Cisco TrustSec® How-To Guide: User to Data Center Access Control with Cisco TrustSec

Guide

October 2013

Contents

Introduction

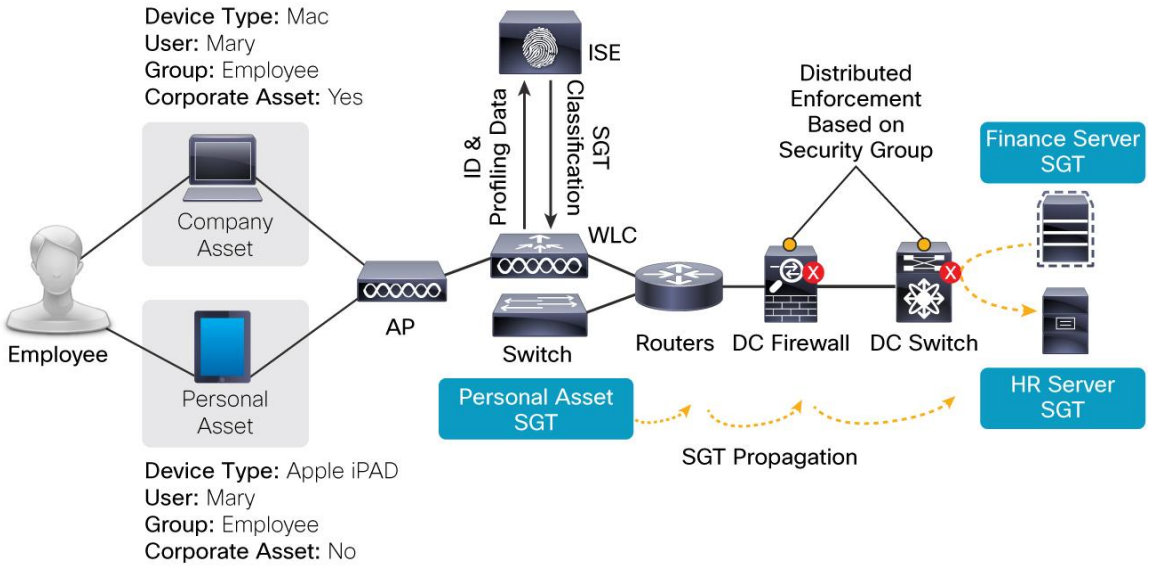
Cisco TrustSec® simplifies the provisioning and management of secure access to network services and applications. Compared to access control mechanisms that are based on network topology, Cisco TrustSec defines policies using logical policy groupings, so secure access is consistently maintained even as resources are moved in mobile and virtualized networks. De-coupling access entitlements from IP addresses and VLANs simplifies security policy maintenance tasks, lowers operational costs, and allows common access policies to be applied to wired, wireless, and VPN access consistently.

Cisco TrustSec classification and policy enforcement functions are embedded in Cisco switching, routing, wireless LAN, and firewall products. By classifying traffic based on the contextual identity of the endpoint versus its IP address, Cisco TrustSec enables more flexible access controls for dynamic networking environments and data centers. At the point of network access, a Cisco TrustSec policy group called a Security Group Tag (SGT) is assigned to an endpoint, typically based on that endpoint's user, device, and location attributes. The SGT denotes the endpoint's access entitlements, and all traffic from the endpoint will carry the SGT information. The SGT is used by switches, routers, and firewalls to make forwarding decisions based on security policy. Since SGT assignments can denote business roles and functions, Cisco TrustSec controls can be defined in terms of business needs and not underlying networking detail.

Cisco TrustSec Overview

Cisco TrustSec technology is embedded in Cisco switches, routers, and firewalls. It is defined in three phases: classify, propagate, and enforce. When the user's traffic enters the network it is classified based on the results of the authentication, such as 802.1X, MAC Authentication Bypass (MAB), or web authentication (WebAuth). Once the user's traffic is classified, Cisco switches and routers then propagate it automatically without any intervention by the network operator until it hits its enforcement point, which can be a Cisco firewall, router, or switch. The enforcement device determines if the user's traffic should be allowed or denied based on the classification.

Figure 1. Cisco TrustSec Phases: Classify, Propagate, Enforce



About This Document

Note: The “introduction to TrustSec” guide should be read first. It is located here: http://www.cisco.com/go/trustsec

This document focuses on how Cisco TrustSec provides access control from user to data center (“north to south”) traffic for wired and wireless users. CiscoTrustSec provides policy-based segmentation and enables secure BYOD access.

The general Cisco TrustSec flow for campus to data center traffic starts with SGT assignment at the access layer. The SGT is then propagated to the data center, where enforcement is performed on devices such as Cisco ASA 5500-X Series Next-Generation Firewalls using SG Firewall oron Cisco Nexus® 7000 Series or 5000 Series Switchesusing Security Group ACLs (SG-ACLs). SGT propagation may be done using SGT Exchange Protocol (SXP) or inline tagging. Which method used is dependent upon the capabilities of the platform and the neighboring platforms that are inline with the traffic flow as shown in Table 1.

Table 1. User to Data Center Access Control Components

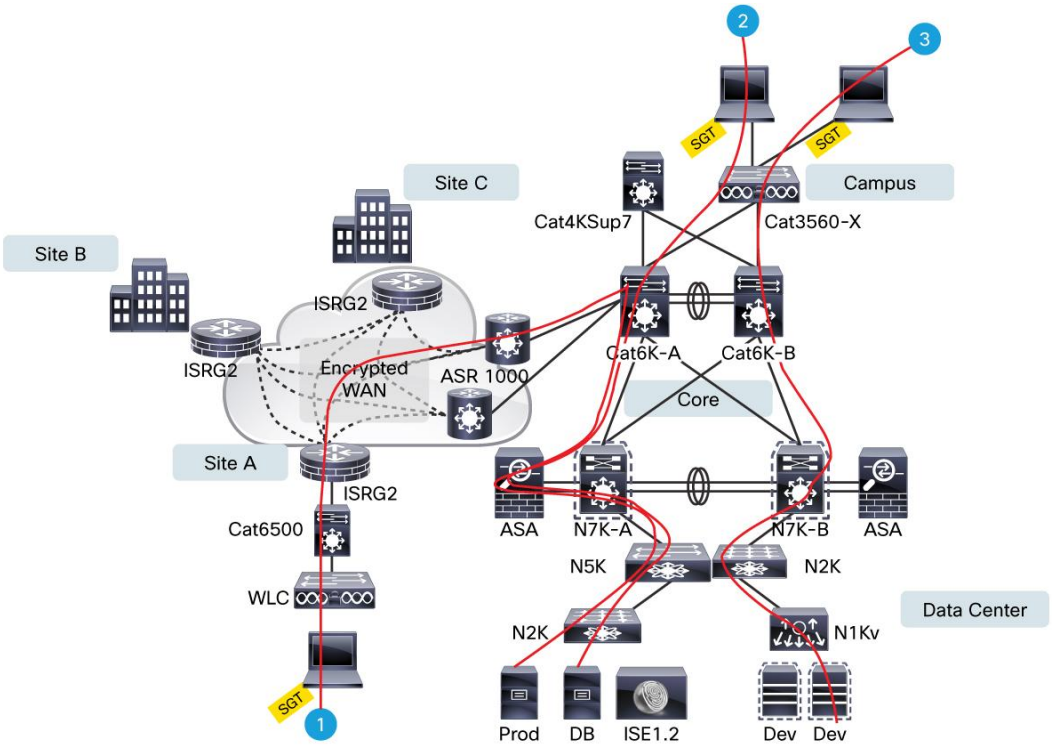
Use Case	SGT Classification at Ingress	SGT Propagation	SGT Enforcement
Role-Based Access Control	Dynamic IP-SGT VLAN-SGT	**SXP:** Catalyst 2960-S, 3000, 4000, 6000 5508 WLC(WiSM2), 2500 WLC(WLCM2) **Inline tagging:** Catalyst 3000-X Catalyst 6000 Sup2T	**SG-FW:** ASA 5500 and 5500-X **SG-ACL:** Catalyst 6000 Sup2T, Catalyst 3000-X, Nexus 7000
BYOD Access Control	Dynamic	**SXP:** 5508 WLC(WiSM2), 2500 WLC(WLCM2)	**SG-FW:** ASA Software Release 9.0 and later **SG-ACL:** Catalyst Sup2T, Catalyst 3000-X, Nexus 7000

In this document, the above use cases are illustrated by three major north to south traffic flows:

1. Branch office user access to data center
2. Campus user access to a data center protected by a firewall
3. Campus user access toserversin the data center

Figure 2 illustrates these three traffic flows.

Figure 2. User to Data Center Traffic Flow Examples



We will first discuss what should be considered when implementing Cisco TrustSec for campus to data center access control.We willthen use the above traffic flow examples to illustrate how the tag is assigned at the access layer and used for enforcement in the data center. Please reference the following table for the Cisco TrustSec classification, propagation, and enforcement methods supported per Cisco device.

Table 2. TrustSec Platform Support

System Component	Platform	Solution Minimum Version	Solution-Level Validated Version	SGT Classification	Control Plane Propagation (SXP)	SGT over Ethernet (Inline SGT)	SGT over MACsec	SGT over xVPN (for WAN)	SGT Enforcement
Cisco Identity Services Engine	Cisco ISE 3315, 3355, 3395, 3415, 3495 Appliances and VMware	ISE 1.0	ISE 1.2 Patch 1 (Requires Advanced License)	-	-	-	-	-	-
Cisco Catalyst® 2000 Series	Cisco Catalyst 2960-Plus Series (LAN Base required)	IOS® 15.2(1)E	-	Dynamic, IP-SGT, VLAN-SGT	SXP (speaker only)	No	No	No	No
	Cisco Catalyst 2960C Series (LAN Base required)	IOS 15.0(1)SE2	IOS 15.0(2)SE2	Dynamic, IP-SGT, VLAN-SGT	SXP (speaker only)	No	No	No	No
	Cisco Catalyst 2960S/SF Series (LAN Base required)	IOS 15.0(1)SE2	IOS 15.0(2)SE2	Dynamic, IP-SGT, VLAN-SGT	SXP (speaker only)	No	No	No	No
	Cisco Catalyst 2960X/XR Series (LAN Base required)	IOS 15.0(2)EX1	-	Dynamic, IP-SGT, VLAN-SGT	SXP (speaker only)	No	No	No	No

System Component	Platform	Solution Minimum Version	Solution-Level Validated Version	SGT Classification	Control Plane Propagation (SXP)	SGT over Ethernet (Inline SGT)	SGT over MACsec	SGT over xVPN (for WAN)	SGT Enforcement
Cisco Catalyst 3000 Series	Cisco Catalyst 3560-E, 3750-E (IP Base required)	IOS 15.0(1)SE2	IOS 15.0(2)SE2	Dynamic, IP-SGT, VLAN-SGT	SXP (S/L)	No	No	No	No
	Cisco Catalyst 3560C Series (IP Base required)	IOS 15.0(1)SE2	IOS 15.0(2)SE2	Dynamic, IP-SGT, VLAN-SGT	SXP (S/L)	No	No	No	No
	Cisco Catalyst 3560-X, 3750-X (IP Base required)	IOS 15.0(1)SE2	IOS 15.0(2)SE4	Dynamic, IP-SGT, VLAN-SGT	SXP (S/L)	Yes	Yes (with C3KX-SM-10G)	No	SGACL
	Cisco Catalyst 3850	-	-	No	No	No	No	No	No
Cisco Catalyst 4000 Series	Cisco Catalyst 4500 (Sup6-E and Sup6L-E) (IP Base required)	IOS15.1.(1)SG	IOS 15.1(1)SG	Dynamic, IP-SGT, VLAN-SGT	SXP (S/L)	No	No	No	No
	Cisco Catalyst 4500 (Sup7-E and Sup7L-E) (IP Base required)	IOS-XE 3.3.0SG	IOS-XE 3.3.0SG	Dynamic, IP-SGT, VLAN-SGT	SXP (S/L)	No	No	No	No
Cisco Catalyst 6500 Series	Cisco Catalyst 6500 (Sup-32 and Sup-720) (IP Base required)	IOS 12.2(33)SXJ2	IOS 12.2(33)SXJ2	Dynamic, IP-SGT	SXP (S/L)	No	No	No	No
	Cisco Catalyst 6500 (Sup-2T) (IP Base required)	IOS 15.0(1)SY1	IOS 15.1(1)SY1	Dynamic, IP-SGT, VLAN-SGT, Subnet-SGT, L3IF-SGT	SXP (S/L)	Yes (requires WS-X69xx line card)	Yes (with Sup2T built-in ports and WS-X69xx line card)	No	SGACL
Cisco Connected Grid Routers	Cisco CGR 2010 Routers	IOS 15.3(2)T	IOS 15.3(2)T	Dynamic, IP-SGT, VLAN-SGT	SXP (S/L)	No	No	SGT over GETVPN	SG Firewall
Cisco Industrial Ethernet Switches	Cisco IE 2000	IOS 15.0(2) EB	IOS 15.0(2) EB	No	No	No	No	No	No
Cisco Wireless Controllers	Cisco 5500 Series and 2500 Series, Cisco Wireless Services Module 2 (WiSM2), Cisco Wireless LAN Controller Module for Integrated Services Routers G2 (WLCM2) **Note:** WLC7500/8500/ vWLC do not support TrustSec	AirOS 7.2 MR1	AirOS 7.4.110	Dynamic	SXP (speaker only)	No	No	No	No
	Cisco WLC 5760	IOS-XE 3.2.1 SE	IOS-XE 3.2.1 SE	No	No	No	No	No	No

System Component	Platform	Solution Minimum Version	Solution-Level Validated Version	SGT Classification	Control Plane Propagation (SXP)	SGT over Ethernet (Inline SGT)	SGT over MACsec	SGT over xVPN (for WAN)	SGT Enforcement
Cisco Nexus® 7000/2000	All Cisco Nexus 7000 line cards and chassis	NX-OS 6.1(1) (SGT support in base license from 6.1)	NX-OS 6.2(2)	Static IP-SGT, L2IF-SGT, Port Profile-SGT	SXP (S/L)	Yes	Yes (All line cards except F1 and F2 line cards)	No	SGACL
Cisco Nexus 5000/2000	Cisco Nexus 5548P, 5596UP	NX-OS 5.1(3)N1	NX-OS 5.1(3)N2(1c)	L2IF-SGT	SXP (speaker only)	Yes (No MACsec option)	No	No	SGACL
Cisco Nexus 1000v	Cisco Nexus 1000v	NX-OS 4.2(1)SV2 (1.1) with Advanced feature license	NX-OS 4.2(1)SV2 (1.1) with Advanced feature license	IP-SGT, Port Profile to SGT	SXP (speaker only)	No	No	No	No
Cisco Integrated Services Router (ISR) G2	Cisco ISR 890, 1900, 2900, 3900 Series	IOS 15.2(2)T	IOS 15.3(2)T	Dynamic, IP-SGT	SXP (S/L)	Only C2951 and C3945	No	SGT over GETVPN	SG Firewall
Cisco ASR 1000 Series Aggregation Services Routers	Cisco ASR 1000 Series Router Processor 1 or 2 (RP1/RP2) ASR 1001, 1002, 1004, 1006, and 1013 Routers with ESP (10, 20, or 40 Gbps) and SIP (10/40)	IOS-XE 3.5	IOS-XE 3.9	Static IP-SGT	SXP (S/L)	Yes	No	SGT over GETVPN	SG Firewall
Cisco ASA 5500 and 5500-X Series	Cisco ASA 5505, 5510, 5520, 5540, 5550, 5580, 5585-X, ASA-SM and5512-X, 5515-X, 5525-X, 5545-X, 5555-X	ASA 9.0.1 ASDM 7.0.1	ASA 9.1 ASDM 7.0.1	-	SXP (S/L)	No	No	No	SG Firewall

Note:

For SXP role, “S” represents “Speaker” and “L” represents “Listener” role.

For classification, propagation, and enforcement, the IP Base/K9 License is required for Catalyst 3560, 3560-E, 3750, 3750-E, 3560-C, 3560-X, 3750-X, Catalyst 4500 Sup6(L)-E, Catalyst 4500 Sup7(L)-E, Catalyst 6500 Sup720, Catalyst 6500 Sup2T.

The ISR Base/K9 License is required for secure access features. For classification, propagation, and enforcement, the ISR SEC/K9 License is required.

The ASR1000 SEC-FW License is required for ASR1000 Series routers for all Cisco TrustSec functions.

Note: Please review the platform support document for current information.

Design Considerations: Classification

In this phase, users and servers are placed into logical groupings, such as engineers and development servers. These grouping can be manually defined or they can be predefined groupings from Active Directory or LDAP servers. These groupings are represented by a Security Group Tag.

A Security Group Tag (SGT) is a unique number that is used to represent the role (or groupings) of a user or server. Every SGT has an associated name (Security Group Name) and value. For example, the employee role can have an arbitrarily assigned value of 101 and a security group name of “employee.” When Cisco TrustSec devices receive traffic tagged with SGT=101, filtering decisions are made based on policies defined for this tag.

SGTs can be centrally created, managed, and administered by the Cisco Identity Services Engine (ISE). Cisco switches, routers, and firewalls query ISE periodically for these SGT-to-role mappings. Once the SGT is created, the next step is to assign the SGT to a user or server.

Assigning the SGT at the Access Layer

At the access layer, dynamic classification is the best method of SGT assignment because SGT assignment occurs as the user enters the network. Dynamic classification starts with an authenticationmethod such as 802.1x, MAB, or WebAuth to provide user-specific control. After authentication, ISE evaluates the policy and will then classify the user and assign an SGT that’s associated with that classification. The tag is then downloaded to the access device, a Cisco switch or wireless LAN controller (WLC), to be associated with the user’s IP and MAC address.

In environments where authentication isn’t available,static classification methods are necessary. At the access layer, the recommended classification method is VLAN to SGT. In this case,theSGT represents the classification of all of the devices within that VLAN.

Note: The ability to provide access control based on user is lost with VLAN to SGT.

For networks with third-party devices or switches that don’t support Cisco TrustSec, static methods like subnet to SGT or Layer 3 interface to SGT are recommended. These methods summarize traffic from a specific subnet or interface to a security group.

Assigning the SGT at the Data Center

Instead of providing campus access through Ciscoswitches and WLCs, where dynamic SGT mappings are communicated and created through 802.1X, most organizations do not implement 802.1X for server connectivity. Commonly used methods of SGT assignment are as follows:

- IP to SGT: Binds the specified host IP address with the specified SGT
- VLAN to SGT: Binds an SGT with a specified VLAN or a set of VLANs
- Port to SGT: Binds an SGT to the port so that the host connected to the port assumes the associated classification (specific to the Nexus 5500 Series)
- Port profile to SGT: Binds an SGT to a port profile so that any port defined with that profile has the same classification (specific to the Nexus 1000V)

Note: At the time of this writing, ISE has the ability to push IP-to-SGT mappings directory to the Nexus 7000 and the Nexus 5000. All other Cisco switching platforms must rely on manual CLI entries or third-party orchestration tools. Please refer to the “Data Center Segmentation” document for further details.

Platform-Specific Considerations

Cisco Catalyst 3560-X and 3750-X Switches:

- Enable “IP Device Tracking” (IPDT) must be enabled to be able to tag/filter. When 802.1X/MAB/WebAuth or VLAN to SGT features are used, IPDT is enabled by default. IPDT must be enabled manually when static assignment is used on a port. To enable IPDT, use the command “ip device tracking maximum xx” (maximum is 10).
- Layer 2-adjacent hosts (small WLCs) trunked these switches is supported. In releases prior to WLC 7.2, SGTs are not supported. A workaround for classification is to assign a SGT to the trunked VLAN at the switch.

Note: Cisco TrustSec enforcement is supported only on up to eight VLANs on a VLAN-trunk link. If there are more than eight VLANs configured on a VLAN-trunk link and Cisco TrustSec enforcement is enabled on those VLANs, the switch ports on those VLAN-trunk links will be error-disabled.

- You cannot statically map an IPsubnet to an SGT. You can only map IP addresses to an SGT. When you configure IP-address-to-SGT mappings, the IP address prefix must be 32.

Note: For additional details, see
http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/appa_cat3k.html#wp1016377

Cisco Catalyst 4500 Series Switches:
See http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/appb_cat4k.html

Design Considerations: Propagation

Inline Tagging vs. SXP

Which propagation method is used is dependent upon the platforms in the path. Not all devices are capable of inline SGT, and some devices support both methods. From an operational perspective, it is best to use inline SGT because with SXP, you're building a peering connection that requires maintenance and introduces scaling limitations. Inline SGT occurs within the data plane so there is no maintenance required.

Inline Tagging and SXP

When it’s necessary to use both inline SGT (data plane) and SXP (control plane) to propagate the SGT through the network, there must be a device in the path that can propagate the SGT between a data plane mechanism and a control plane mechanism (called “SGT caching”). Currently, the Catalyst 6500 with Sup2T is the only device that has this ability. In a user-to-data-center flow, the Cisco ASA firewall is the most common reason why a combination of inline SGT and SXP is necessary. This is because the ASA firewall only supports SXP currently.

Note: Inline SGT support on Cisco ASAplatforms will be available in future software releases.

When the Catalyst 6500 with Sup2T receives a tagged packet on the data plane when SGT caching is enabled, the switchcan propagate the tag via SXP to the ASA firewall (the SXP listener), thus forwarding the traffic untagged. In this case, the tag will be cached and propagated with a default time to live. The ASA firewall can then enforce based on the received SGT and, upon egress, forward the SGT back to the Catalyst 6500 with Sup2T to propagate the tag back onto the data plane.

SXP Scalability

Unlike inline SGT, there are platform specific limits to the number of IP-to-SGT mappings that can be maintained. Please refer to the SXP scalability chart on http://www.cisco.com/go/trustsec for additional information

Platform-Specific Considerations

Cisco Catalyst 3560-X and 3750-X Switches:

- These switches can be SXP listeners for Layer 2 adjacent trafficonly. This means that they cannot be listeners for peers sending aggregated IP-SGT bindings and they cannot take IP-SGT bindings from multi-hop SXP connections.

Cisco Wireless Controllers:

- Wireless LAN Controller to Nexus 7000 Switch: To have the controller peer with the switch, WLC Release 7.4 or later is required.
- Wireless LAN Controller to Cisco ASA Firewall: To have the controller peer with the ASA firewall, WLC release 7.4 or later is required.
- Cisco Wireless Access Points do not support SXP. Therefore, when using FlexConnect, where the data traffic is switched locally, the local switch must use VLAN-to-SGT mapping for classification.

Design Considerations: Enforcement

When choosing the enforcement device, a general guideline is to enforce on the enforcement-capable device that is closest to the resources that are being protected. However, in some cases, the closest enforcement device may not be the best choice because of how the device learned the SGTs, because of device-specific enforcement limitations, or because of compliance policies. We will discuss these dependencies and list some useful features that may affect where enforcement should occur in the traffic flow design section of this document.

Platform-Specific Features

- Monitor Mode: Catalyst 6500 with Sup2T

During the pre-deployment phase, an administrator would use the simulator to see what his or her policies would look like and to make sure those access policies are what he or she intended.

- Per-Policy Change of Authorization

A switch automatically downloads policy from ISE periodically (configurable timer). The switch pulls the policy when this timer expires, so policy changes made before the timer expires require the administrator to manually invoke a policy download from the switch.

To address this, the Catalyst 6500 running Cisco IOS® Software Release 15.1(1)SY or better supports RADIUS Change of Authorization (CoA) for SG-ACLs. This means thatthe administrator can immediately push the new policy from the ISE to the Catalyst 6500 via a CoA request so that the new policy takes effect immediately.

Unknown SGT (SGT=0)

It is unrealistic to have all users and servers mapped to a SGT on the first day. To address this, packets that arrive untagged are tagged with SGT=0 or the “Unknown” tag. In other words, even the lack of an SGT can be used in a security policy.

Unlike ACLs with an implicit deny at the end, SG-ACLs implemented on a switching platform have an implicit permit to Unknown or all; this is not true on the ASA firewall or IOS zone-based firewall acting as an SG-FW where an implicit deny is still maintained. Hence on a switch, by default, if no specific tag value is assigned to a server, the destination is considered Unknown (SGT=0) and the packet is forwarded.

A common error is to create a rule to “deny ip” for the Unknown tag. This, however, would mean that every packet with an Unknown destination tag would be dropped. It is recommended to omit policy for SGT=0 until classifications are fully understood.

Enforcement Priority

If a switch receives SGT mapping information from two classification methods, enforcement is based on the following order of precedence, from lowest (1) to highest (7):

1. **VLAN** - Bindings learned from snooped Address Resolution Protocol (ARP) packets on a VLAN that has VLAN-SGT mapping configured.
2. **CLI** - Address bindings configured using the IP-SGT form of the cts role-based sgt-map global configuration command.
3. **Layer 3 Interface (L3IF)** - Bindings added due to FIB forwarding entries that have paths through one or more interfaces with consistent L3IF-SGT mapping or identity port mapping on routed ports.
4. **SXP** - Bindings learned from SXP peers.
5. **IP_ARP** - Bindings learned when tagged ARP packets are received on a Cisco TrustSec-capable link.
6. **LOCAL** - Bindings of authenticated hosts thatare learned via Cisco Enterprise Policy Managerand device tracking. This type of binding also includes individual hosts that are learned via ARP snooping on Layer 2 Port Mirroring-configured ports.
7. **INTERNAL** - Bindings between locally configured IP addresses and the device’s own SGT.

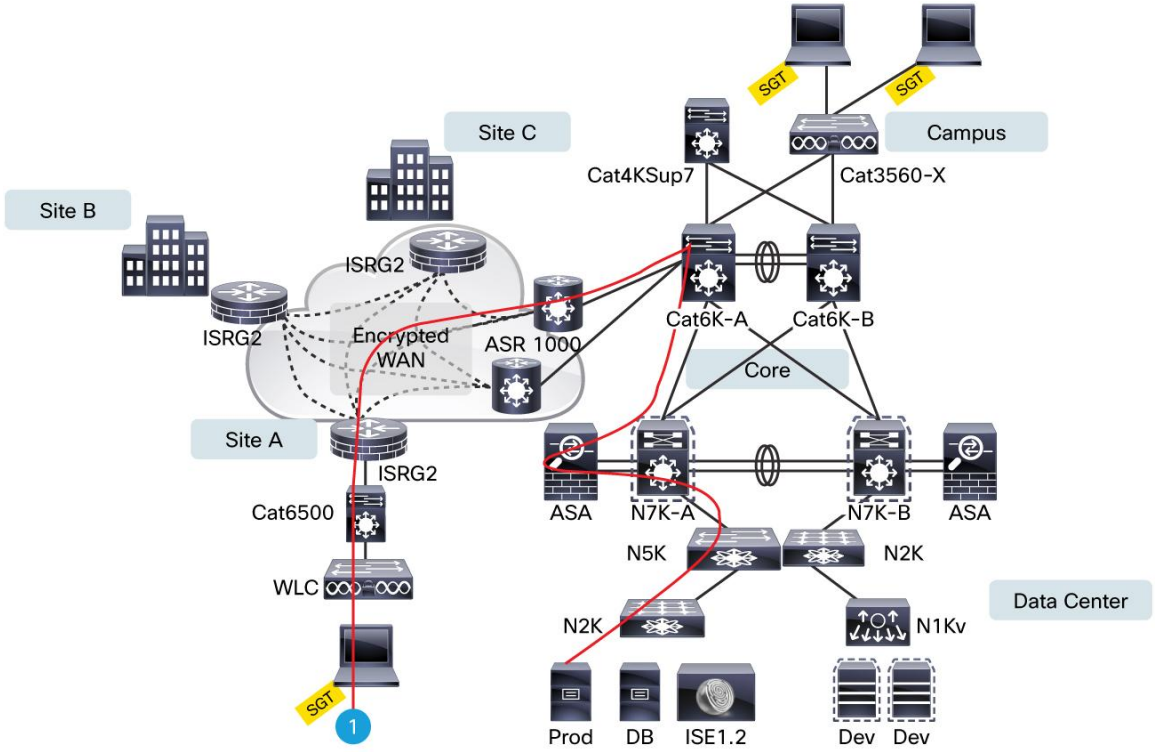
In the next section we’ll look at individual traffic flows as depicted in Figure 1. We’ll go through each flow to determine how classification is done, how the SGT is propagated, and what device provides the enforcement.

Traffic Flow Design

Branch Office User Access to Data Center

In this example, a wireless user at Site A needs to access the production server located in the data center.For compliance reasons, policy dictates that all user traffic must route through the firewall before entering the data center. Therefore, the ASA firewall is chosen as the Cisco TrustSec enforcement point.

To start, classification is done at Site A for the user traffic and at the Nexus 5000 switchfor the production server. Classifications from Site A are propagated to the ASA firewall as the source SGTs. Classifications from the Nexus 5000 switch are propagated to the ASA firewall as the destination SGTs. Finally, these source and destination SGTs are used in an ASA firewall policy.



Classification

Device		SGT Classification	Notes
Access Layer			
WLC		Dynamic	
Data Center			
Nexus 5500	**Port to SGT**		

Propagation

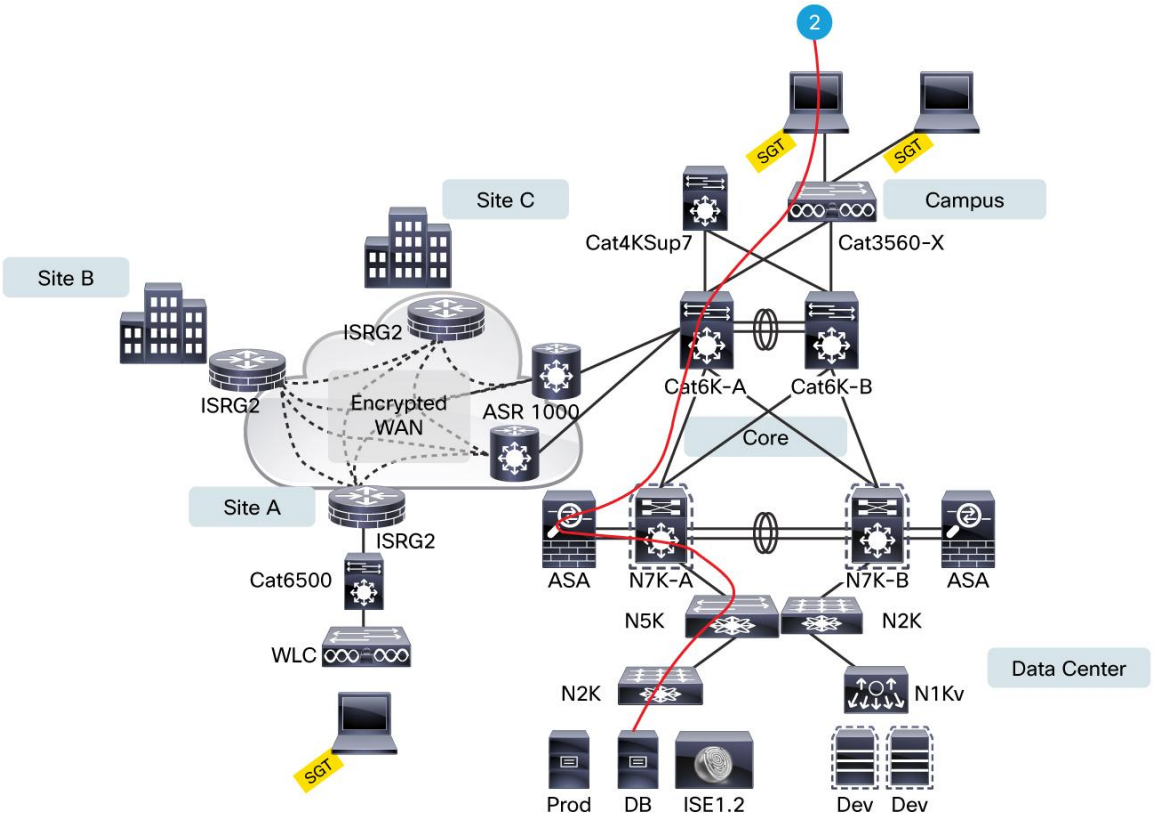
Device	SGT Propagation	Notes
Access Layer to Enforcement Point		
WLC to Catalyst 6500	SXP	WLC is an SXP speaker only
Catalyst 6500(Sup 2T) to ISR **ISR to ASR** **ASR to Campus Catalyst 6500 (Sup 2T) to Cisco ASA 5500/5500-X**	Inline SGT GetVPN Inline SGT	Must have SGT caching enabled on campus Catalyst 6500 (Sup 2T) to propagate SGT from data plane (incoming from ASR) to control plane (outgoing to ASA)
Catalyst 6500(Sup-32 andSup-720) to ISR to ASR to Campus Catalyst 6500 (Sup 2T) to Cisco ASA 5500	SXP	
Data Center Access to Enforcement Point		
Nexus 5500 to Nexus 7000	SXP	Nexus 5500 is an SXP speaker only Nexus 7000 can aggregate all SXP traffic from data center access layer Nexus 7000 6.2.6 code or later is required due to CSCuj14795
Nexus 7000 to Cisco ASA 5500	SXP	

Enforcement

Device	SGT Enforcement	Notes
Cisco ASA 5500	SG-FW	

Campus User to Data Center

In this example, a wired user at the campus access layer needs to access the database server in the data center.Classification is done at the Catalyst 3560-X and Nexus 5000 switches. Classifications from the 3560-X switch are propagated to the ASA firewall as the source SGTs. Classifications from the Nexus 5000 switch are propagated to the ASA firewall as the destination SGTs.



Classification

Device	SGT Classification	Notes
Access Layer		
Catalyst 3560-X	Dynamic	
Data Center		
Nexus 5500	Port and IP to SGT	

Propagation

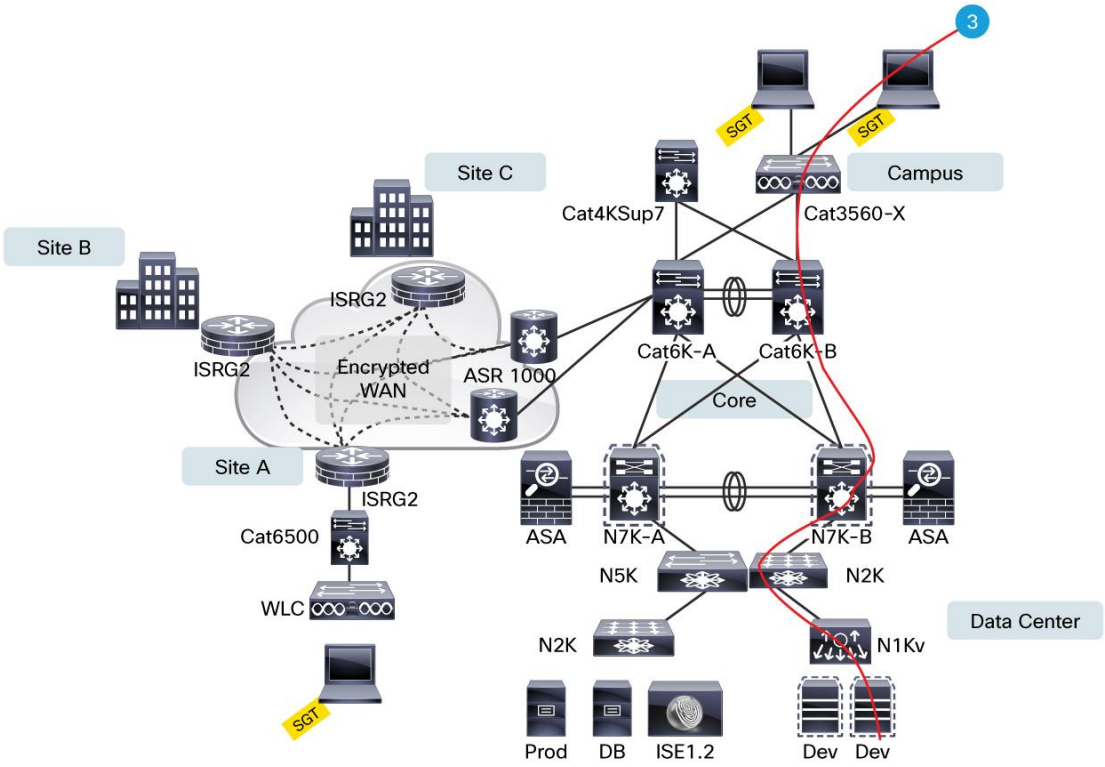
Device	SGT Propagation	Notes
Access Layer to ASA		
Catalyst 3560-X to Catalyst 6500 (Sup 2T) to Cisco ASA 5500	Inline SGT, SXP to ASA	Must have SGT caching enabled on campus Catalyst 6500 (Sup 2T) to propagate SGT from data plane (incoming from Catalyst 3560-X) to control plane (outgoing to ASA)
Catalyst 3560-X to Catalyst 6500(Sup-32 andSup-720) to Nexus 7000 to Cisco ASA 5500	SXP	Nexus 7000 can aggregate all SXP traffic from the access layer and data center Nexus 7000 6.2.6 code or later is required due to CSCuj14795
Data Center Access to ASA		
Nexus 5500 to Cisco ASA 5500	SXP	Nexus 5500 is an SXP speaker only

Enforcement

Device	SGT Enforcement	Notes
Cisco ASA 5500	SG-FW	

Campus to Data Center

In this example, a wired user at the campus access layer needs to access the virtual servers in the data center. Classification is done at the Catalyst 3560-X and the Nexus 1000V switches. Classifications from the Catalyst 3560-X switch are propagated to the Nexus 7000 switch as the source SGTs. Classifications from the Nexus 1000 switch are propagated to the Nexus 7000 switch as the destination SGTs.



Classification

Device	SGT Classification	Notes
Access Layer		
Catalyst 3560-X	Dynamic	
Data Center		
Nexus 1000V	Port-Profile	

Propagation

Device	SGT Propagation	Notes
Access Layer to Nexus 7000		
Catalyst 3560-X to Catalyst 6500 (Sup 2T) to Nexus 7000	Inline SGT	
Catalyst 3560-X to Catalyst 6500(Sup-32 andSup-720) to Nexus 7000	SXP	
Data Center Access to Nexus 7000		
Nexus 1000V to Nexus 7000	SXP	

Enforcement

Device	SGT Enforcement	Notes
Nexus 7000	SG-ACL	

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 www.cisco.com/go/offices.

Printed in USA C07-729951-00 10/13