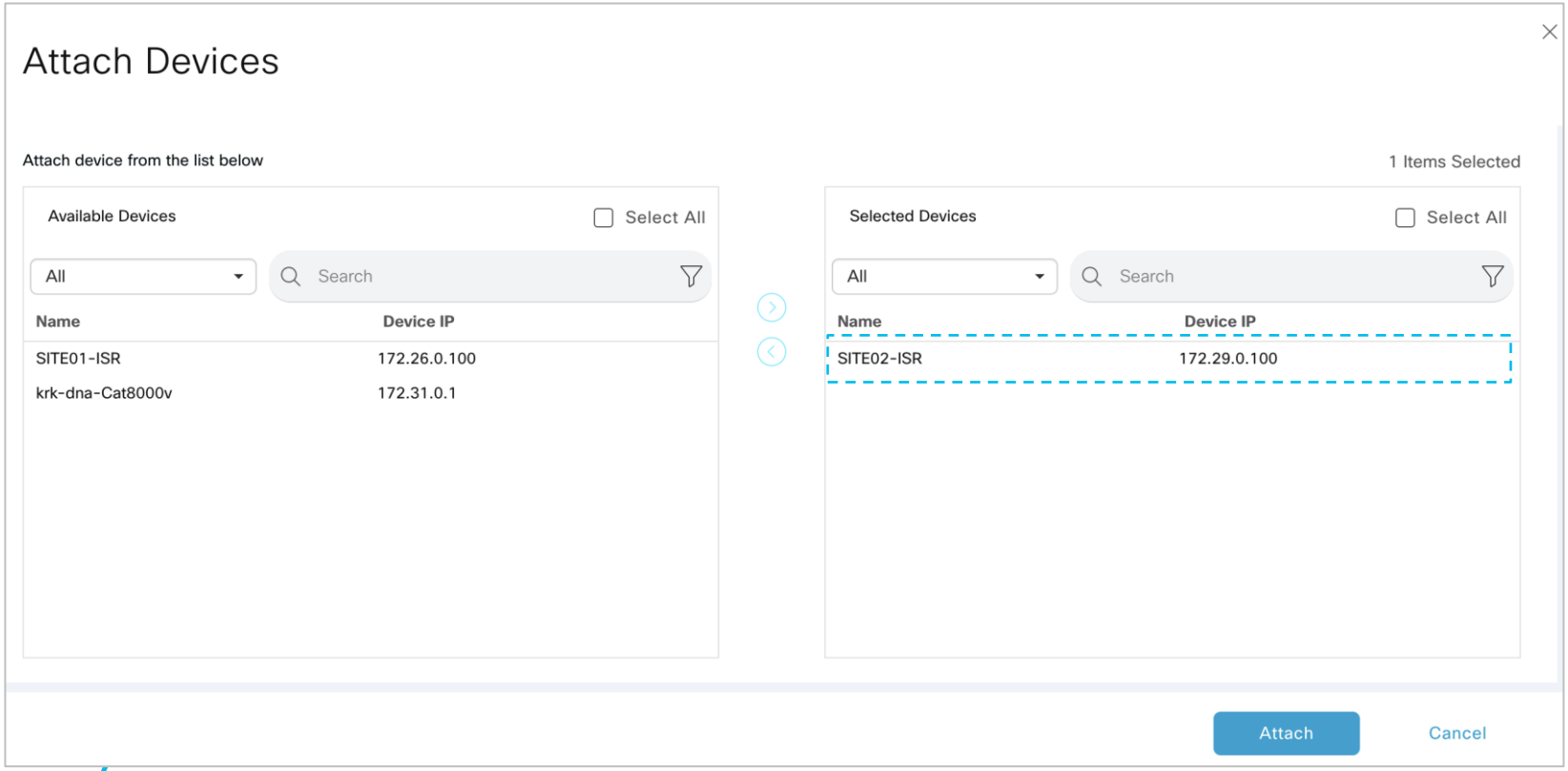
SDA – SD-WAN: SDWAN Transit



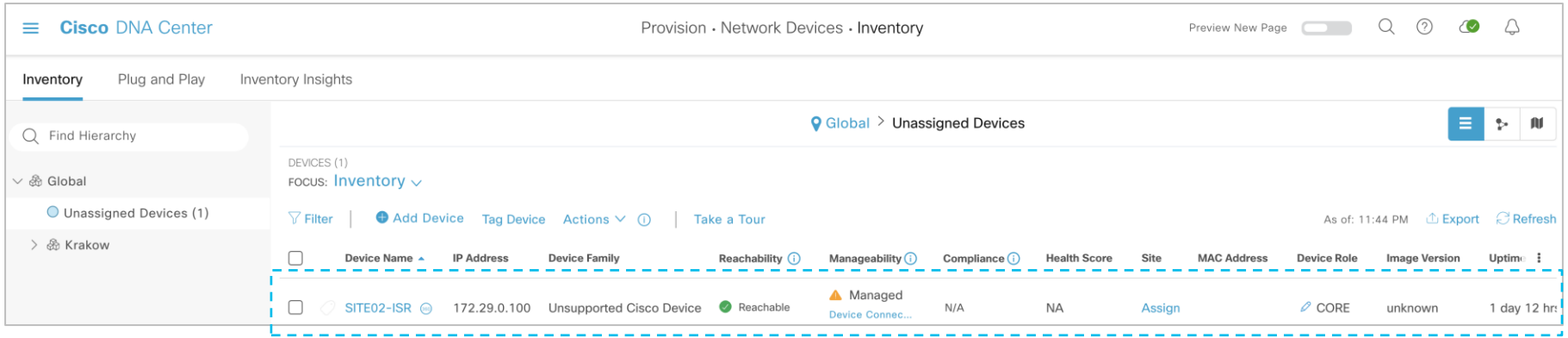
SDA – SD-WAN: Attaching devices



SDA – SD-WAN: Attaching devices

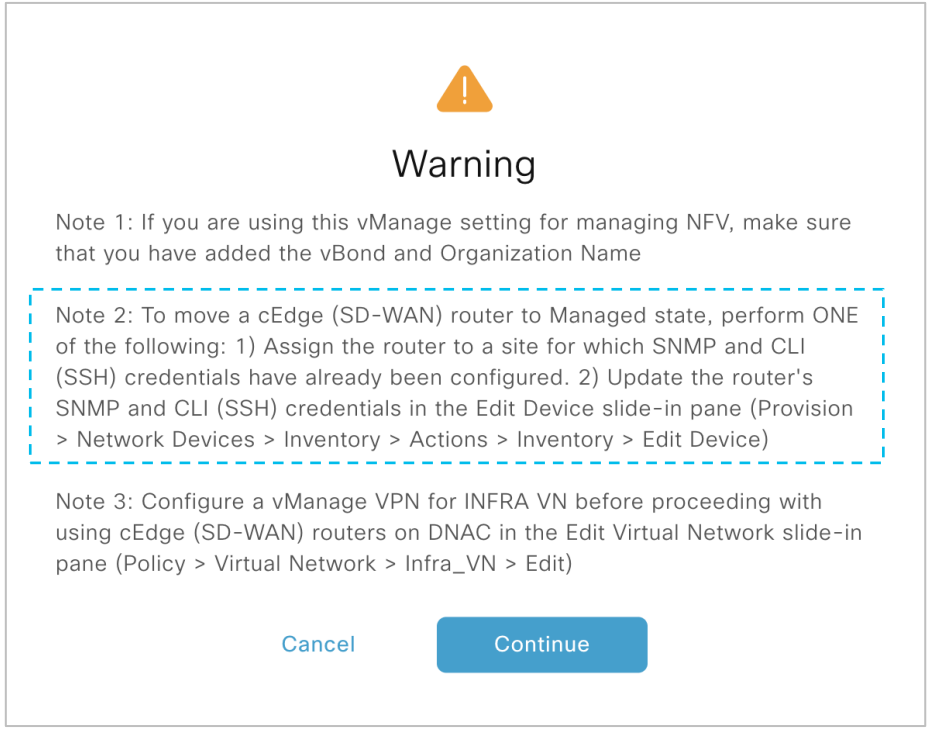


SD-WAN cEdge in Cisco DNA Center



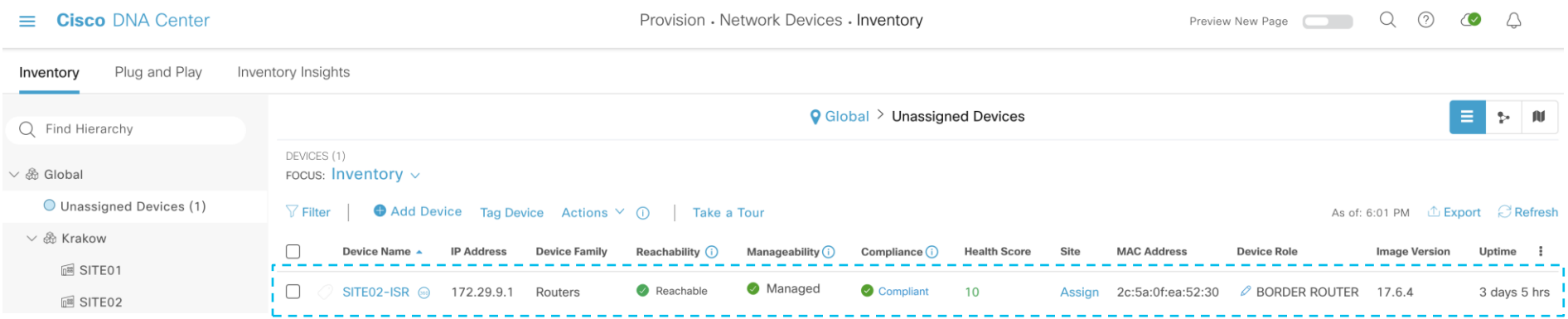
When device is added from SD-WAN to Cisco DNA Center, it will not be assigned to any site. Site assignment needs to be done manually from Cisco DNA Center.

SD-WAN cEdge in Cisco DNA Center



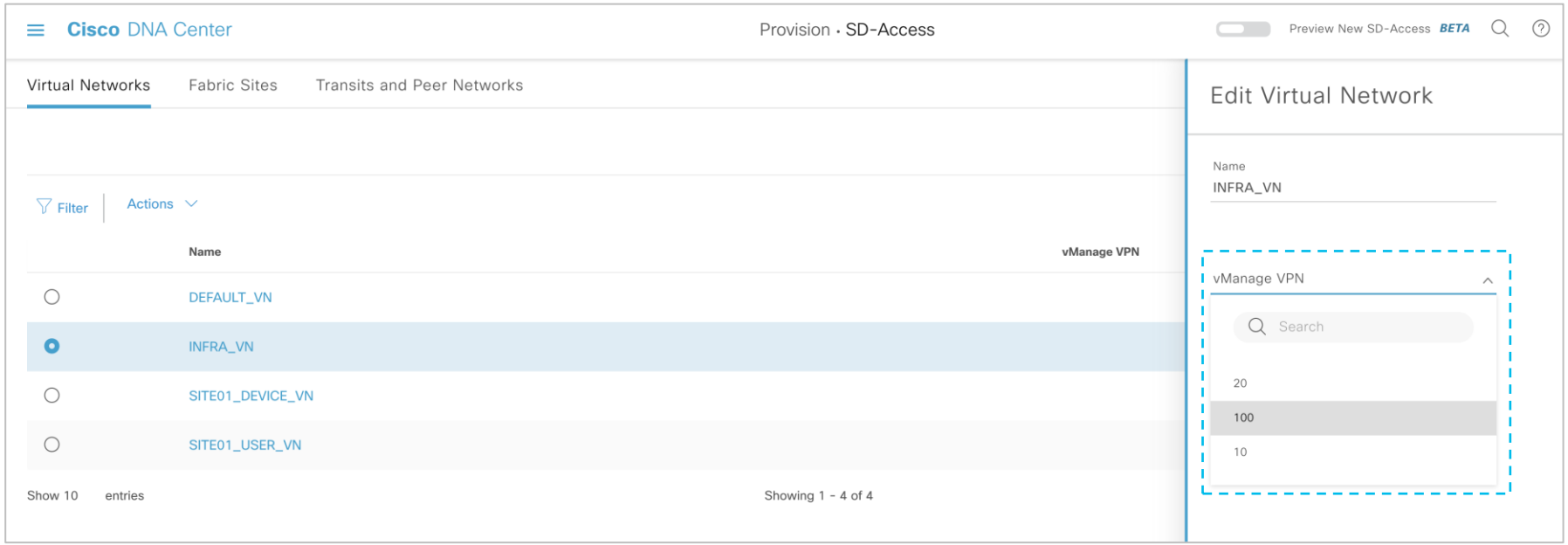
Make sure that a site to which device is assigned, has SNMP and CLI credentials already configured or update credentials manually after assigning to the side.

SD-WAN cEdge in Cisco DNA Center



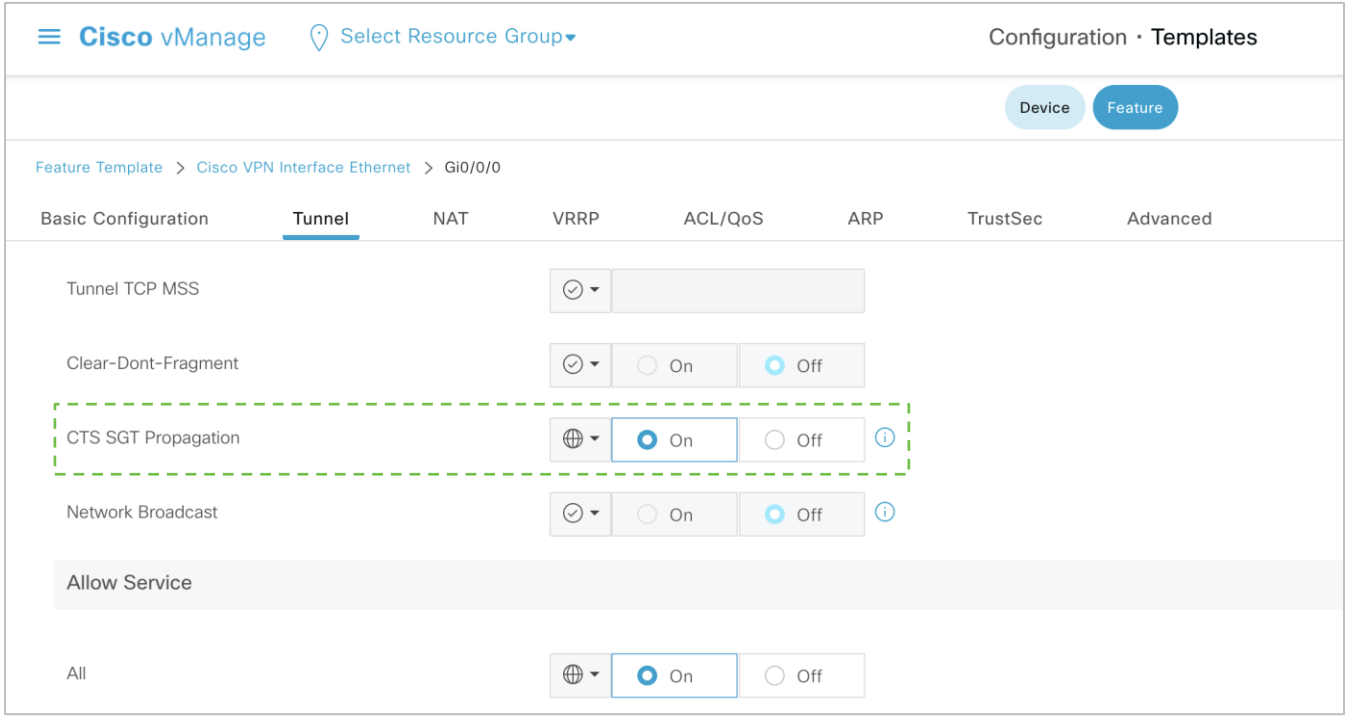
Prior proceeding with the next integration steps, make sure that device is **reachable** and in fully **managed** state.

SDA Virtual Network - SD-WAN VPN Mapping



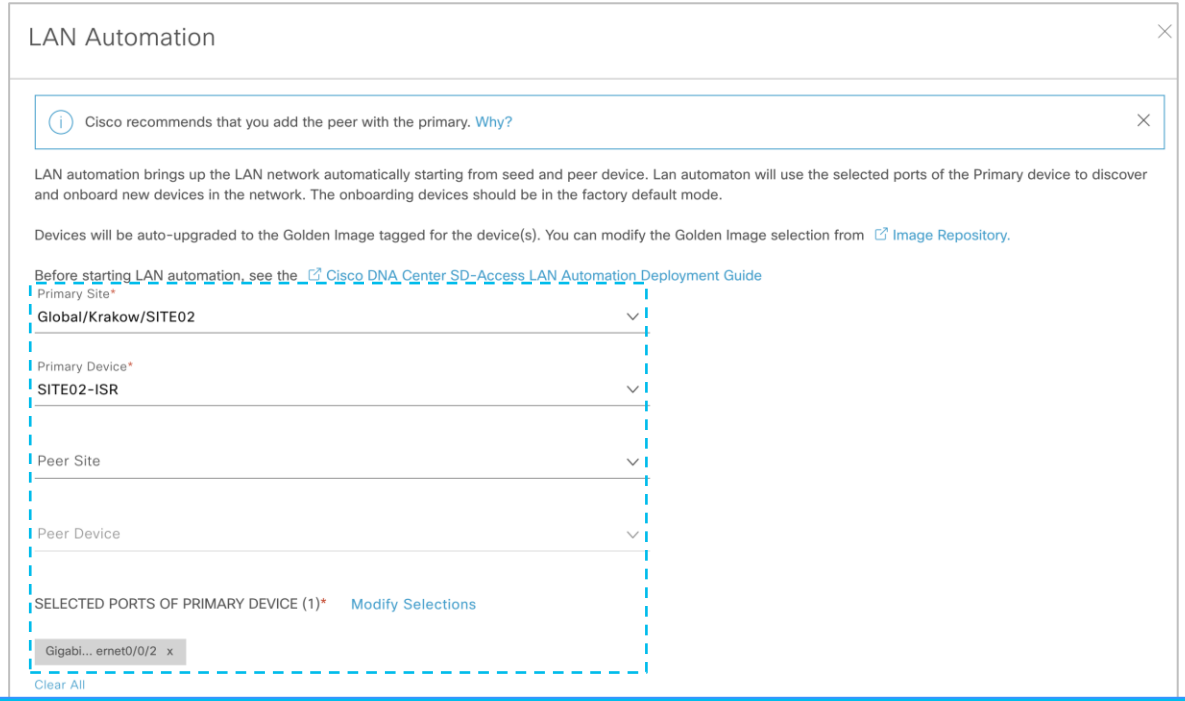
Prior proceeding with the next integration steps, make sure that you connect SDA and SD-WAN domain together by allocating SD-WAN VPN IDs to respective SDA VNs.

SD-WAN: integration state



CTS SGT Propagation needs to be enabled on VPN0 interface to allow CTS rewrite to IPSec header.

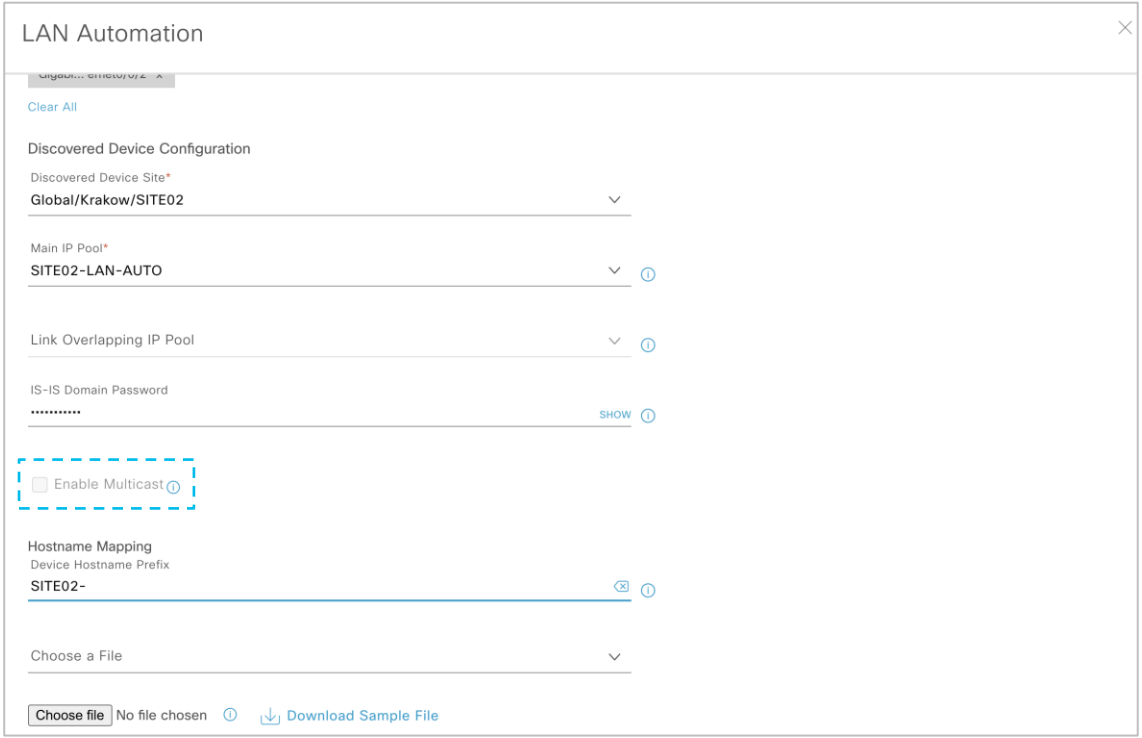
Enable LAN-Automation to on-board SDA Edge



While deploying LAN Automation, INFRA_VN configuration is added to SD-WAN cEdge router.

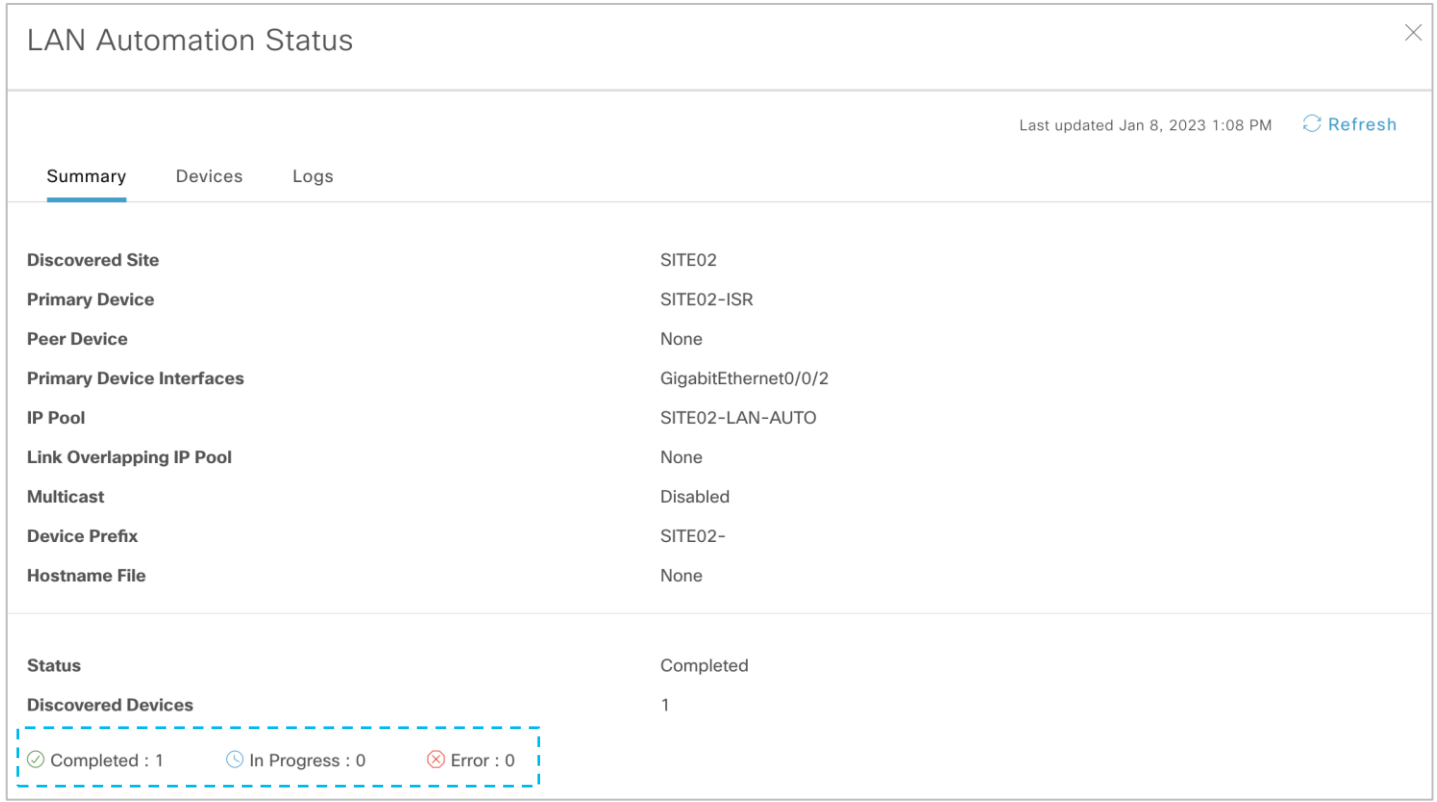
It is critical that deployed INFRA_VN subnet is properly routed to Cisco DNA Center from SD-WAN perspective (as otherwise PnP & LAN Automation will not work)

Enable LAN-Automation to on-board SDA Edge

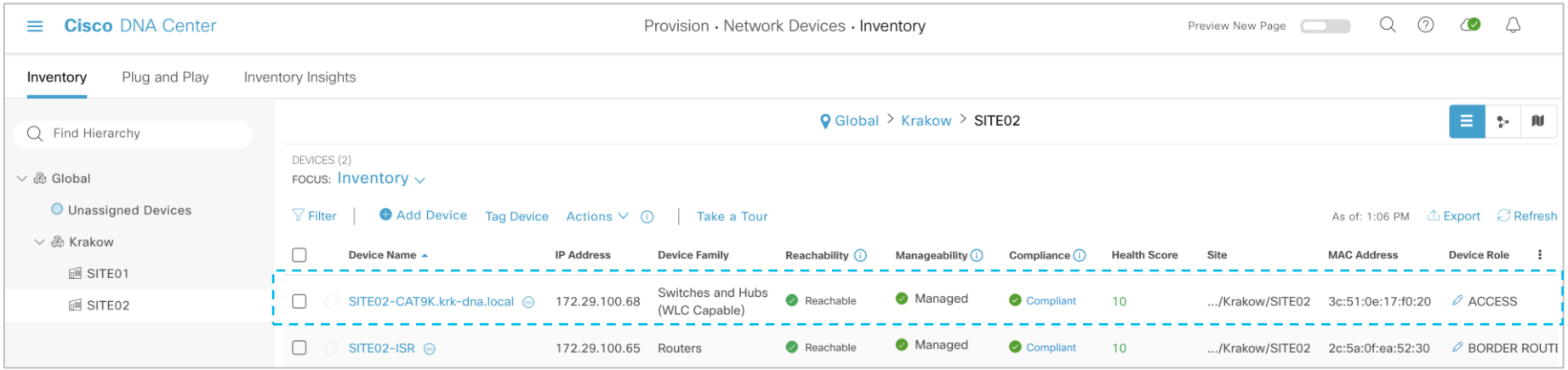


Multicast is not supported in SD-WAN – SDA Integrated Domain mode!

Enable LAN-Automation to on-board SDA Edge

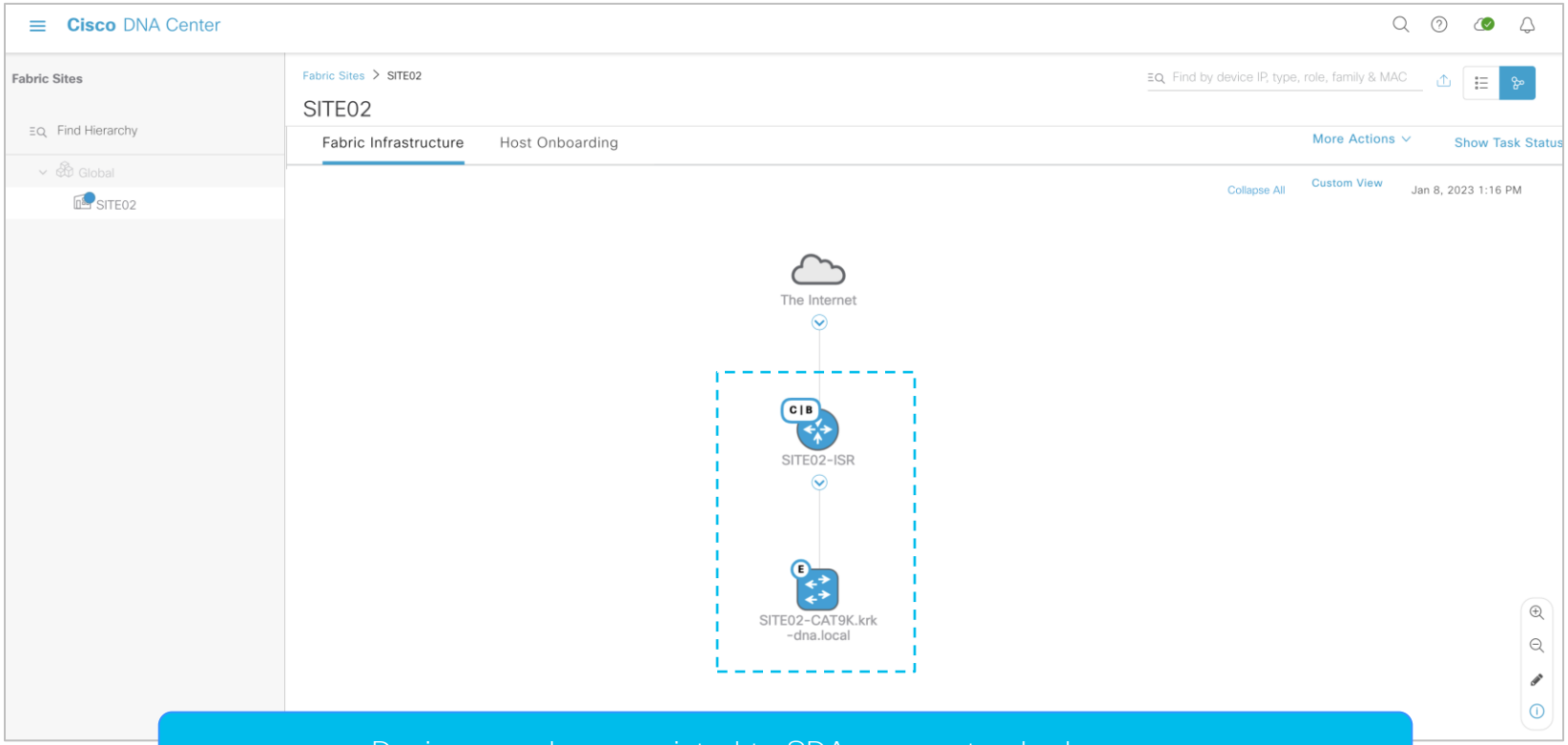


Enable LAN-Automation to on-board SDA Edge



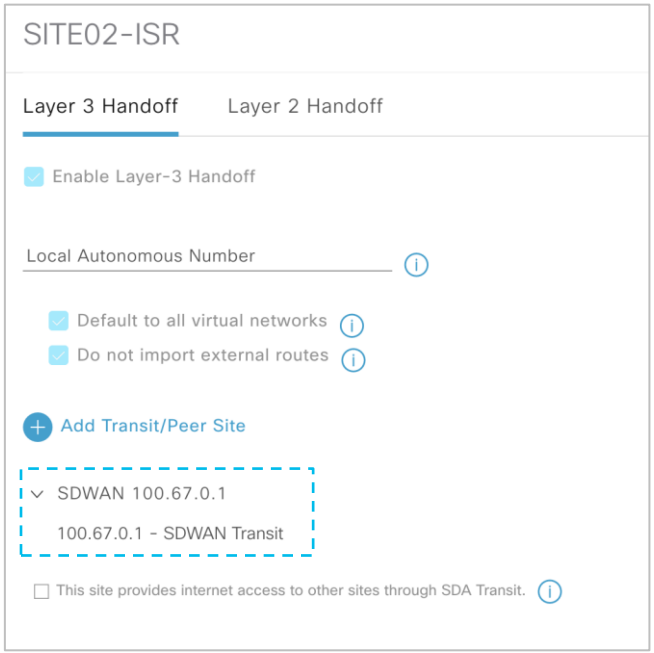
After successful LAN Automation, on-boarded device will be automatically added to Cisco DNA Center.

Configure SDA Fabric



Devices can be associated to SDA as per standard process.

Configure SDA Fabric



SD-WAN Transit will be automatically selected for SDA Border
(and cannot be removed)

Integrated Domain
Validation

cisco Live!

SDA - SD-WAN: integration validation

```
SITE02-ISR#show ip interface brief | in LISP|Loopback
LISP0                  unassigned      YES unset  up                    up
LISP0.4101             192.168.120.254 YES unset  up                    up
LISP0.4102             192.168.110.254 YES unset  up                    up
Loopback0              172.29.100.65   YES other  up                    up
Loopback1031           192.168.110.254 YES other  up                    up
Loopback1041           192.168.120.254 YES other  up                    up
Loopback65528          192.168.1.1     YES other  up                    up
```

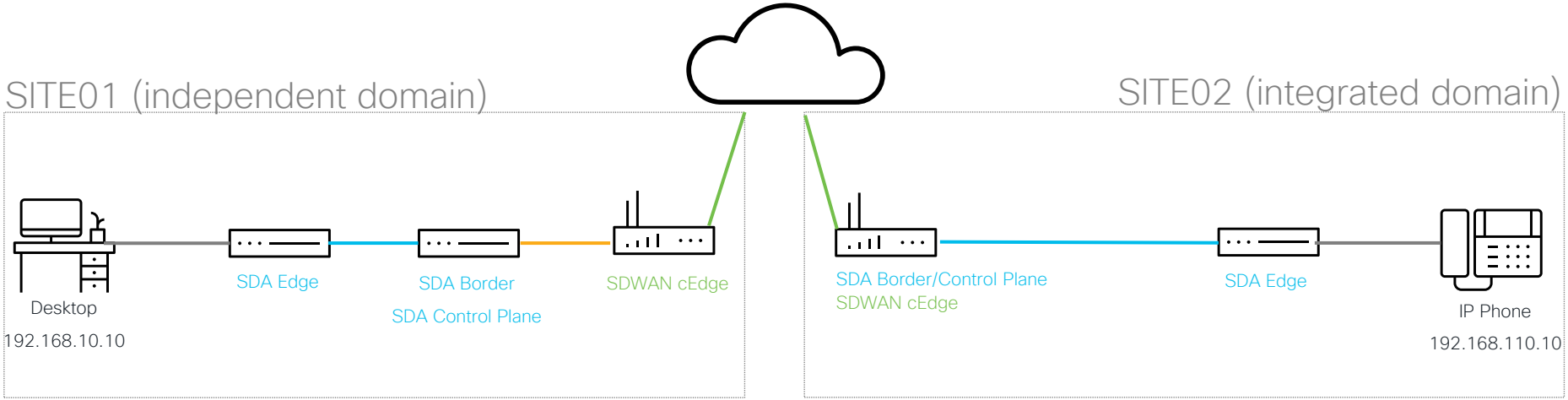
```
SITE02-ISR#show vrf
  Name                             Default RD          Protocols   Interfaces
  10                               1:10                ipv4,ipv6   Lo1031
                                                                   LI0.4102
  100                              1:100               ipv4,ipv6   Gi0/0/2
                                                                   Lo0
  20                               1:20                ipv4,ipv6   Lo1041
                                                                   LI0.4101
  65528                            <not set>           ipv4        Lo65528
  Mgmt-intf                        1:512               ipv4,ipv6   Gi0
```

Make sure that SD-WAN cEdge is fully configured as SDA Border and Control Plane including all required VNs and interfaces.

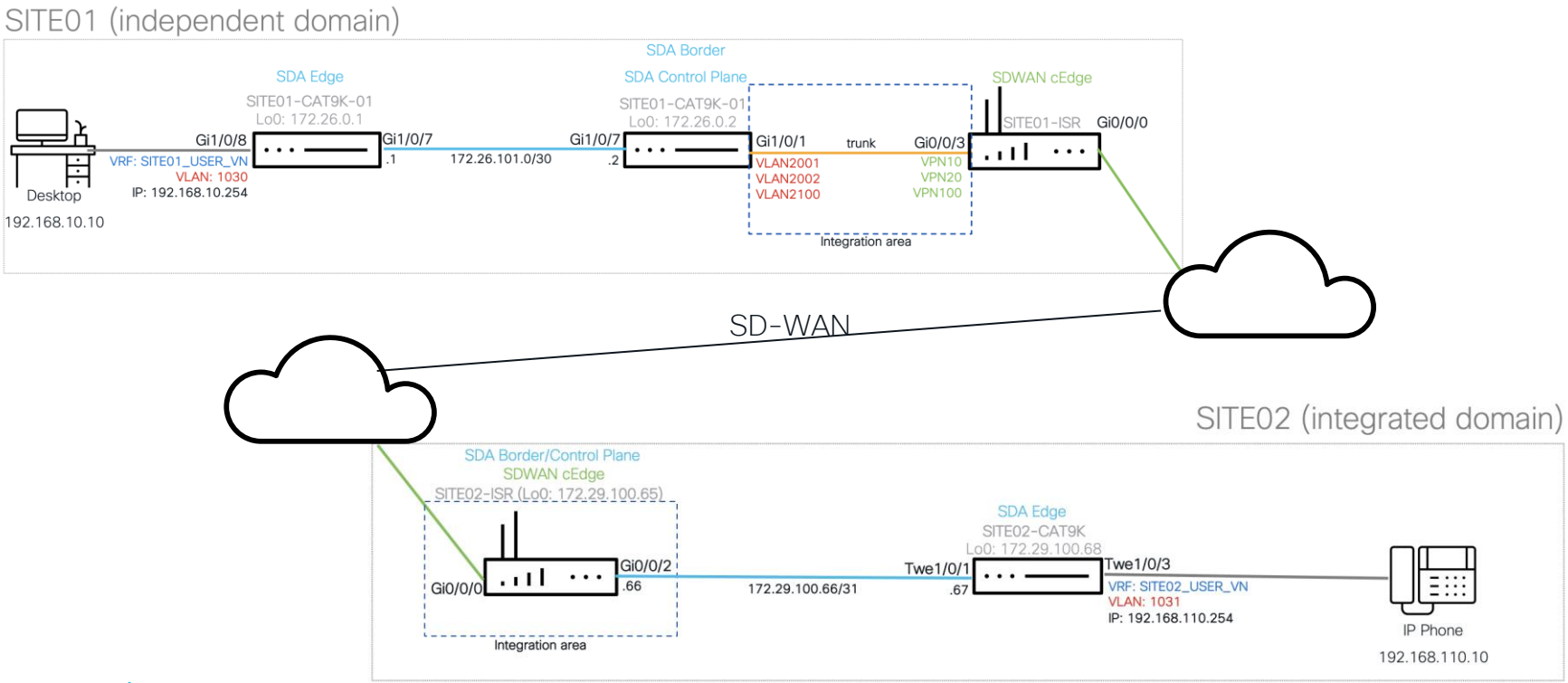
Network Troubleshooting

SDA – SD-WAN: Full Lab Setup

SDA
SD-WAN
manual TrustSec (VRF-lite)



SDA – SD-WAN: Full Lab Setup (details)



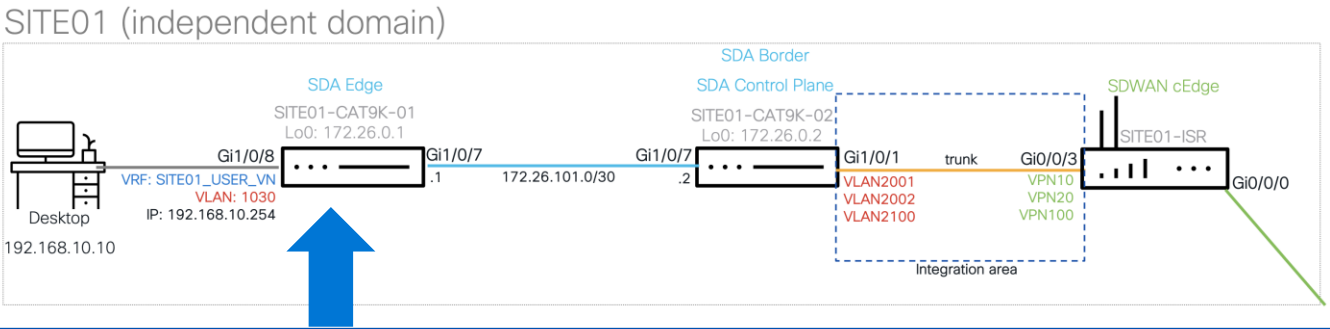
Troubleshooting SDA – SD-WAN integration

Interface configuration

cisco Live!

Troubleshooting Control plane (SDA – SDWAN)

End-Point facing configuration

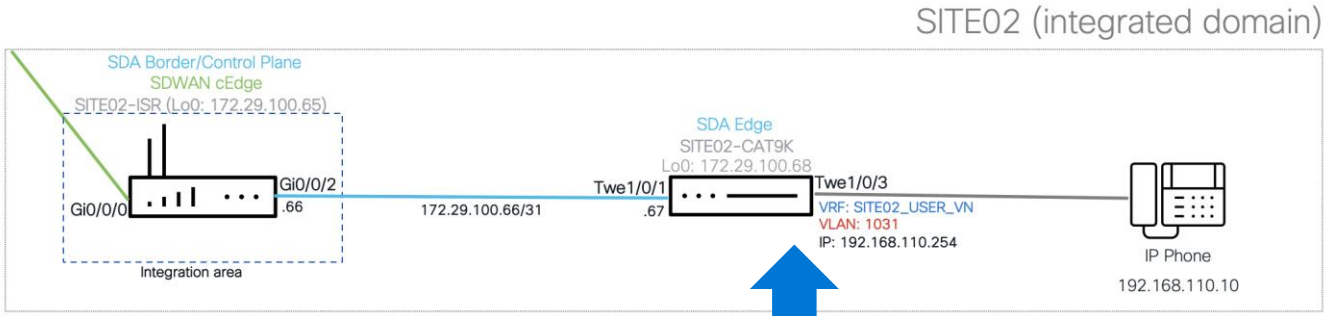



```
interface GigabitEthernet1/0/8
 switchport access vlan 1030
 switchport mode access
 device-tracking attach-policy IPDT_POLICY
 load-interval 30
 cts manual
  policy static sgt 5
  no propagate sgt
 no macro auto processing
 spanning-tree portfast
 spanning-tree bpduguard enable
end
```

```
interface Vlan1030
 description Configured from Cisco DNA-Center
 mac-address 0000.0c9f.f926
 vrf forwarding SITE01_USER_VN
 ip address 192.168.10.254 255.255.255.0
 ip helper-address 100.64.0.3
 no ip redirects
 ip route-cache same-interface
 no lisp mobility liveness test
 lisp mobility 192_168_10_0-SITE01_USER_VN-IPV4
end
```

Troubleshooting Control plane (SDA – SDWAN)

End-Point facing configuration




```
interface TwentyFiveGigE1/0/3
 switchport access vlan 1031
 switchport mode access
 load-interval 30
 cts manual
  policy static sgt 8
  no propagate sgt
 no macro auto processing
 spanning-tree portfast edge
 spanning-tree bpduguard enable
end
```

```
interface Vlan1031
 description Configured from Cisco DNA-Center
 mac-address 0000.0c9f.f608
 vrf forwarding SITE02_USER_VN
 ip address 192.168.110.254 255.255.255.0
 ip helper-address 100.64.0.3
 no ip redirects
 ip route-cache same-interface
 no lisp mobility liveness test
 lisp mobility 192_168_110_0-SITE02_USER_VN-IPV4
end
```

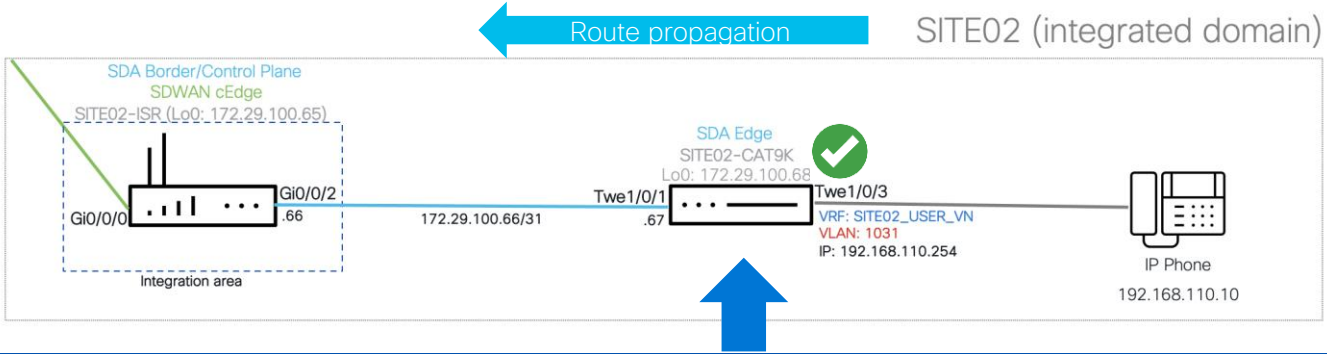
Troubleshooting SDA – SD-WAN integration

Control Plane checks

cisco Live!

Troubleshooting Control plane (SDA – SDWAN)

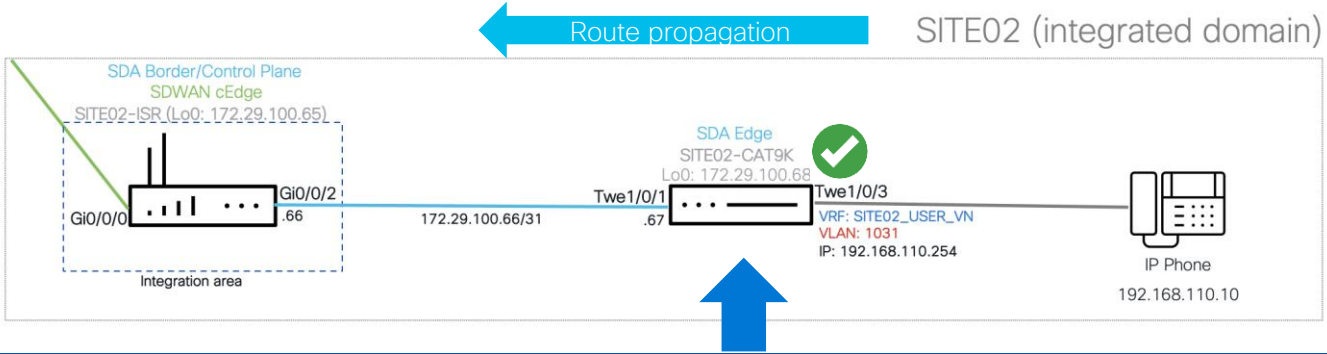
SITE02 - LISP checks




```
SITE02-CAT9K#show device-tracking database | b Network Layer
    Network Layer Address                  Link Layer Address     Interface  vlan       prlvl      age        state      Time left
L   192.168.120.254                        0000.0c9f.f0bc         Vl1041     1041       0100       40017mn    REACHABLE
L   192.168.110.254                        0000.0c9f.f608         Vl1031     1031       0100       40017mn    REACHABLE
ARP 192.168.110.10                         0000.4444.1111         Twe1/0/3   1031       0005       76s        REACHABLE  176 s try 0

SITE02-CAT9K#sh ip route vrf SITE02_USER_VN | b Gateway
Gateway of last resort is not set

      192.168.110.0/24 is variably subnetted, 3 subnets, 2 masks
C        192.168.110.0/24 is directly connected, Vlan1031
L        192.168.110.10/32 [10/1] via 192.168.110.10, 3w6d, Vlan1031
L        192.168.110.254/32 is directly connected, Vlan1031
```

Troubleshooting Control plane (SDA – SDWAN)

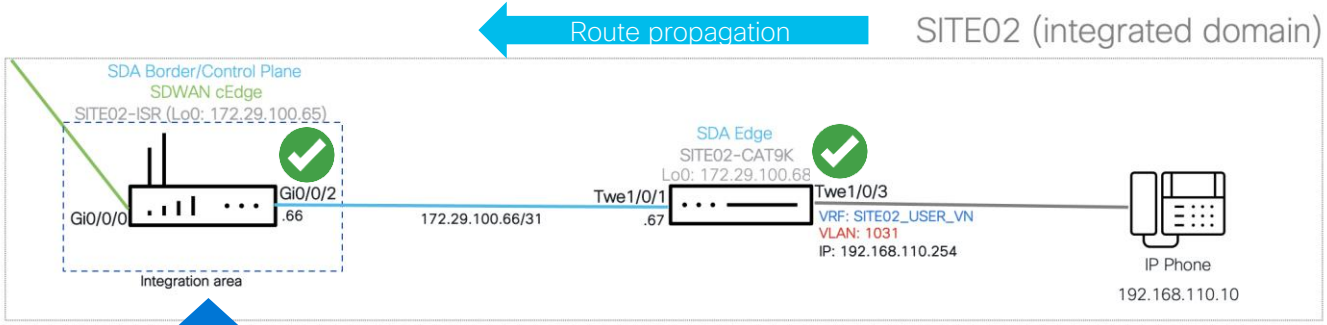
SITE02 - LISP checks




```
SITE02-CAT9K#sh lisp eid-table vrf SITE02_USER_VN ipv4 | in Instance
 Instance ID:                            4102
SITE02-CAT9K#
SITE02-CAT9K#show lisp instance-id 4102 ipv4 database 192.168.110.10/32
LISP ETR IPv4 Mapping Database for EID-table vrf SITE02_USER_VN (IID 4102), LSBs: 0x1
Entries total 2, no-route 0, inactive 0, do-not-register 1

192.168.110.10/32, dynamic-eid 192_168_110_0-SITE02_USER_VN-IPV4, inherited from default locator-set rloc_ca39f84e-3ef1-4dd3-ac21-5f775cad6b0b
  Uptime: 18:10:32, Last-change: 18:10:32
  Domain-ID: unset
  Service-Insertion: N/A (0)
  Locator        Pri/Wgt  Source     State
  172.29.100.68   10/10   cfg-intf   site-self, reachable
  Map-server       Uptime         ACK  Domain-ID
  172.29.100.65    18:10:32       Yes  0
```

Troubleshooting Control plane (SDA – SDWAN)

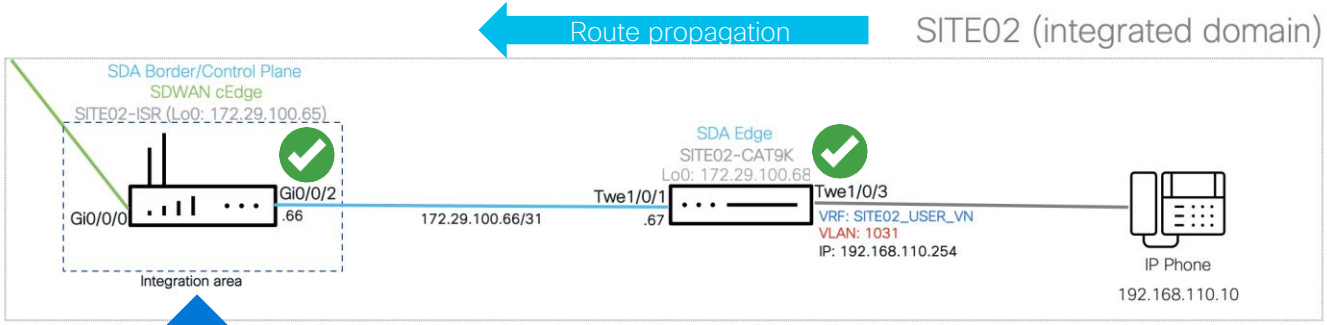
SITE02 - LISP checks




```
SITE02-ISR#sh lisp instance-id 4102 ipv4 server
LISP Site Registration Information
* = Some locators are down or unreachable
# = Some registrations are sourced by reliable transport

Site Name      Last      Up     Who Last            Inst     EID Prefix
               Register         Registered          ID
site_uci       never     no     --                  4102     192.168.110.0/24
               3w6d      yes#   172.29.100.68:46954 4102     192.168.110.10/32
SITE02-ISR#
SITE02-ISR#sh lisp instance-id 4102 ipv4 map-cache
LISP IPv4 Mapping Cache for EID-table vrf 10 (IID 4102), 1 entries

192.168.110.10/32, uptime: 2w5d, expires: never, via site-registration, send-map-request
  Negative cache entry, action: send-map-request
```

Troubleshooting Control plane (SDA – SDWAN)

SITE02 - RIB checks

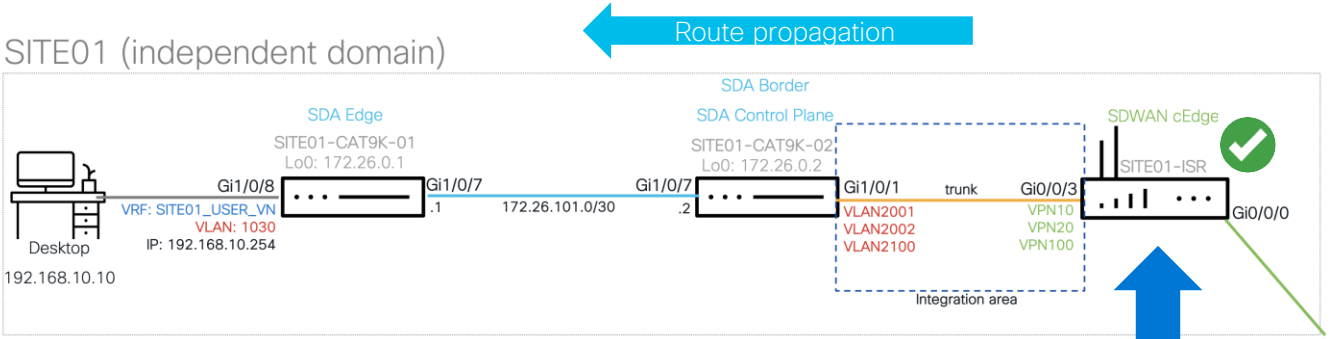



```
SITE02-ISR#sh run | sec instance-id 4102
 instance-id 4102
  remote-rloc-probe on-route-change
  service ipv4
   eid-table vrf 10
   route-export site-registrations
   distance site-registrations 252
   map-cache site-registration
   exit-service-ipv4
  !
```

```
SITE02-ISR#sh ip route vrf 10 192.168.110.10

Routing Table: 10
Routing entry for 192.168.110.10/32
  Known via "lisp", distance 252, metric 1, type intra area
  Redistributing via omp
  Routing Descriptor Blocks:
  * directly connected, via Null0
      Route metric is 1, traffic share count is 1
```

Troubleshooting Control plane (SDA – SDWAN)

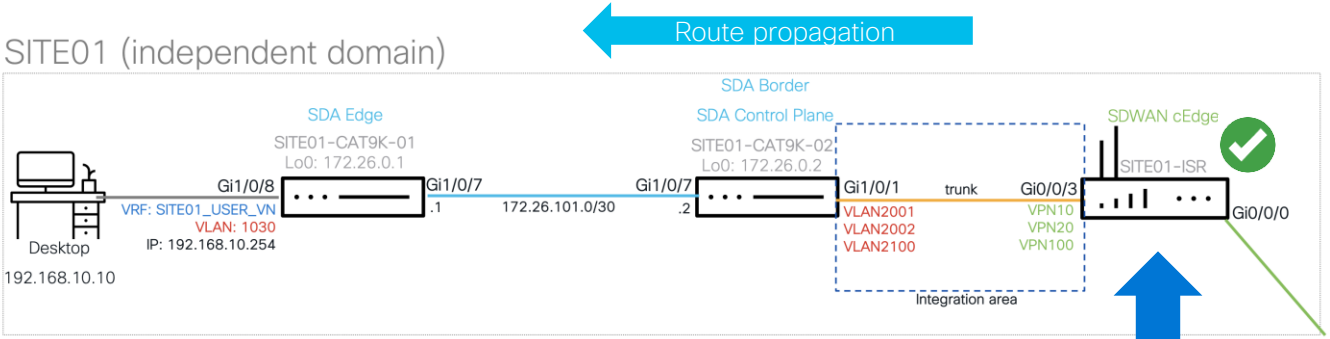
SITE01 - RIB checks




```
SITE01-ISR#show ip route vrf 10 192.168.110.10

Routing Table: 10
Routing entry for 192.168.110.10/32
  Known via "omp", distance 251, metric 0, type omp
  Redistributing via bgp 65000
  Advertised by bgp 65000
  Last update from 172.29.0.100 on Sdwan-system-intf, 17:01:25 ago
  Routing Descriptor Blocks:
  * 172.29.0.100 (default), from 172.29.0.100, 17:01:25 ago, via Sdwan-system-intf
      Route metric is 0, traffic share count is 1
```

Troubleshooting Control plane (SDA – SDWAN)

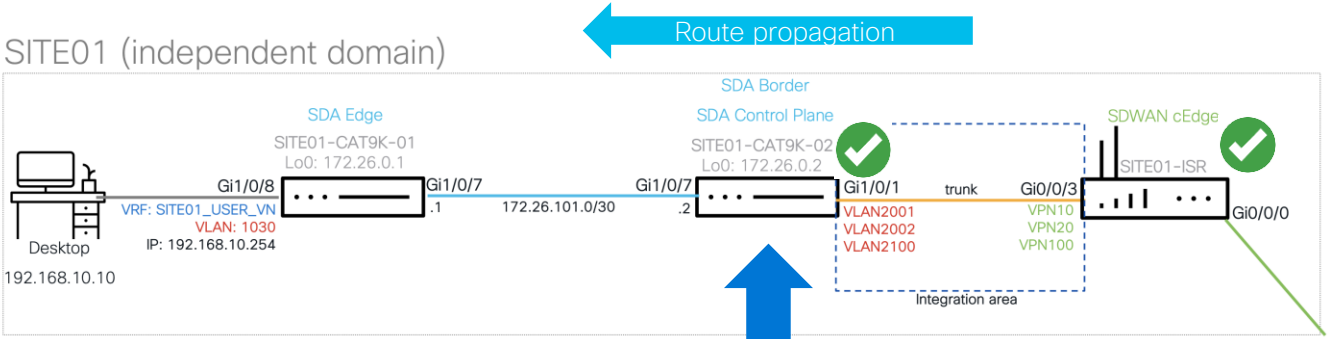
SITE01 - BGP checks




```
SITE01-ISR#show ip bgp vpnv4 vrf 10 neighbors 172.26.100.1 advertised-routes 192.168.110.10/32
Route Distinguisher: 1:10 (default for vrf 10)
BGP routing table entry for 1:10:192.168.110.10/32, version 79
  Paths: (1 available, best #1, table 10)
  Advertised Attributes
    Local Preference: 0
    Metric: 1000
    Origin: incomplete
    AS-Path:  65000
    Nexthop: 172.26.100.2
```

Troubleshooting Control plane (SDA – SDWAN)

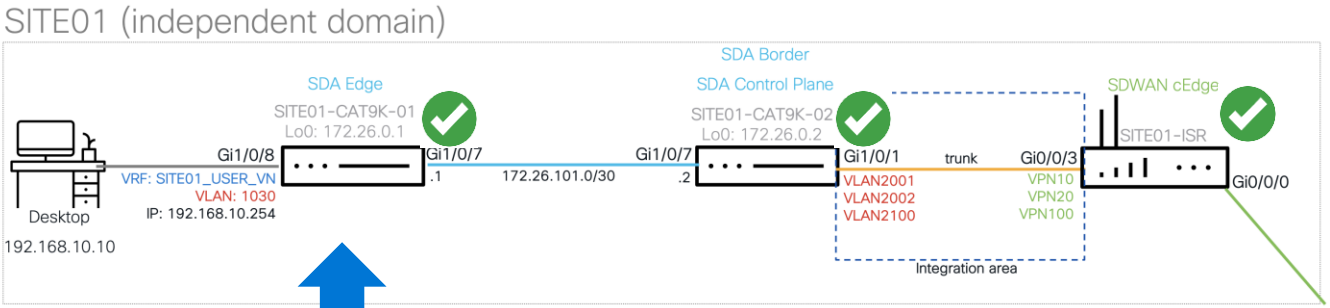
SITE01 - RIB checks




```
SITE01-CAT9K-02#show ip route vrf SITE01_USER_VN 192.168.110.10

Routing Table: SITE01_USER_VN
Routing entry for 192.168.110.10/32
  Known via "bgp 65100", distance 20, metric 1000
  Tag 65000, type external
  Last update from 172.26.100.2 16:57:13 ago
  Routing Descriptor Blocks:
  * 172.26.100.2, from 172.26.100.2, 16:57:13 ago
      opaque_ptr 0x7FBBF8FAAF80
      Route metric is 1000, traffic share count is 1
      AS Hops 1
      Route tag 65000
      MPLS label: none
      MPLS Flags: NSF
```

As SDA Border is a default border, route is no longer propagated in LISP!

SDA – SD-WAN: SITE01 - LISP checks




```
SITE01-CAT9K-01#lig instance-id 4099 192.168.110.10
Mapping information for EID 192.168.110.10 from 172.26.0.2 with RTT 1 msecs
192.168.64.0/18, uptime: 00:00:13, expires: 00:14:59, via map-reply, forward-native
  Encapsulating to proxy ETR
SITE01-CAT9K-01#
SITE01-CAT9K-01#show lisp instance-id 4099 ipv4 map-cache 192.168.110.10
LISP IPv4 Mapping Cache for EID-table vrf SITE01_USER_VN (IID 4099), 3 entries

192.168.64.0/18, uptime: 00:00:17, expires: 00:14:55, via map-reply, forward-native
  Sources: map-reply
  State: forward-native, last modified: 00:00:17, map-source: 172.26.0.2
  Active, Packets out: 0(0 bytes), counters are not accurate
  Encapsulating to proxy ETR
```

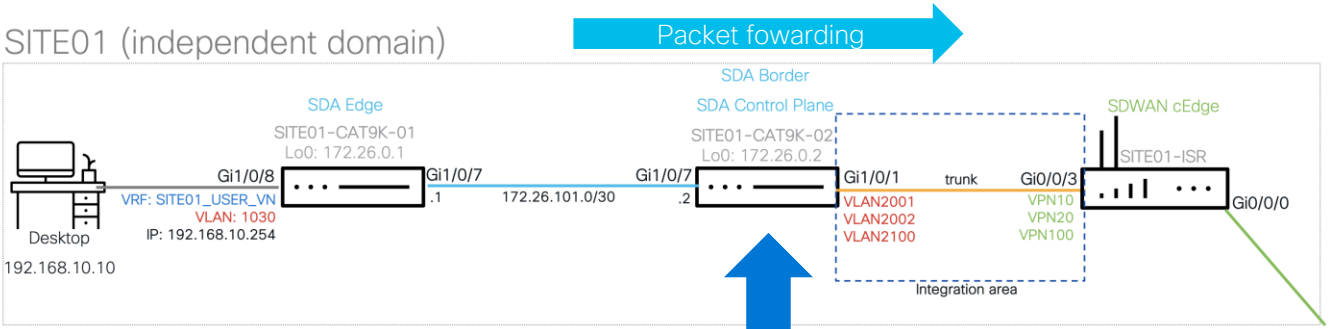
Troubleshooting SDA – SD-WAN integration

Data Plane checks

cisco Live!

Data Plane Tools

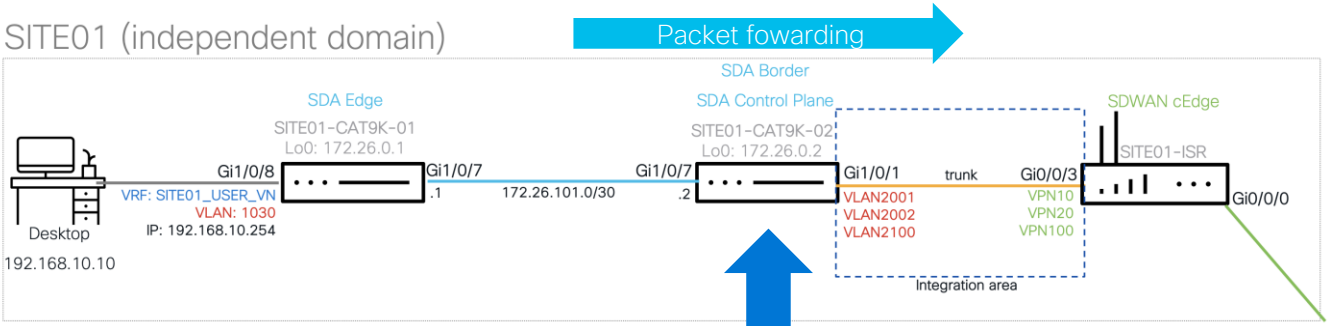
Cat9000 Series: Embedded Packet Capture




```
SITE01-CAT9K-02#monitor capture SDA interface gi1/0/1 out match ipv4 host 192.168.10.10 host 192.168.110.10 buffer size 10 start
SITE01-CAT9K-02#! send packets
SITE01-CAT9K-02#monitor capture SDA stop
Capture statistics collected at software:
       Capture duration - 11 seconds
       Packets received - 100
       Packets dropped - 0
       Packets oversized - 0

Bytes dropped in asic - 0

Capture buffer will exists till exported or cleared

Stopped capture point : SDA
```

Data Plane Tools

Cat9000 Series: Embedded Packet Capture




```
SITE01-CAT9K-02#show monitor capture SDA buffer display-filter frame.number==1
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

   1   0.000000 192.168.10.10 -> 192.168.110.10 ICMP 122 Echo (ping) request  id=0x14b1, seq=0/0, ttl=253

SITE01-CAT9K-02#show monitor capture SDA buffer display-filter frame.number==1 dump
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

0000  ff ff ff ff ff ff 7c 21 0d bd 00 00 89 09 01 01   ......|!........
0010  00 01 00 05 08 00 45 00 00 64 d2 e3 00 00 fd 01   ......E..d......
0020  f1 4f c0 a8 0a 0a c0 a8 6e 0a 08 00 1b d2 14 b1   .O......n.......
0030  00 00 00 00 00 00 09 6d 44 5a ab cd ab cd ab cd   .......mDZ......
0040  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0050  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0060  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0070  ab cd ab cd ab cd ab cd ab cd                     ..........
```

Embedded Packet Capture (EPC) allows to capture packets that are forwarded fully in the hardware!

Data Plane Tools

wireshark analysis

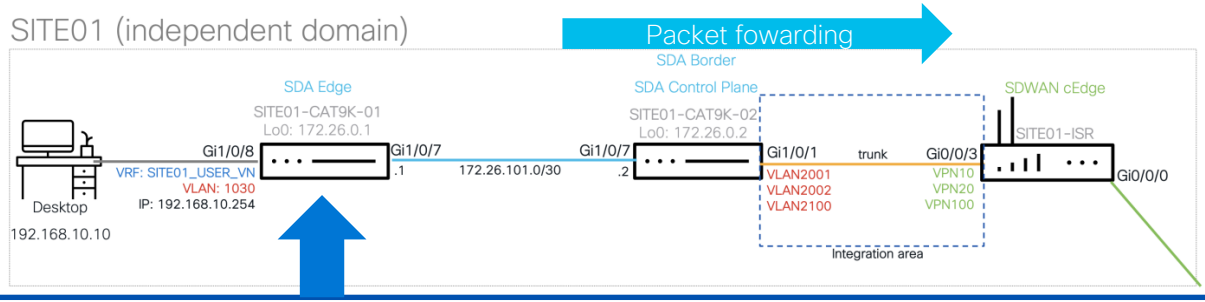
```
> Frame 1: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
> Ethernet II, Src: Cisco_bd:00:00 (7c:21:0d:bd:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Cisco MetaData
    Version: 1
    Length: 1
    Options: 0x0001
    SGT: 5
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.110.10
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 100
    Identification: 0xd2e3 (53987)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 253
    Protocol: ICMP (1)
    Header Checksum: 0xf14f [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.10.10
    Destination Address: 192.168.110.10
> Internet Control Message Protocol
```

Cisco MetaData header

Original Packet & Payload

Embedded Packet Capture (EPC) on ingress is fully reliable!
EPC on egress interface might not provide the final frame (above – missing dot1q header)

Data Plane Tools
Catalyst 9000 Series: Show Platform Forward

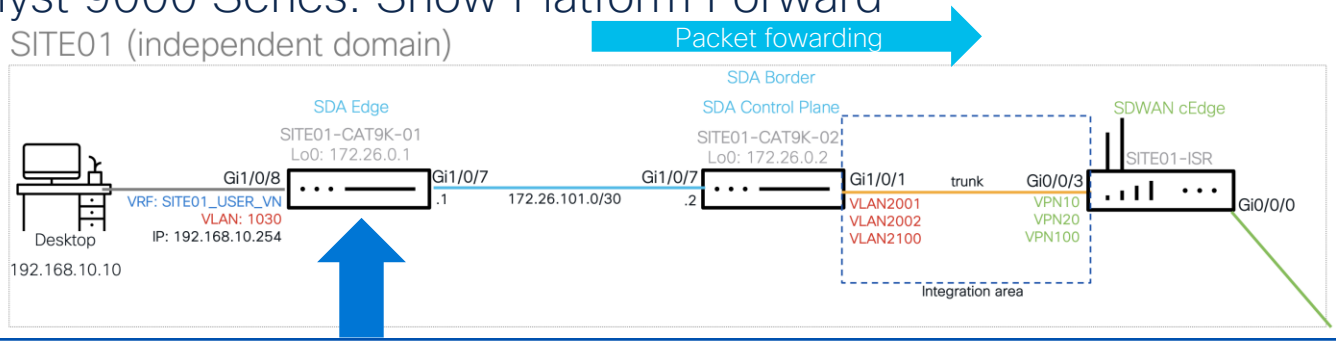



```
SITE01-CAT9K-01#monitor capture SDA interface gi1/0/8 in match ipv4 host 192.168.10.10 host 192.168.110.10
SITE01-CAT9K-01#monitor capture SDA file location flash:capture.pcap start
SITE01-CAT9K-01#! send packets
SITE01-CAT9K-01#monitor capture SDA stop
Capture statistics collected at software:
        Capture duration - 14 seconds
        Packets received - 100
        Packets dropped - 0
        Packets oversized - 0

Bytes dropped in asic - 0

Stopped capture point : SDA
SITE01-CAT9K-01#show platform hardware fed switch 1 forward interface gi1/0/8 pcap flash:capture.pcap number 1 data
Show forward is running in the background. After completion, syslog will be generated.
```

The fastest way to run “Show Platform Forward” is to first capture exact traffic via EPC (SPF) and then use it as a trigger in SPF execution.

Data Plane Tools

Catalyst 9000 Series: Show Platform Forward



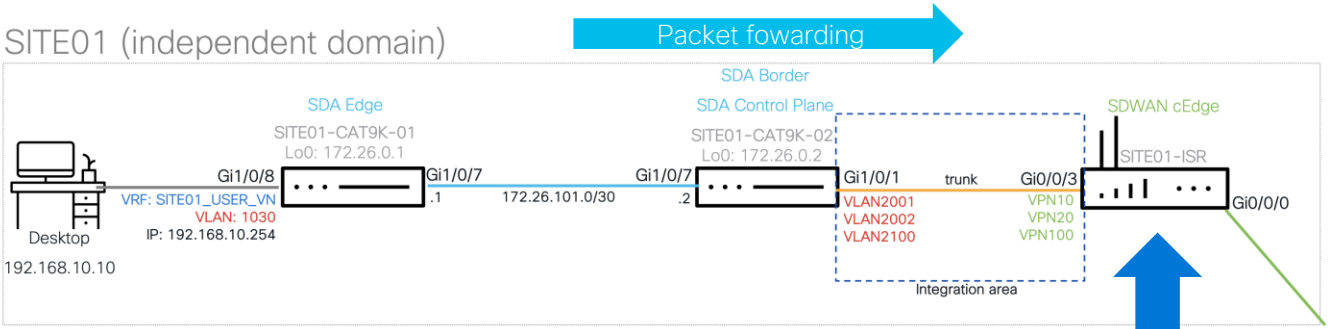

```
SITE01-CAT9K-01#show platform hardware fed switch 1 forward last summary
Input Packet Details:
###[ Ethernet ]###
  dst       = 00:00:0c:9f:f9:26
  src       = 00:00:00:00:00:01
  type      = 0x800
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 100
     id        = 53746
     flags     =
     frag      = 0
     ttl       = 254
     proto     = icmp
     chksum    = 0xf140
     src       = 192.168.10.10
     dst       = 192.168.110.10
```

```
Output Packet Details:
   Port                    : GigabitEthernet1/0/7
###[ Ethernet ]###
  dst       = 6c:4e:f6:70:93:40
  src       = 7c:21:0d:bd:a3:c0
  type      = 0x800
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 150
     id        = 48360
     flags     = DF
     frag      = 0
     ttl       = 253
     proto     = udp
     chksum    = 0x6836
     src       = 172.26.0.1
     dst       = 172.26.0.2
     options   = ''
```

Show Platform Forward (SPF) shows hardware forwarding decision, as well as ingress/egress packet dump (all headers).

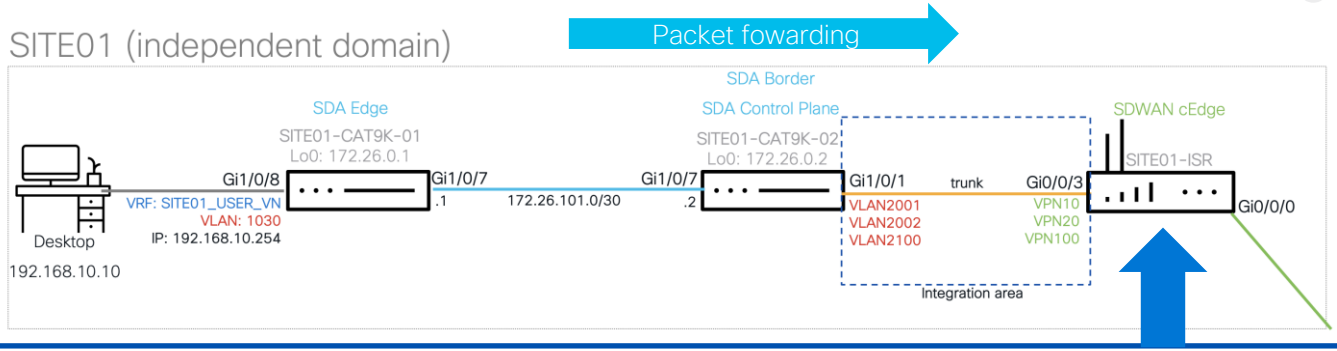
Data Plane Tools

Packet Trace




```
SITE01-ISR#debug platform packet-trace copy packet both size 2048
SITE01-ISR#debug platform packet-trace packet 8192 circular data-size 16384 fia-trace
 Please remember to turn on 'debug platform condition start' for packet-trace to work
SITE01-ISR#debug platform condition interface Gig 0/0/3.2001 ipv4 192.168.110.10/32 ingress
SITE01-ISR#debug platform condition start
SITE01-ISR#! wait for packets
SITE01-ISR#debug platform condition stop
```

Data Plane Tools
Packet Trace




```
SITE01-ISR#show platform packet-trace packet 0 decode
Packet: 0           CBUG ID: 402
Summary
  Input     : GigabitEthernet0/0/3.2001
  Output    : GigabitEthernet0/0/0
  State     : FWD
  Timestamp
    Start   : 290159962056467 ns (01/08/2
    Stop    : 290159962133250 ns (01/08/2
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet0/0/3.20
    Output      : <unknown>
    Source      : 192.168.10.10
    Destination : 192.168.110.10
    Protocol    : 1 (ICMP)
  Feature: DEBUG_COND_INPUT_PKT
    Entry       : Input - 0x116930b8
    Input       : GigabitEthernet0/0/3.20
    Output      : <unknown>
    Lapsed time : 379 ns
```

```
Packet Copy In
  c4b23902 46936c4e f670934c 810007d1 8909010
  0000fc01 f42ac0a8 0a0ac0a8 6e0a0800 5124146
  abcdabcd abcdabcd abcdabcd abcdabcd abcdabc
  abcdabcd abcdabcd abcdabcd abcdabcd abcdabc
  ARPA
    Destination MAC     : c4b2.3902.4693
    Source MAC          : 6c4e.f670.934c
    Type                : 0x8100 (DOT1Q)
  DOT1Q
    VLAN ID             : 2001
    Canonical Form Ind  : 0
    Priority            : 0
    Type                : 0x8909 (CMD)
  CMD
    Version             : 1
    Length              : 1
    Option Length       : 0
    Option              : 0x1 (CTS)
    CTS SGT             : 5
    Type                : 0x0800 (IPV4)
```

```
Packet Copy Out
  7c210d1d ac54c4b2 39024690 08004500 00a2abfb 4000ff11 6915ac1a 0501ac1d
  09013062 308a008e 00000400 01100000 01930000 0000dff2 83ec3ee1 7d383892
  4f59209f cee9af1a d93e5714 e5b0b6c4 ab9e6798 1de57ffc 09b9155f cdb28dc7
  8fb834a0 3ce4bdc8 bd6112c1 b34a6c9b ec639729 17e77435 3d474e96 a63a88e5
  3ac7f9fa fd57d97a ab73f1a0 3feca91a 09f18adc f37eba75 66a191fd e5f9c63d
  605e3edb 89b366d5 d56519cb dc012ea0
  ARPA
    Destination MAC     : 7c21.0d1d.ac54
    Source MAC          : c4b2.3902.4690
    Type                : 0x0800 (IPV4)
  IPv4
    Version             : 4
    Header Length       : 5
    ToS                 : 0x00
    Total Length        : 162
    Identifier          : 0xabfb
    IP Flags            : 0x2 (Don't fragment)
    Frag Offset         : 0
    TTL                 : 255
    Protocol            : 17 (UDP)
    Header Checksum     : 0x6915
    Source Address      : 172.26.5.1
    Destination Address : 172.29.9.1
```

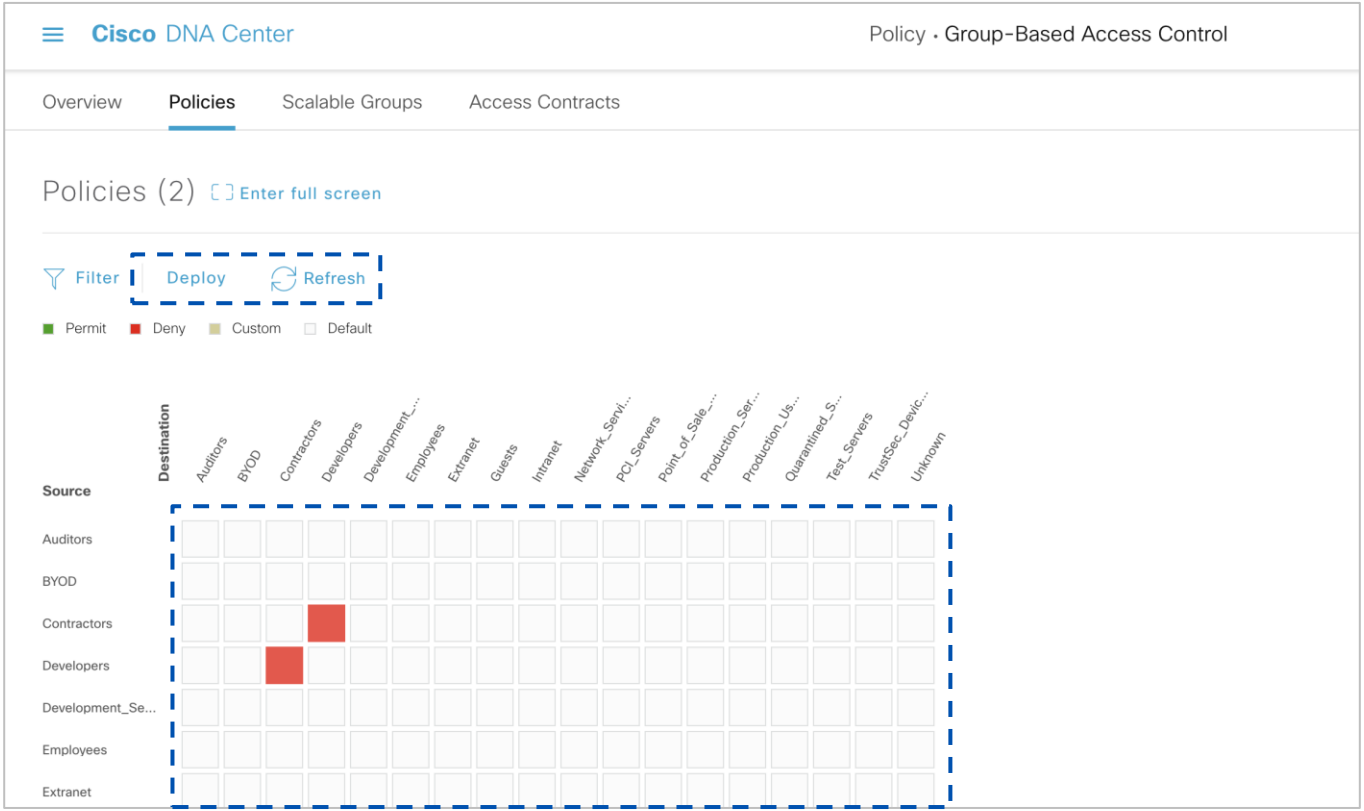
Troubleshooting SDA – SD-WAN integration

Security Plane checks

cisco Live!

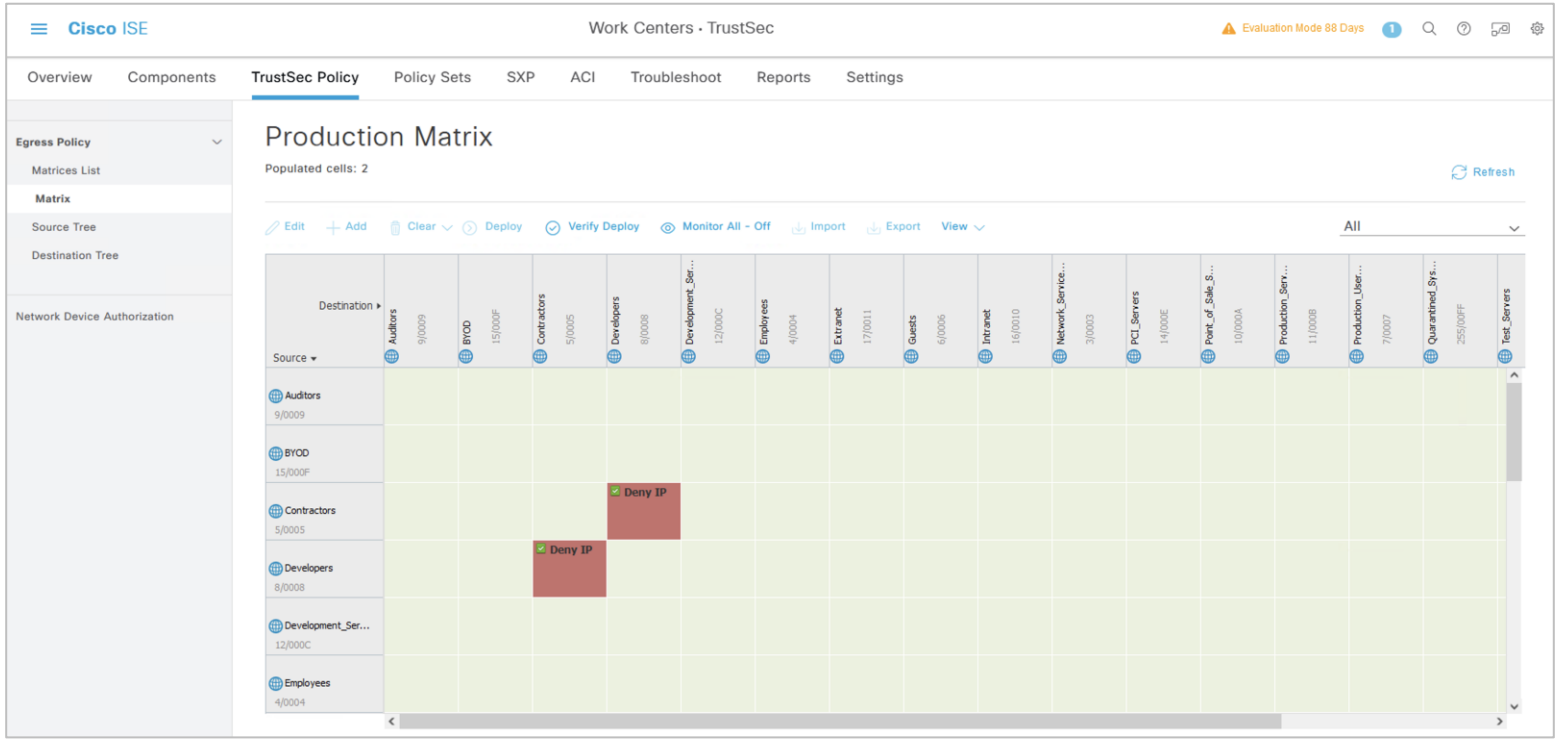
Security Plane validation

Cisco DNA Center



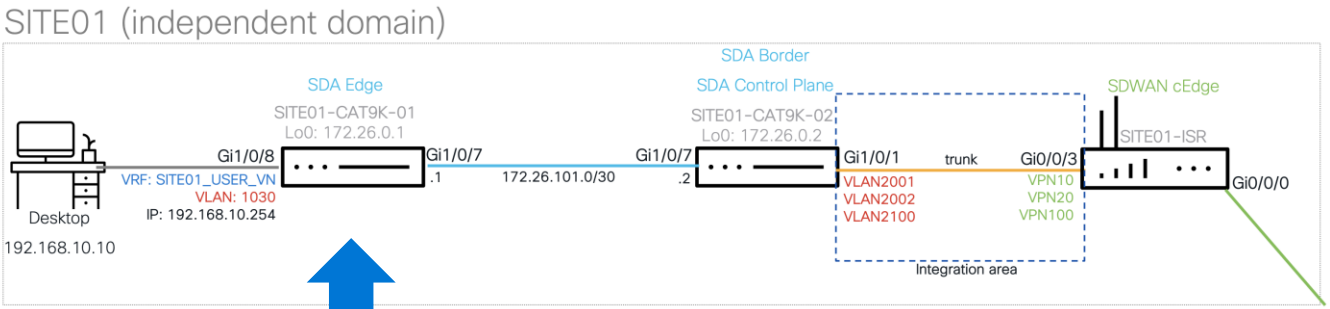
Security Plane validation

Cisco ISE



Security Plane validation

SDA Edge to ISE communication



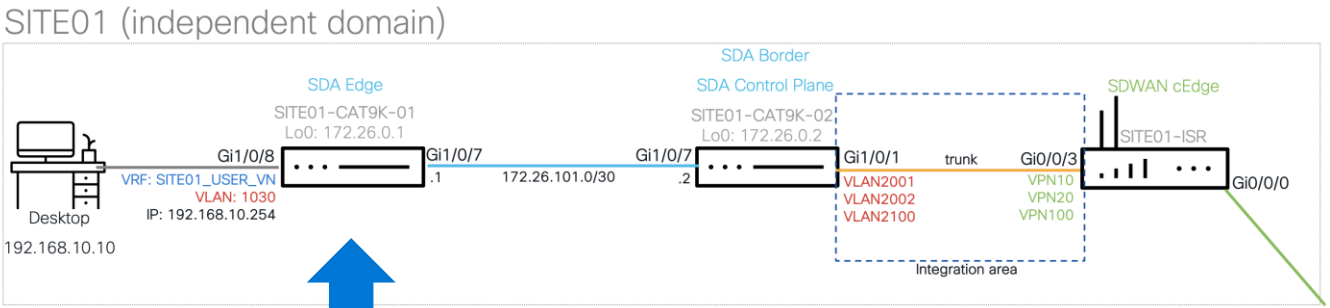

```
SITE01-CAT9K-01#sh cts pacs
AID: 14908C13AE989650BD871CF0CE9E81AD
PAC-Info:
  PAC-type = Cisco Trustsec
  AID: 14908C13AE989650BD871CF0CE9E81AD
  I-ID: FOC2340X0DV
  A-ID-Info: Identity Services Engine
  Credential Lifetime: 23:40:28 UTC Fri Apr 07 2023
PAC-Opaque: 000200B800030001000400101 4908C13AE989650BD
0FF2DBD9777072D2FABC969395C0D15CAC58B03D88F343D3EBAEF7
E60EB509FA9BDBD5B6CB925D0AC5815F002F056FE78D6D3BF8736B
Refresh timer is set for 12w4d
```

```
SITE01-CAT9K-01#show cts env
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Service Info Table:
Local Device SGT:
  SGT tag = 2-00:TrustSec_Devices
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 100.64.0.102, port 1812, A-ID 14908C13AE989650BD871CF0CE9E81AD
          Status = ALIVE
          auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
```

PAC = Protected Access Credentials

Security Plane validation

Ingress SDA Edge :: ingress tagging

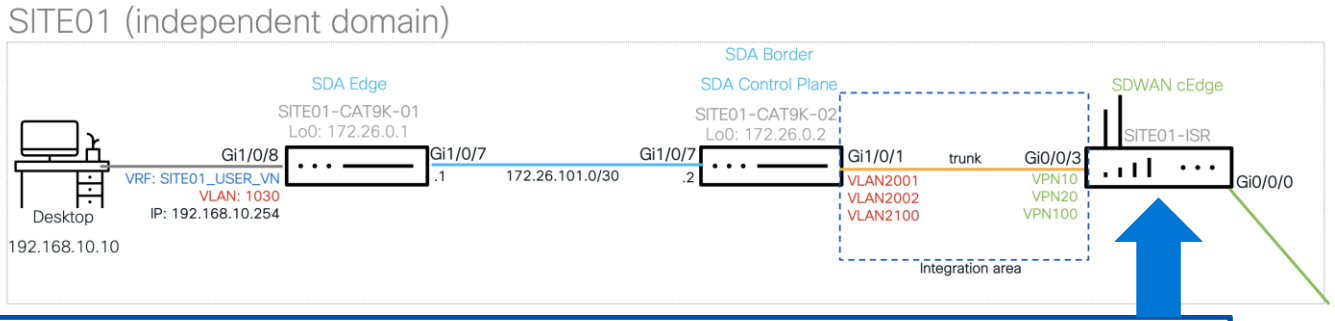



```
SITE01-CAT9K-01#sh cts role-based sgt-map vrf SITE01_USER_VN host 192.168.10.10
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
192.168.10.10           5       LOCAL
```

SGT source tag is added on ingress port and carried through to the final destination.

Security Plane validation

SGT propagation to SD-WAN

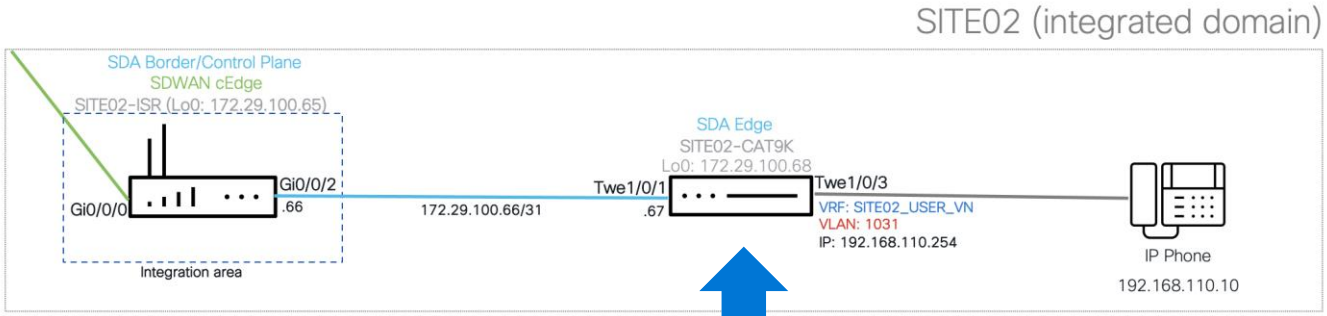



```
SITE01-ISR#show platform hardware qfp active feature cts client interface
Interface GigabitEthernet0/0/3(10):
        Enable=1, Policy=0, Trust=0, Propagate=0, Internal=0
         SGT=0, SGT_caching_in=0 SGT_caching_eg=0
         IN_dbg/ IN_err=0/0, OUT_dbg/ OUT_err=0/0

Interface Tunnel0(14):
        Enable=1, Policy=0, Trust=0, Propagate=1, Internal=0
         SGT=0, SGT_caching_in=0 SGT_caching_eg=0
         IN_dbg/ IN_err=0/0, OUT_dbg/ OUT_err=0/0
```

CTS SGT propagation is enabled on Tunnel0 interface

Security Plane validation

Egress SDA Edge :: egress enforcement

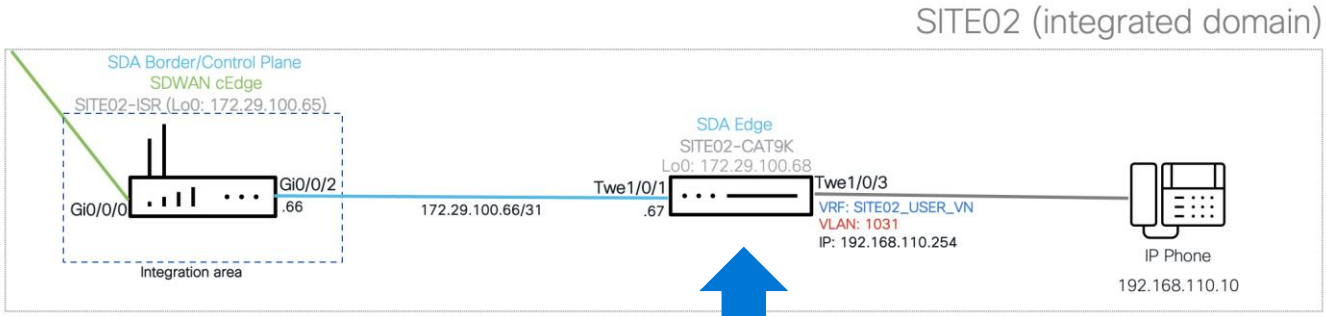



```
SITE02-CAT9K#sh cts role-based sgt-map vrf SITE02_USER_VN host 192.168.110.10
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
========================================
192.168.110.10          8       LOCAL
SITE02-CAT9K#
SITE02-CAT9K#sh cts role-based permissions from 5 to 8
IPv4 Role-based permissions from group 5:Contractors to group 8:Developers:
        Deny IP-00
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

SGT source tag (carried over in the packet header) and SGT destination tag (associated to the destination end-point) create a pair that points out to the specific policy.

Security Plane validation

Egress SDA Edge :: egress enforcement




```
SITE02-CAT9K#sh cts role-based counters from 5 to 8
Role-based IPv4 counters
From    To      SW-Denied       HW-Denied       SW-Permitt      HW-Permitt      SW-Monitor      HW-Monitor
5       8       0               100             0               0               0               0
```

Enforcement occurs on the egress device.
Number of packets dropped can be seen in the counters.

Summary

Prescriptive Deployment Guides

1) Cisco SD-Access - SD-WAN Integrated Domain Pairwise Integration

https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/Cisco-SD-Access-SD-WAN-Integrated-Domain-Guide.pdf

2) Cisco SD-Access - SD-WAN Independent Domain Pairwise Integration

https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/Cisco-SD-Access-SD-WAN-Independent-Domain-Guide.pdf

Troubleshoting deep dives

SDA:

BRKTRS-3820 - SD Access: Troubleshooting the Fabric

BRKTRS-3090 - Troubleshooting the Cisco Catalyst 9000 Series Switches

BRKTRS-2811 - Overview of Packet Capturing Tools in Cisco Switches and Routers

SD-WAN:

BRKTRS-3793 - Advanced SD-WAN Routing Troubleshooting

BRKTRS-3475 - Advanced Troubleshooting of cat8k,asr1k, ISR and SD-WAN Edge Made Easy

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.

- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.


cisco
The bridge to possible
Thank you
cisco Live!


CISCO Live!
ALL IN