White Paper

Network as a Sensor and Encrypted Traffic Analytics Integration

Software-Defined Access

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
https://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Contents

NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESSED OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT OR PRODUCTS ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

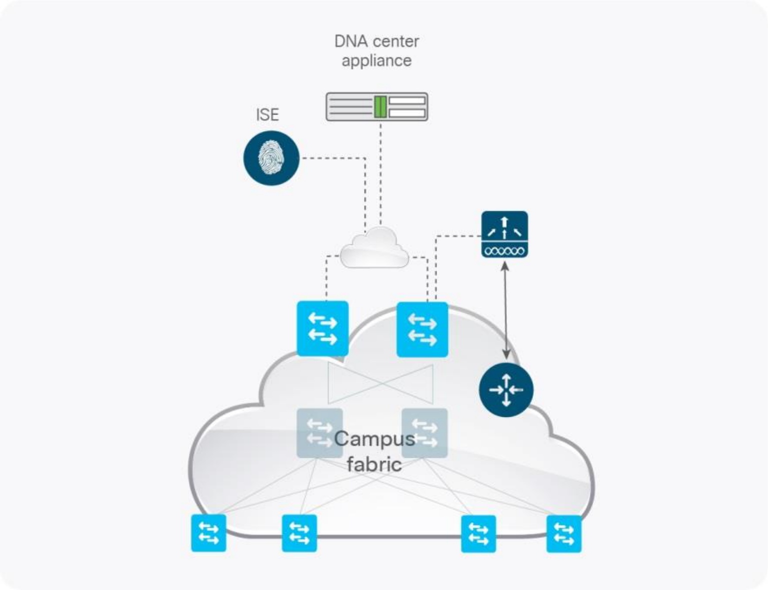
NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED 'AS IS' WITH ALL FAULTS. CISCO AND THIRD-PARTY SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Introduction

The Cisco® Software-Defined Access (SD-Access) solution uses Cisco DNA Center™ to provide intent-based policy automation and assurance for your campus fabric. The SD-Access solution consists of the enterprise DNA Center controller, Cisco Identity Services Engine (ISE), fabric control plane, fabric border, intermediate nodes, fabric wireless LAN controller, and fabric edge nodes (Figure 1).

Figure 1. SD-Access campus fabric



Cisco DNA Center controller

The enterprise software-defined networking (SDN) controller, which runs on the Application Policy Infrastructure Controller Enterprise Module (APIC-EM), provides GUI management and abstraction. Cisco DNA Center is largely responsible for the design, policy, provisioning, and assurance workflows.

Identity Services Engine

Cisco ISE integrates with the SD-Access controller using Cisco Platform Exchange Grid (pxGrid) to exchange client information and automation of fabric-related configurations on ISE.

Control plane node

The SD-Access fabric control plane node is a map system that manages endpoint ID-to-device relationships.

Edge nodes

The SD-Access fabric edge nodes are equivalent to the access layer switch in a traditional campus design. Wired endpoints and fabric access points connect to the SD-Access fabric using fabric edge nodes.

Border node

An SD-Access fabric border node connects external Layer 3 networks to the SD-Access fabric. These nodes serve as the gateway for known networks within the company or as a default exit point from the fabric to the Internet or outside world.

Fabric Wireless LAN controller (WLC)

The SD-Access fabric WLC connects wireless endpoints to the SD-Access fabric.

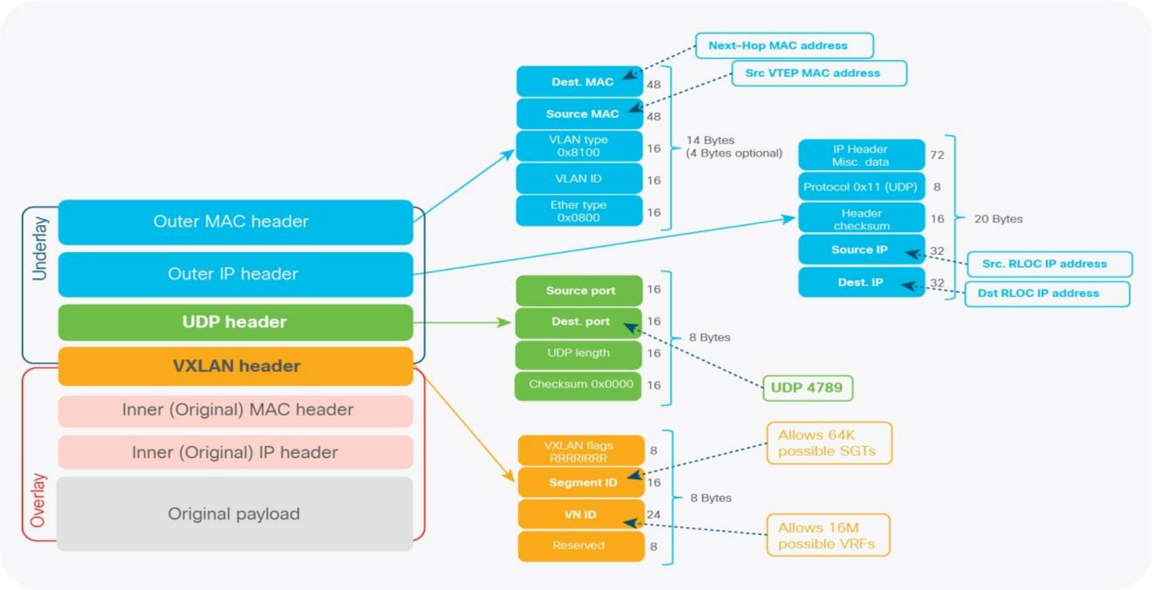
Intermediate nodes

The SD-Access fabric intermediate nodes are part of the Layer 3 network that interconnects the edge nodes to the border nodes. They operate in the underlay and are responsible only for routing the IP traffic inside the fabric.

This white paper describes the Cisco SD-Access solution integration with Network as a Sensor (NaaS) and Encrypted Traffic Analytics (ETA) at a medium technical level. For more details on the SD-Access 1.0 solution, please refer to the SD-Access 1.0 white paper.

The SD-Access architecture enables the use of overlay networks running on a physical underlay network to create dynamic logical topologies to connect devices. The underlay network in an SD-Access network consists of physical switches and routers that enable IP connectivity within the fabric using a dynamic routing protocol. The overlay network, on the other hand, runs over the underlay network by encapsulating user traffic over IP tunnels using Virtual Extensible LAN (VXLAN). Using VXLAN, the original Layer 2 frame is tunneled on a User Datagram Protocol (UDP) packet across the Layer 3 underlay network. Each overlay network, called a VXLAN segment, is identified using a 24-bit VXLAN Network Identifier (VNI) (Figure 2).

Figure 2. VXLAN header



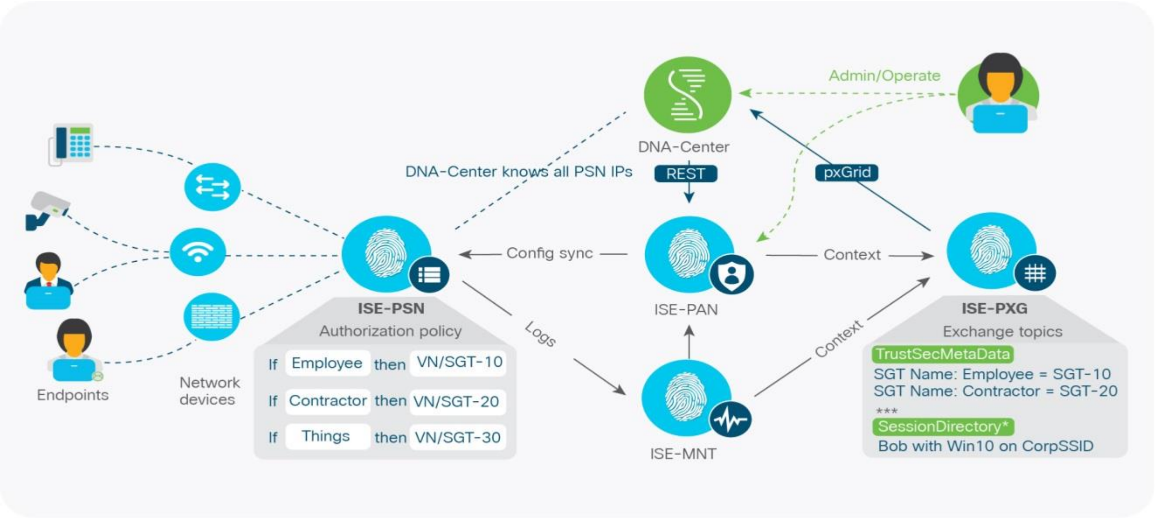
SD-Access fabric replaces 16 of the reserved bits in the VXLAN header in order to transport up to 64,000 security group tags (SGTs). These SGTs carry users' group membership information and enable micro-level segmentation inside the virtualized network. The VXLAN overlay simplifies SGT propagation in the SD-Access fabric without having to configure a hop-by-hop cts-manual/cts-dot1x command to enable inline SGT propagation.

SD-Access also introduces the concept of subnet stretching; that is, a single subnet can be extended across all SD-Access fabric edge nodes. This enables seamless client roaming as the client IP address, default-gateway, remains unchanged even as the client moves across the stretch subnet.

Cisco DNA Center and ISE integration

Cisco ISE is an integral part of SD-Access for policy implementation, enabling dynamic mapping of users and devices to scalable groups and simplifying end-to-end security policy enforcement. ISE integrates with the SD-Access controller by using Cisco pxGrid and RESTful APIs for exchange of client information and automation of fabric-related configurations on ISE (Figure 3).

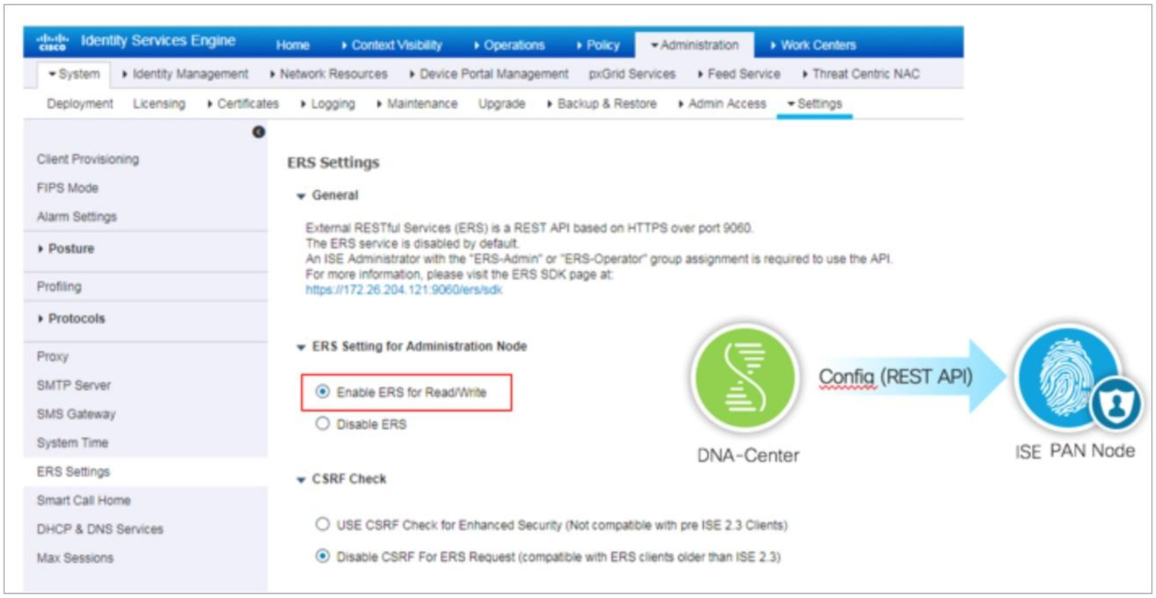
Figure 3. ISE in SD-Access fabric



The following are the steps to integrate ISE into Cisco DNA Center.

Enable ERS setting on the ISE administration node for REST services (Figure 4).

Figure 4. Enabling ERS on ISE



ERS Settings

General

External RESTful Services (ERS) is a REST API based on HTTPS over port 9060.
The ERS service is disabled by default.
An ISE Administrator with the "ERS-Admin" or "ERS-Operator" group assignment is required to use the API.
For more information, please visit the ERS SDK page at:
https://172.26.204.121:9060/ers/sdk

ERS Setting for Administration Node

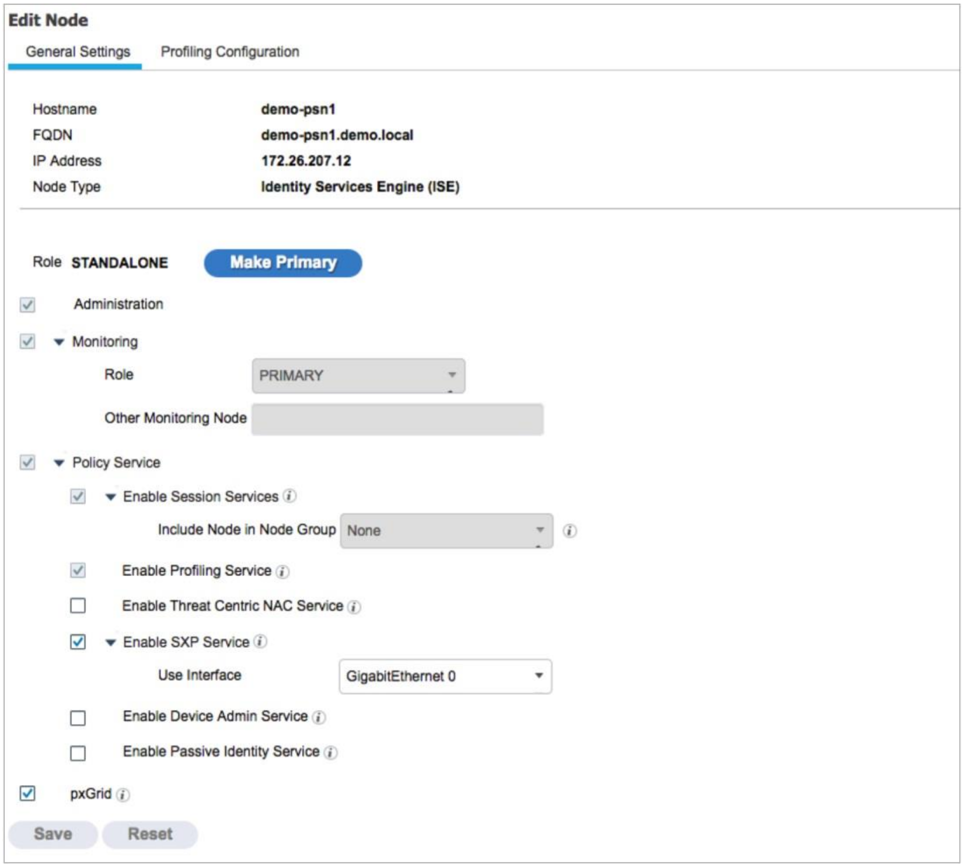
● Enable ERS for Read/Write
○ Disable ERS

CSRF Check

○ USE CSRF Check for Enhanced Security (Not compatible with pre ISE 2.3 Clients)
● Disable CSRF For ERS Request (compatible with ERS clients older than ISE 2.3)

Enable pxGrid services (Figure 5).

Figure 5. Enabling ISE pxGrid



Hostname	demo-psn1
FQDN	demo-psn1.demo.local
IP Address	172.26.207.12
Node Type	Identity Services Engine (ISE)

Role STANDALONE

☑ Administration

☑ Monitoring

Role PRIMARY

Other Monitoring Node

☑ Policy Service

☑ Enable Session Services

Include Node in Node Group None

☑ Enable Profiling Service

□ Enable Threat Centric NAC Service

☑ Enable SXP Service

Use Interface GigabitEthernet 0

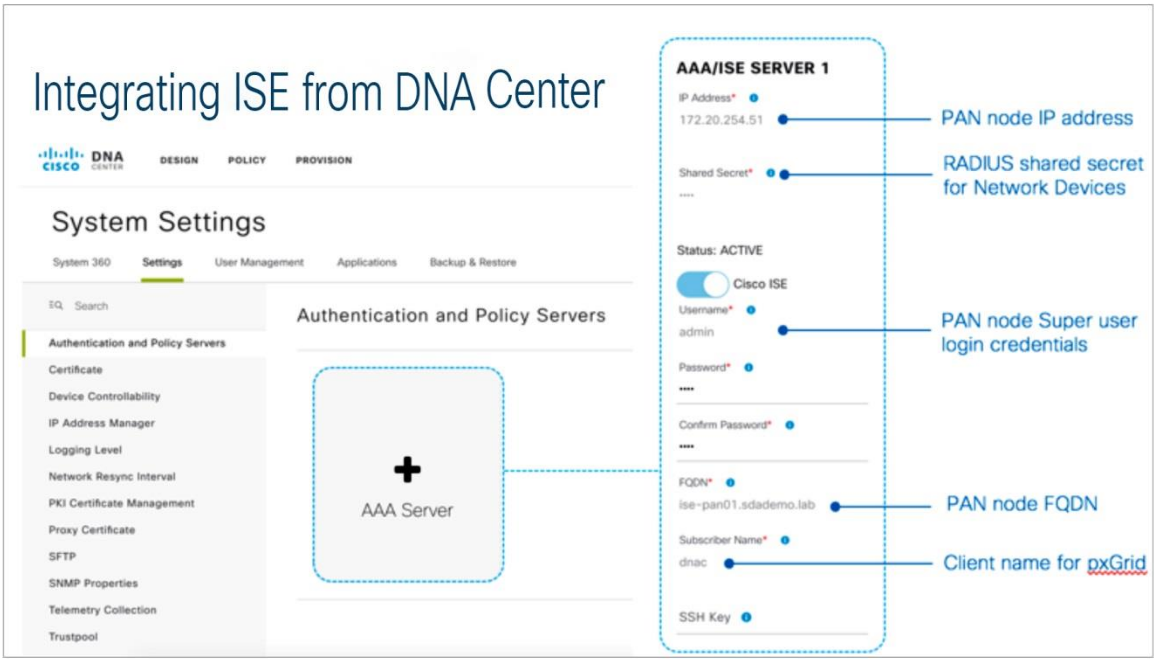
□ Enable Device Admin Service

□ Enable Passive Identity Service

☑ pxGrid

Define the Authentication, Authorization, and Accounting (AAA) server on Cisco DNA Center (Figure 6).

Figure 6. Configuring Cisco DNA Center AAA



Integrating ISE from DNA Center

System Settings

Authentication and Policy Servers

AAA/ISE SERVER 1

IP Address*: 172.20.254.51 — PAN node IP address

Shared Secret*: •••• — RADIUS shared secret for Network Devices

Status: ACTIVE

Cisco ISE

Username*: admin — PAN node Super user login credentials

Password*: ••••

Confirm Password*: ••••

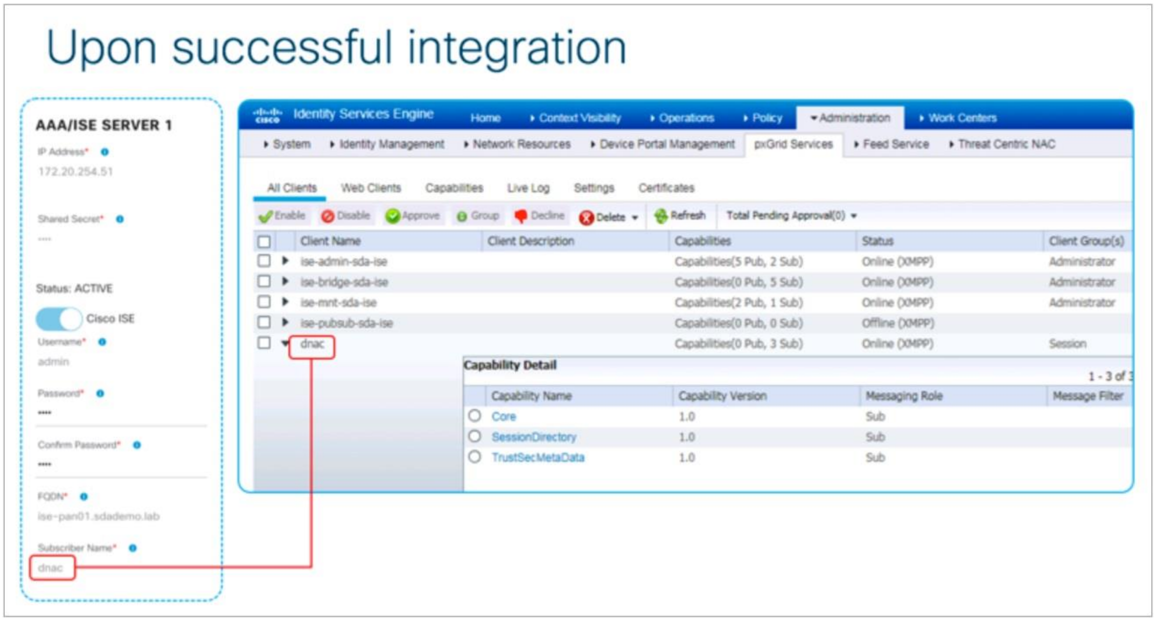
FQDN*: ise-pan01.sdademo.lab — PAN node FQDN

Subscriber Name*: dnac — Client name for pxGrid

SSH Key

Verify the successful Cisco DNA Center and ISE integration (Figure 7).

Figure 7. Successful Cisco DNA Center and ISE integration



Upon successful integration

AAA/ISE SERVER 1

IP Address*: 172.20.254.51

Shared Secret*: ····

Status: ACTIVE

Cisco ISE

Username*: admin

Password*: ••••

Confirm Password*: ••••

FQDN*: ise-pan01.sdademo.lab

Subscriber Name*: dnac

□	Client Name	Client Description	Capabilities	Status	Client Group(s)
□	ise-admin-sda-ise		Capabilities(5 Pub, 2 Sub)	Online (XMPP)	Administrator
□	ise-bridge-sda-ise		Capabilities(0 Pub, 5 Sub)	Online (XMPP)	Administrator
□	ise-mnt-sda-ise		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Administrator
□	ise-pubsub-sda-ise		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)	
□	dnac		Capabilities(0 Pub, 3 Sub)	Online (XMPP)	Session

Capability Detail

1 - 3 of 3

	Capability Name	Capability Version	Messaging Role	Message Filter
○	Core	1.0	Sub	
○	SessionDirectory	1.0	Sub	
○	TrustSecMetaData	1.0	Sub	

Network as a Sensor and Enforcer (NaaS)

A network's attack surface is continually growing. Today's technology trends, such as mobility, cloud, and the Internet of Things (IOT), are multiplying the points of infiltration into your network, and attackers are getting more sophisticated. Often attackers are part of international cybercrime organizations or organizations such as WikiLeaks, and individuals from both inside and outside of the trusted network may have various motivations for disclosing vital proprietary or personal information. The attackers may understand your network and defenses better than you do. Many times, they will use legitimate user credentials to accomplish their objectives. As a result, discovery and network remediation of the breaches are complex, time-consuming, and extremely costly.

When addressing such a complex security problem, depending on a single hardware or software component is not the right approach. Rather than taking a Swiss army knife approach (using a single tool for multiple purposes), you need to take a toolbox approach, using function-specific tools.

The Cisco NaaS solution is a toolbox consisting of NetFlow, ISE, and Cisco Stealthwatch™. These tools are tightly integrated to help you leverage the entire network to:

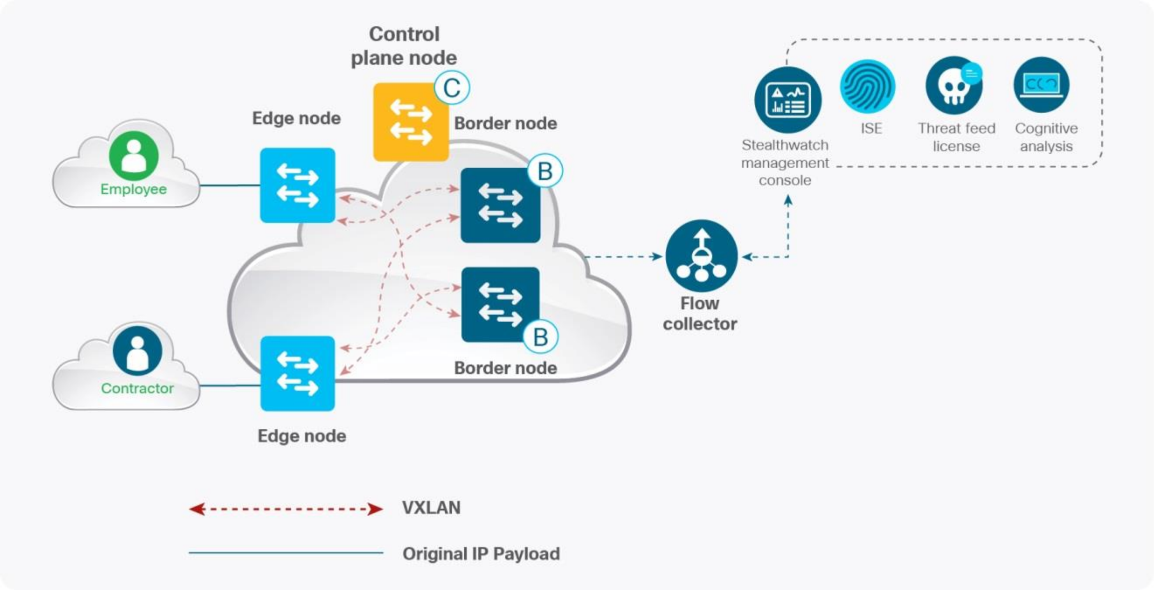
- Detect anomalous traffic flows such as malware
- Identify user access policy violations
- Obtain deep and broad visibility into all network traffic

The NaaS solution has two main components: devices configured as NetFlow agents and the Cisco Stealthwatch system.

NetFlow agents can be configured on any NetFlow-capable devices in your network. For the purpose of security analytics, network forensics, and attack detection, NetFlow should be enabled in the access layer switches in order to get complete visibility into the traffic flow.

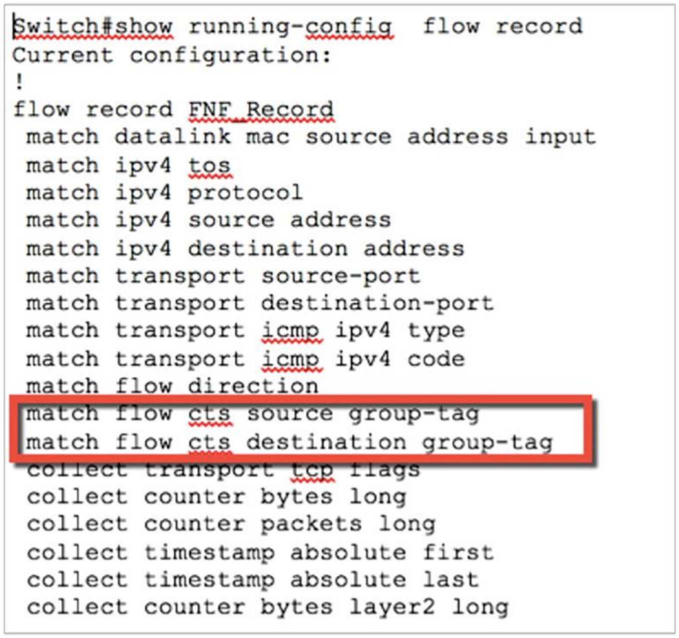
There are additional considerations when deploying NaaS in an SD-Access fabric. To get complete visibility into the traffic flow, and for security auditing, you will need to export the actual IP payload and not the VXLAN header; hence we recommend configuring a NetFlow agent and flow export on the ingress interface on a fabric edge device and/or the egress interface on a fabric border. This will enable Stealthwatch to correlate both unidirectional flow records and stitch them as a bidirectional conversation flow record, to allow easy visualization and analysis (Figure 8).

Figure 8. NetFlow export in SD-Access fabric



Since client authentication, dynamic endpoint classification, and SGT group assignment are part of Cisco DNA Center host onboarding and provisioning flow, a security administrator could include SGTs while exporting NetFlow records from SD-Access fabric edge nodes (Figure 9).

Figure 9. NetFlow record configuration in SD-Access fabric

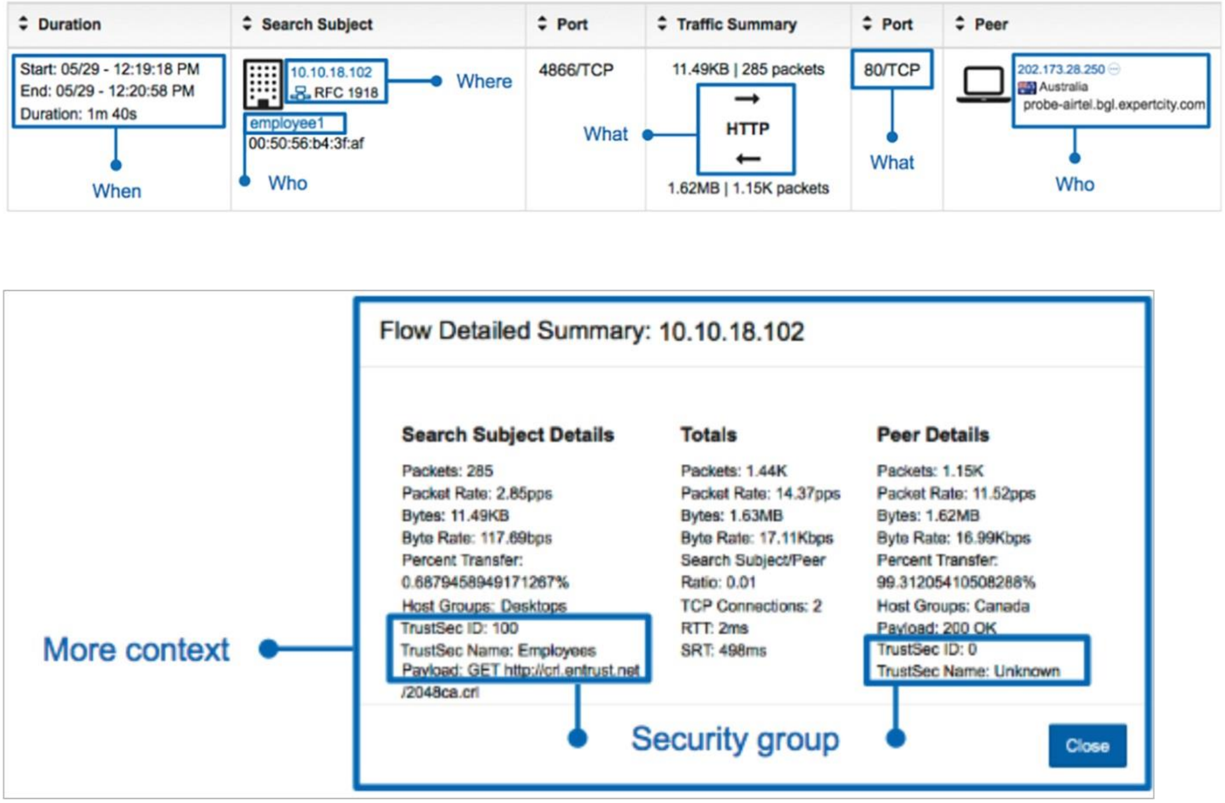


```
Switch#show running-config  flow record
Current configuration:
!
flow record FNF_Record
 match datalink mac source address input
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match transport icmp ipv4 type
 match transport icmp ipv4 code
 match flow direction
 match flow cts source group-tag
 match flow cts destination group-tag
 collect transport tcp flags
 collect counter bytes long
 collect counter packets long
 collect timestamp absolute first
 collect timestamp absolute last
 collect counter bytes layer2 long
```

Note that the flow record in Figure 9 contains two fields involving security groups. These commands ensure that all the security group classifications known to the SD-Access fabric nodes are exported in the flow record.

Additionally, Cisco Stealthwatch can be integrated with ISE using PxGrid. This enables Stealthwatch to get additional contextual identity data on a user, device type, and posture information (Figure 10).

Figure 10. Stealthwatch conversational record



⇕ Duration	⇕ Search Subject	⇕ Port	⇕ Traffic Summary	⇕ Port	⇕ Peer
Start: 05/29 - 12:19:18 PM End: 05/29 - 12:20:58 PM Duration: 1m 40s	10.10.18.102 RFC 1918 employee1 00:50:56:b4:3f:af	4866/TCP	11.49KB | 285 packets → HTTP ← 1.62MB | 1.15K packets	80/TCP	202.173.28.250 Australia probe-airtel.bgl.expertcity.com

Flow Detailed Summary: 10.10.18.102

Search Subject Details

Packets: 285
Packet Rate: 2.85pps
Bytes: 11.49KB
Byte Rate: 117.69bps
Percent Transfer:
0.6879458949171267%
Host Groups: Desktops
TrustSec ID: 100
TrustSec Name: Employees
Payload: GET http://crl.entrust.net
/2048ca.crl

Totals

Packets: 1.44K
Packet Rate: 14.37pps
Bytes: 1.63MB
Byte Rate: 17.11Kbps
Search Subject/Peer
Ratio: 0.01
TCP Connections: 2
RTT: 2ms
SRT: 498ms

Peer Details

Packets: 1.15K
Packet Rate: 11.52pps
Bytes: 1.62MB
Byte Rate: 16.99Kbps
Percent Transfer:
99.31205410508288%
Host Groups: Canada
Payload: 200 OK
TrustSec ID: 0
TrustSec Name: Unknown

With PxGrid integration, ISE acts as the telemetry source, providing details on device profiling, device, and user authentication. Stealthwatch can then use this data to correlate NetFlow to a username, which aids in building user-centric reports.

For details on Flexible NetFlow and Stealthwatch components, please refer to the Network as a Security Sensor white paper.

Encrypted Traffic Analytics

The rapid rise in encrypted traffic is changing the threat landscape. As more businesses become digital, a significant number of services and applications are using encryption as the primary method of securing information. The majority of organizations today do not have a way to detect malicious content in encrypted traffic. Barring legal issues with respect to decrypting encrypted traffic in a campus, the solution always comes with a cost in terms of SSL offload, bulk decryption, analysis, and reencryption. Due to the complexity and scaling concerns with this model, deep packet inspection is no longer a viable solution, and most organizations tend to stay away from this model.

Encrypted Traffic Analytics (ETA) focuses on identifying malware communications in encrypted traffic through passive monitoring, extraction of relevant data elements, and supervised machine learning with cloud-based global visibility.

From a Transport Layer Security (TLS) packet, ETA extracts the initial data packet (IDP), Sequence of Packet Lengths and Times (SPLT), and threat intelligence map. The IDP is the initial communication between two endpoints initiating a TLS handshake, which is unencrypted. ETA uses the IDP to collect the TLS version used, server data, cipher suites, and the certificate used to establish trust. The SPLT telemetry is composed of the first 10 packets in a flow, which has an application payload. Data collected from the IDP and SPLT is exported to the Stealthwatch Flow Collector. For any encrypted traffic egressing from the SD-Access fabric to the external world, including the Internet, Stealthwatch queries Cognitive Threat Analytics (CTA) to identify any malware presence. CTA is a cloud-based product that uses machine learning to identify anomalies in your network.

Northbound traffic egressing from an SD-Access fabric border toward external networks such as the Internet is subjected to CTA analysis. Since SD-Access uses VXLAN encapsulation for the data path, we recommended that you configure ETA on the SD-Access fabric edge ingress interface, where endpoints are connected, and Flexible NetFlow on the SD-Access fabric border egress interface as the traffic exits the fabric. ETA on an SD-Access fabric comprising Cisco Stealthwatch and CTA cloud is currently supported on the Cisco Catalyst® 9300 and 9400 Series Switches and the Cisco ASR 1000 Series Aggregation Services Routers and 4000 Series Integrated Services Routers.

The following are examples of ETA configurations on SD-Access fabric edge nodes.

ETA globally on the switch

```
Switch(config)#et-analytics
Switch(config-et-analytics)#ip flow-export destination 172.26.207.58 2055
Switch(config-et-analytics)#inactive-timeout 15
```

ETA interface configuration on an SD-Access fabric edge node

```
Switch(config)#interface GigabitEthernet 1/0/1
Switch(config)#et-analytics enable

Switch# show platform software et-analytics global
ET-Analytics Global state
=========================
 All Interfaces   : Off
 IP Flow-record Destination: 172.26.207.58 2055
 Inactive timer: 15

ET-Analytics interfaces
 GigabitEthernet1/0/1

ET-Analytics VLANs
```

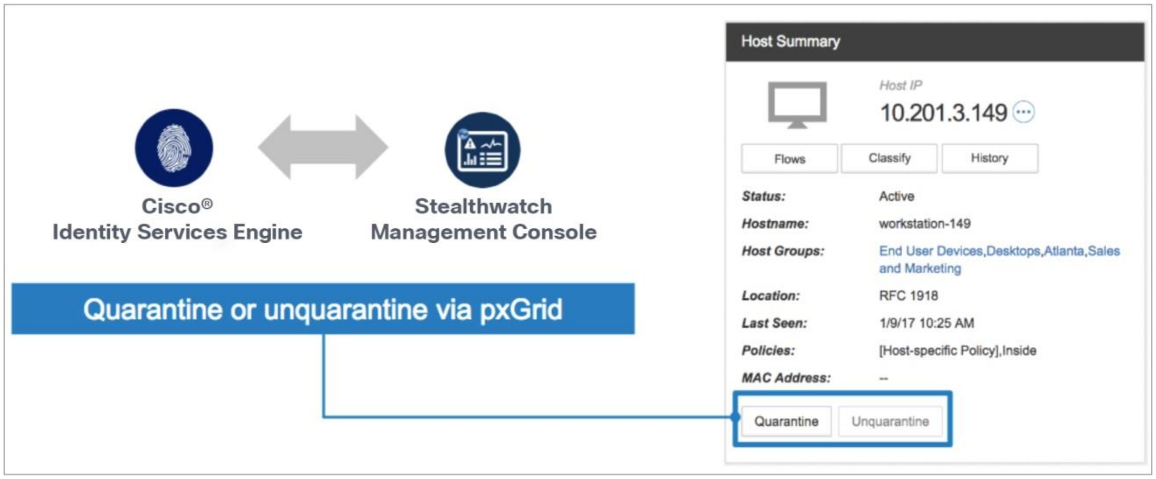
Since ETA analyzes the initial TLS handshake, we can audit the TLS libraries and cipher suites used to encrypt the traffic. Security administrators can use these audit statistics to identify how many endpoints are compliant with their cryptographic cipher standards.

Rapid threat containment

Cisco pxGrid is a unified framework that enables ecosystem partners to obtain user and device contextual information from Cisco ISE. ISE publishes topics of information, and ecosystem partners can subscribe to these published topics, obtaining ISE session information and taking Adaptive Network Control (ANC) mitigation actions on endpoints.

Cisco Stealthwatch registers to the ISE pxGrid node as a client, subscribes to the EndpointProtectionService capability, and performs ANC mitigation actions on the endpoint. These mitigation actions include quarantining and unquarantining of an IEEE 802.1X endpoint authenticated by ISE (Figure 11).

Figure 11. Rapid threat containment



Host IP
10.201.3.149

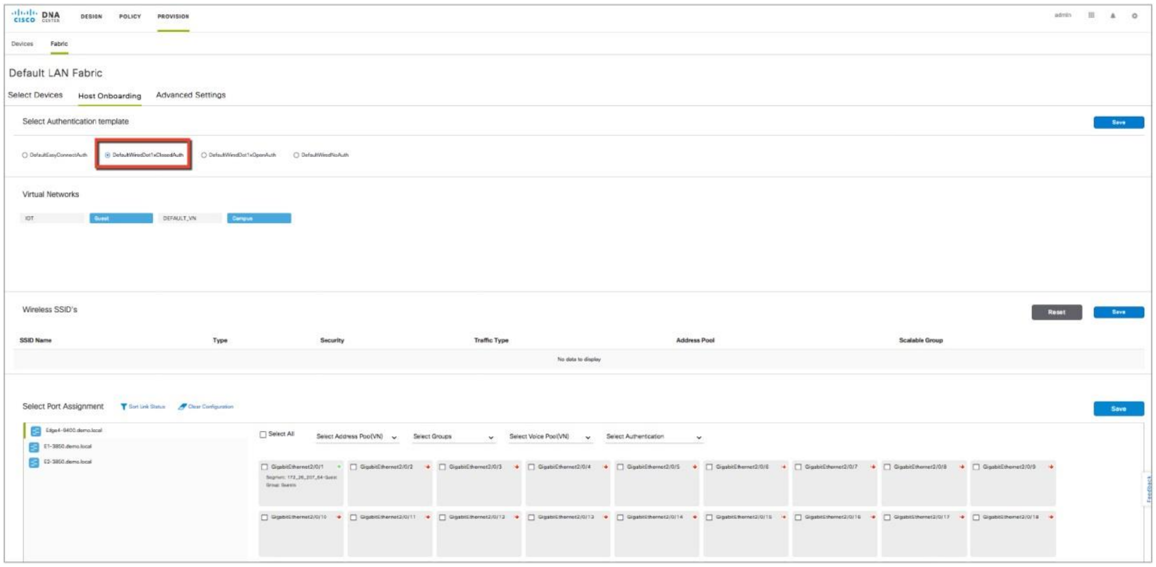
Status: Active
Hostname: workstation-149
Host Groups: End User Devices,Desktops,Atlanta,Sales and Marketing
Location: RFC 1918
Last Seen: 1/9/17 10:25 AM
Policies: [Host-specific Policy],Inside
MAC Address: --

Policy enforcement

Most of the traditional NaaS deployments use a quarantine VLAN to isolate an endpoint that has been marked suspicious. Once ISE receives a quarantine notification from Cisco Stealthwatch, it issues a Change of Authorization (CoA) to dynamically change the endpoint to the quarantine VLAN. Assigning a dynamic VLAN from ISE results in undesired behavior, as not all the endpoints are intelligent enough to detect a network change and will retain the previous IP address. This affects the ability for a security administrator to perform forensic analysis on the endpoint.

With SD-Access, ISE and Cisco TrustSec® policy enforcement is integrated as part of the overall solution. Cisco DNA Center provisioning workflows allow you to specify an authentication template during host onboarding (Figure 12).

Figure 12. Cisco DNA Center authentication template



Once provisioned, all the required AAA and RADIUS commands are configured on the fabric edge nodes:

```
Switch#show running-config aaa
aaa new-model
aaa session-id common
aaa authentication login default group dnac-group local
aaa authentication enable default enable
aaa authentication dot1x default group dnac-group
aaa authorization exec default group dnac-group local
aaa authorization network default group dnac-group
aaa authorization network dnac-cts-list group dnac-group
aaa accounting dot1x default start-stop group dnac-group
!
aaa server radius dynamic-author
 client <RADIUS-SERVER> server-key <KEY>
!
radius server dnac-radius_<RADIUS-SERVER>
 address ipv4 <RADIUS-SERVER> auth-port 1812 acct-port 1813
 pac key <KEY>
!
cts authorization list dnac-cts-list
cts role-based enforcement
cts role-based enforcement vlan-list 1021-1022

radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
```

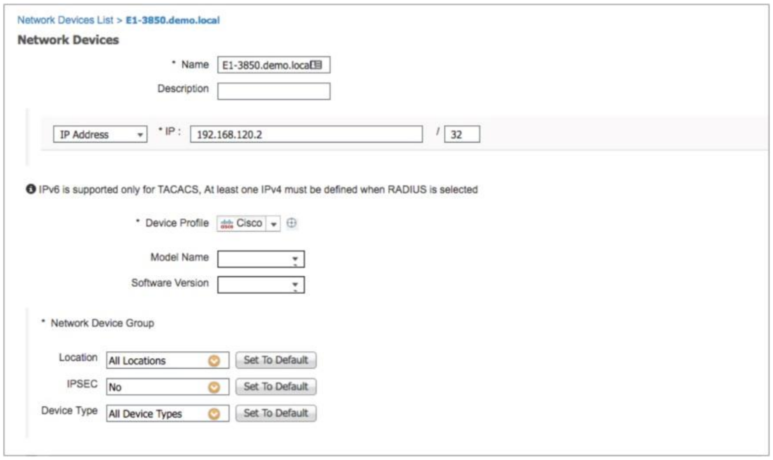
```
radius-server dead-criteria time 2 tries 1

aaa group server radius dnac-group
 server name dnac-radius_<RADIUS-SERVER>
 ip radius source-interface Loopback0
```

Default 802.1X Closed Mode template – **DefaultWiredDot1xClosedAuth** in Cisco DNA Center – provisions the configurations below that are applied on the edge interfaces.

```
interface GigabitEthernet1/0/1
 switchport mode access
 switchport voice vlan 4000
 authentication control-direction in
 authentication event server dead action authorize vlan 3999
 authentication event server dead action authorize voice
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server
 authentication timer inactivity server dynamic
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
 spanning-tree portfast
end
```

Note that all the relevant Cisco TrustSec configurations are also enabled as part of the provisioning workflow, including Security Group Access Control List (SGACL) enforcement. Cisco DNA Center also automates the Network Access Device (NAD) configuration in ISE for RADIUS, Simple Network Management Protocol (SNMP), and advanced Cisco TrustSec settings (Figure 13).

Figure 13. ISE network devices list



Network Devices List > **E1-3850.demo.local**

Network Devices

* Name: E1-3850.demo.local

Description:

IP Address * IP : 192.168.120.2 / 32

IPv6 is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected

* Device Profile: Cisco

Model Name:

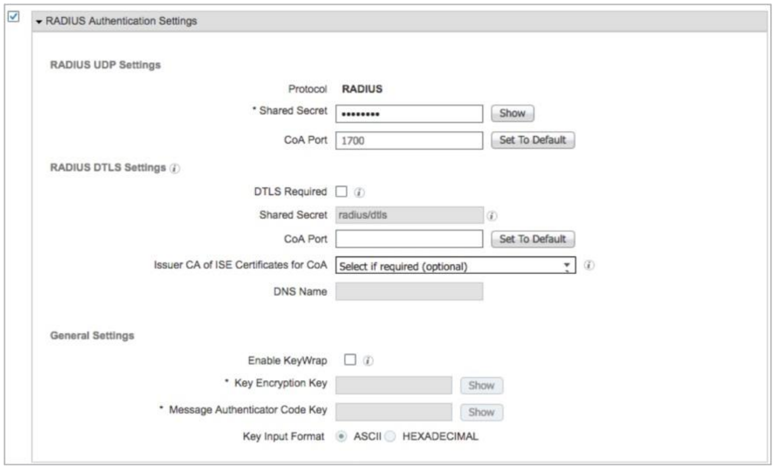
Software Version:

* Network Device Group

Location: All Locations

IPSEC: No

Device Type: All Device Types



☑ ▾ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

* Shared Secret •••••••• Show

CoA Port 1700 Set To Default

RADIUS DTLS Settings ⓘ

DTLS Required □ ⓘ

Shared Secret radius/dtls ⓘ

CoA Port Set To Default

Issuer CA of ISE Certificates for CoA Select if required (optional) ⓘ

DNS Name

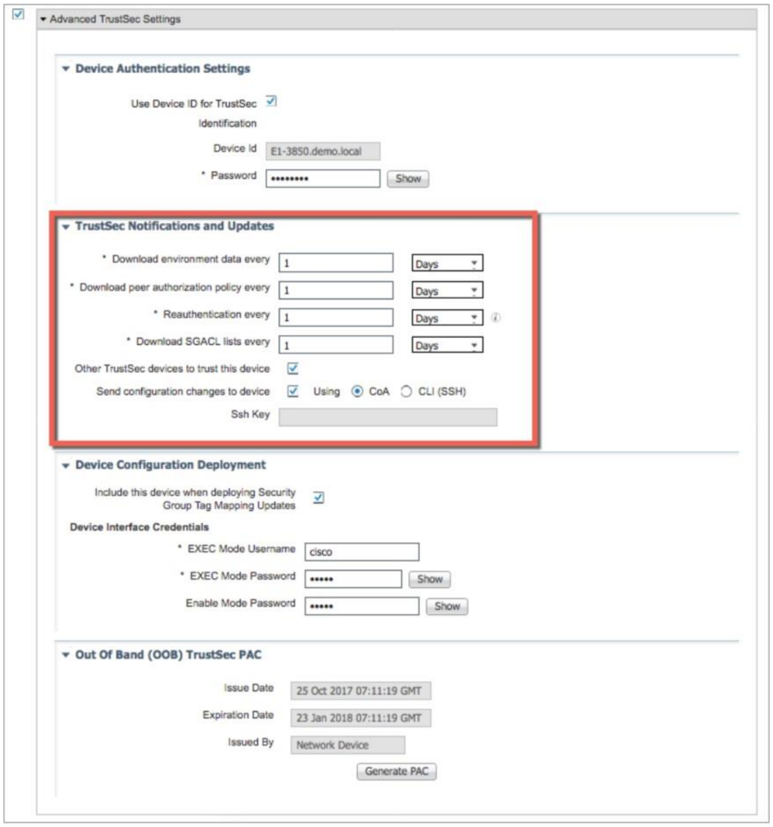
General Settings

Enable KeyWrap □ ⓘ

* Key Encryption Key Show

* Message Authenticator Code Key Show

Key Input Format ● ASCII ○ HEXADECIMAL



☑ ▾ Advanced TrustSec Settings

▾ Device Authentication Settings

Use Device ID for TrustSec Identification ☑

Device Id E1-3850.demo.local

* Password •••••••• Show

▾ TrustSec Notifications and Updates

* Download environment data every 1 Days

* Download peer authorization policy every 1 Days

* Reauthentication every 1 Days ⓘ

* Download SGACL lists every 1 Days

Other TrustSec devices to trust this device ☑

Send configuration changes to device ☑ Using ● CoA ○ CLI (SSH)

Ssh Key

▾ Device Configuration Deployment

Include this device when deploying Security Group Tag Mapping Updates ☑

Device Interface Credentials

* EXEC Mode Username cisco

* EXEC Mode Password ••••• Show

Enable Mode Password ••••• Show

▾ Out Of Band (OOB) TrustSec PAC

Issue Date 25 Oct 2017 07:11:19 GMT

Expiration Date 23 Jan 2018 07:11:19 GMT

Issued By Network Device

Generate PAC

Once the Cisco DNA Center host provisioning flow is complete, SD-Access fabric edge nodes should have a valid Cisco TrustSec Protected Access Credential (PAC) and environment variables. They will then be ready for client authentication.

```
Switch#show aaa server

RADIUS: id 1, priority 1, host 172.26.207.136, auth-port 1812, acct-port 1813
     State: current UP, duration 1010s, previous duration 0s
     Dead: total time 13s, count 28687
     Platform State from SMD: current UNKNOWN, duration 1729691s, previous
duration 0s
     SMD Platform Dead: total time 0s, count 49
     Platform State from WNCD: current UP, duration 0s, previous duration 0s
     Platform Dead: total time 0s, count 0
     Quarantined: No
     Authen: request 129937, timeouts 28680, failover 0, retransmission 21510
             Response: accept 17, reject 101210, challenge 30
             Response: unexpected 0, server error 0, incorrect 0, time 9ms
             Transaction: success 101257, failure 7170
             Throttled: transaction 0, timeout 0, failure 0
     Author: request 217, timeouts 0, failover 0, retransmission 0
             Response: accept 217, reject 0, challenge 0
             Response: unexpected 0, server error 0, incorrect 0, time 13ms
             Transaction: success 217, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Account: request 60, timeouts 5, failover 0, retransmission 5
             Request: start 17, interim 0, stop 16
             Response: start 17, interim 0, stop 16
             Response: unexpected 0, server error 0, incorrect 0, time 6ms
             Transaction: success 55, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Elapsed time since counters last cleared: 4w5d2h58m
     Estimated Outstanding Access Transactions: 0
     Estimated Outstanding Accounting Transactions: 0
     Estimated Throttled Access Transactions: 0
     Estimated Throttled Accounting Transactions: 0
     Maximum Throttled Transactions: access 0, accounting 0
     Requests per minute past 24 hours:
             high - 2 hours, 5 minutes ago: 10
             low  - 2 hours, 56 minutes ago: 0
             average: 0
```

SD-Access edge nodes have a valid Cisco TrustSec PAC:

```
Switch#show cts pac
AID: F5295B216E583339A706B9DC98FBDE42
PAC-Info:
  PAC-type = Cisco Trustsec
  AID: F5295B216E583339A706B9DC98FBDE42
  I-ID: E2-3850.demo.local
  A-ID-Info: Identity Services Engine
  Credential Lifetime: 23:11:55 PST Mon Jan 22 2018
PAC-Opaque:
000200C0000300010004001 0F5295B216E583339A706B9DC98FBDE42000600A400030100136DBE8F3
F1820FDE887D1590DA0BD380000001359EE482C00093A800C5BC14AEEEBC3EF53A6EF833DCD286199
1DCB5176BB0783293988EB3751E4C9DAF68115CD1030BF91E551ABE8C6CA4CE99AA55D6CE196F05C9
```

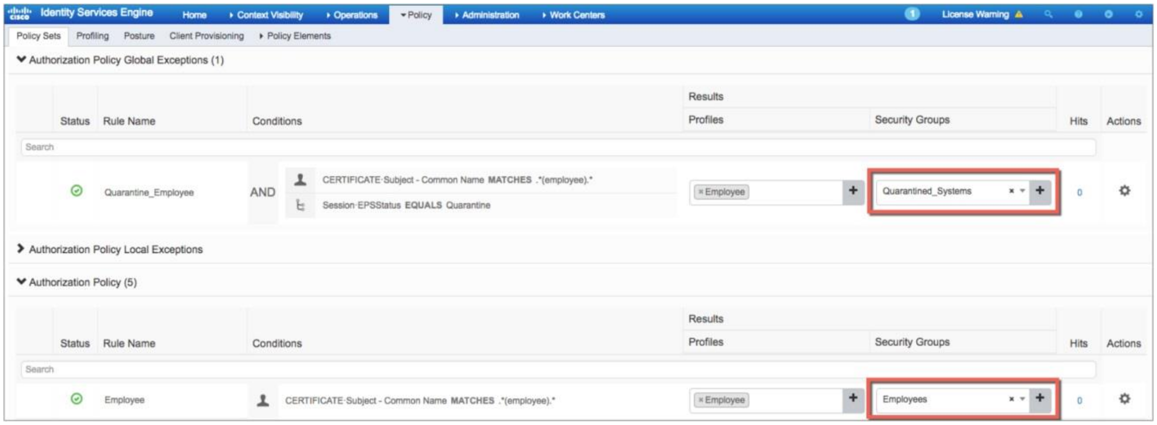
```
E3D6DF821A7B85DBEA574640A196ABBB726A2F575173AB0CB9210619C95D0D7FD2C29F872DB4C7829
943B417177BA8270D75246AD09069C7A9FAF7CDE230C3663953239F1C26BC2A96E70
Refresh timer is set for 7w6d
```

With a valid Cisco TrustSec PAC, the SD-Access edge nodes should download all the Cisco TrustSec environment data from Cisco ISE:

```
Switch#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 0-00:Unknown
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
  Server: 172.26.207.11, port 1812, A-ID F5295B216E583339A706B9DC98FBDE42
          Status = ALIVE
          auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins,
deadtime = 20 secs
Multicast Group SGT Table:
Security Group Name Table:
    0-e1:Unknown
    2-e1:TrustSec_Devices
    3-e1:Network_Services
    4-e1:Employees
    5-e1:Contractors
    6-e1:Guests
    7-e1:Production_Users
    8-e1:Developers
    9-e1:Auditors
    10-e1:Point_of_Sale_Systems
    11-e1:Production_Servers
    12-e1:Development_Servers
    13-e1:Test_Servers
    14-e1:PCI_Servers
    15-e1:BYOD
    16-e1:Contractor_Server
    255-e1:Quarantined_Systems
Environment Data Lifetime = 86400 secs
Last update time = 08:54:41 PST Sun Nov 26 2017
Env-data expires in   0:06:59:30 (dd:hr:mm:sec)
Env-data refreshes in 0:06:59:30 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running
```

In the following example, a corporate owned and managed employee workstation is successfully authenticated and authorized on vlan1021 and assigned employee SGT of 4 (Figures 13 and 14).

Figure 14. ISE employee authorization policy



Authorization Policy Global Exceptions (1)

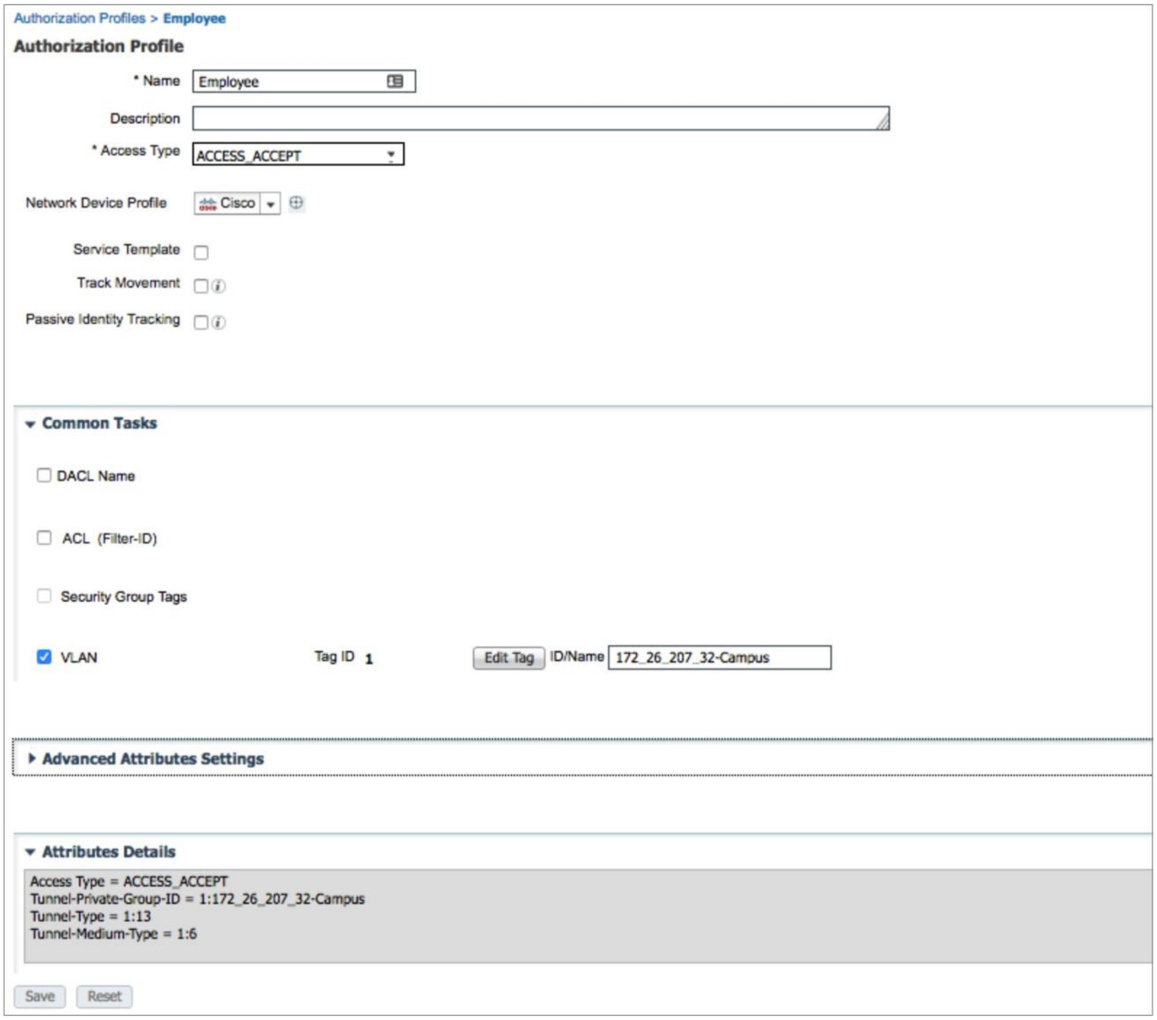
Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
✓	Quarantine_Employee	AND CERTIFICATE·Subject - Common Name **MATCHES** .*(employee).* Session·EPSStatus **EQUALS** Quarantine	Employee	Quarantined_Systems	0	⚙

Authorization Policy Local Exceptions

Authorization Policy (5)

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
✓	Employee	CERTIFICATE·Subject - Common Name **MATCHES** .*(employee).*	Employee	Employees	0	⚙

Figure 15. ISE employee authorization profile



Authorization Profiles > **Employee**

Authorization Profile

* Name	Employee
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	Cisco
Service Template	□
Track Movement	□
Passive Identity Tracking	□

Common Tasks

□ DACL Name

□ ACL (Filter-ID)

□ Security Group Tags

☑ VLAN Tag ID 1 Edit Tag ID/Name 172_26_207_32-Campus

Advanced Attributes Settings

Attributes Details

```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:172_26_207_32-Campus
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6
```

You will notice that the ISE authorization profile uses a specific format for VLAN assignment. The format is **<IP_Host_Pool>-<Virtual Network>**, where the subnet octets are separated by underscores instead of decimals. In the above example, 172_26_207_32 is the subnet, and Campus is the name of the virtual network.

```
Switch#show authentication session interface g1/0/9 detail
          Interface:  GigabitEthernet1/0/9
               IIF-ID:  0x16DA758C
          MAC Address:  000c.2979.6fa2
         IPv6 Address:  fe80::fccd:6814:6fae:5530
         IPv4 Address:  172.26.207.35
            User-Name:  employee1.demo.local
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  in
      Session timeout:  N/A
    Common Session ID:  C0A8020200005F2E95CBDD84
      Acct Session ID:  0x00000015
               Handle:  0x4f000026
       Current Policy:  POLICY_Gi1/0/9
Local Policies:
         Idle timeout:  65536 sec
Server Policies:
           Vlan Group:  Vlan: 1021
      Security Policy:  None
      Security Status:  Link Unsecured
            SGT Value:  4

Method status list:
       Method           State
        dot1x           Authc Success
```

Based on the NetFlow record definition in **Figure 9**, the SGT information is also exported as part of the flow record for additional visibility. With SGACL enforcement in play, all employee assets having an SGT value of 4 have relevant network access to internal servers and the Internet.

```
Switch#show cts role-based permissions from 4
IPv4 Role-based permissions from group 4:Employees to group 4:Employees:
        Permit IP-00
IPv4 Role-based permissions from group 4:Employees to group 5:Contractors:
        Permit IP-00
IPv4 Role-based permissions from group 4:Employees to group 
12:Development_Servers:
        Permit IP-00
```

With Stealthwatch ISE integration via pxGrid, a security administrator can effectively quarantine an endpoint if any suspicious network traffic is observed. ISE, upon receiving this notification from Stealthwatch, can issue a CoA to restrict network access for this endpoint until further forensic analysis is completed.

```
Switch# show authentication session interface g1/0/9 detail
            Interface:  GigabitEthernet1/0/9
               IIF-ID:  0x1A8E970A
          MAC Address:  000c.2979.6fa2
         IPv6 Address:  fe80::fccd:6814:6fae:5530
         IPv4 Address:  172.26.207.35
            User-Name:  employee1.demo.local
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  in
      Session timeout:  N/A
    Common Session ID:  C0A8020200018C48FD3142EE
      Acct Session ID:  0x00000017
               Handle:  0x2100002b
       Current Policy:  POLICY_Gi1/0/9
Local Policies:
         Idle timeout:  65536 sec

   Server Policies:
           Vlan Group:  Vlan: 1021
      Security Policy:  None
      Security Status:  Link Unsecured
           SGT Value:  255

Method status list:
       Method           State
        dot1x           Authc Success
```

Notice above that rapid threat containment is seamless in SD-Access fabric, as the endpoint continues to be operational in the employee VLAN and the IP address remains unchanged. However, the SGT assignment has changed from 4 to 255, which is the quarantine SGT.

Fabric edge devices will then download SGACL permissions specific to SGT 255, which will limit the endpoint's network access until a successful remediation is performed.

```
Switch# show cts role-based permissions from 255
IPv4 Role-based permissions from group 255:Quarantined_Systems to group
12:Development_Servers:
        Deny IP-00
IPv4 Role-based permissions from group 255:Quarantined_Systems to group
255:Quarantined_Systems:
        Deny IP-00
```

Summary

The Cisco SD-Access solution offers end-to-end segmentation by providing macro- and micro-level segmentation choices to a security administrator regardless of the location. Simple and automated workflows provide a consistent user experience for wired and wireless networks. Network architects and administrators now have the tools to orchestrate key business functions, such as user mobility, secure segmentation, user onboarding, guest access, and context-based troubleshooting, as the Cisco DNA Center analytics engine provides a single pane of glass to most common issues and possible resolutions that once had to be dealt with on a day-to-day basis. Enabling Network as a Sensor and Enforcer within the SD-Access fabric provides a high-level view of network communications, which can be analyzed within a flow monitoring network. Encrypted Traffic Analytics enabled on SD-Access fabric edge devices provides the ability to identify traffic anomalies without having to unencrypt the traffic to perform deep packet analysis. Role-based access control built into the SD-Access fabric using Cisco TrustSec provides the ability to effectively quarantine malware and prevent rapid propagation by blocking east-west communications.

References

Here are some other useful references for Cisco DNA and SD-Access:

- Cisco.com – Software-Defined Access Solution Overview
- Cisco.com – Software-Defined Access Solution FAQ
- Cisco.com – Software-Defined Access Migration Guide
- Cisco.com – Cisco DNA Ready Infrastructure Guide
- Cisco.com – Digital Network Architecture Vision White Paper
- TechWiseTV – Introduction to Cisco Software-Defined Access
- TechWiseTV – A Deeper Look at Cisco Software-Defined Access

Glossary

Table 1 provides some basic definitions for acronyms and/or terminology used in this document.

Table 1. Glossary

Acronym/term	Definition/description
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
AP	Access Point
API	Application Programming Interface
APIC-EM	Application Policy Infrastructure Controller Enterprise Module
BGP	Border Gateway Protocol
CAPWAP	Control And Provisioning of Wireless Access Points
DHCP	Dynamic Host Configuration Protocol
DNA	Digital Network Architecture
EID	Endpoint Identifier (LISP)
ETA	Encrypted Threat Analytics
IGP	Interior Gateway Protocol (EIGRP, OSPF, IS-IS)
IPAM	IP Address Management

Acronym/term	Definition/description
ISE	Identity Services Engine
L2	Layer 2 (switching - Data Link Layer of the OSI model)
L3	Layer 3 (routing - Network Layer of the OSI model)
LAN	Local Area Network
LISP	Locator/Identity Separation Protocol
MTU	Maximum Transmission Unit
NaaS	Network as a Sensor
NDP	Network Data Platform
RLOC	Routing Locator (LISP)
SD-Access	Software-Defined Access
SGT	Scalable Group Tag (or security group tag)
SGACL	Security Group ACL
STP	Spanning Tree Protocol
SXP	SGT Exchange Protocol
VLAN	Virtual LAN
VXLAN	Virtual Extensible LAN
VN	Virtual Network (VRF)
VNF	Virtual Network Function
VRF	Virtual Routing and Forwarding
WAN	Wide Area Network
WLAN	Wireless LAN
WLC	Wireless LAN Controller

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C11-740090-00 01/18