Cisco TrustSec 4.0:How to Create Campus and Branch-Office Segmentation

Ordering Guide

November 2013

Contents

Introduction

Cisco TrustSec® technology segments wired and wireless networks using security policies. Cisco TrustSec features are embedded in Cisco switching, routing, wireless LAN, and firewall products to protect assets, endpoints, and applications in enterprise and data center networks.

Cisco TrustSec controls improve upon traditional methods, which segment and protect assets using VLANs and access control lists (ACLs). Instead, the solution defines access entitlements by security group policies written in a plain language matrix (Figure 1). Users and assets with the same role classification are assigned to the same security group. These policies are decoupled from IP addresses and VLANs, so resources can be moved without re-engineering the network.

Cisco TrustSec policies are centrally created and automatically distributed to wired, wireless, and VPNs for enforcement. Users and assets thus receive consistent access and protection as they move in virtual and mobile networks. This consistency helps reduce the time needed for network engineering and compliance validation.

Figure 1. TrustSec Policy Management Matrix Example

Destination ▶ Source ▼	Employee	E-Mail	Finance	Internet
Employee	Deny	Permit	Deny	Permit
Executive	Deny	Deny	Permit	Permit
BYOD	Deny	Permit	Deny	Permit
Guest	Permit	Deny	Deny	Permit

About This Document

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

The Cisco TrustSec solution provides simplified and scalable policy enforcement for network traffic between campus and branch-office users, commonly referred as “east to west” traffic. Initially Cisco ASR 1000 series and Cisco ISR Series routers supported SXP for tag propagation across the WAN. Today has expanded to include various VPN methods: IP Security (IPsec), Dynamic Multipoint VPN (DMVPN), or Group Encrypted Transport VPN (GET VPN). This document will first discuss what should be considered when implementing Cisco TrustSec. Then through traffic flow examples to illustrate how to design TrustSec through the classification, propagation, and enforcement phases.

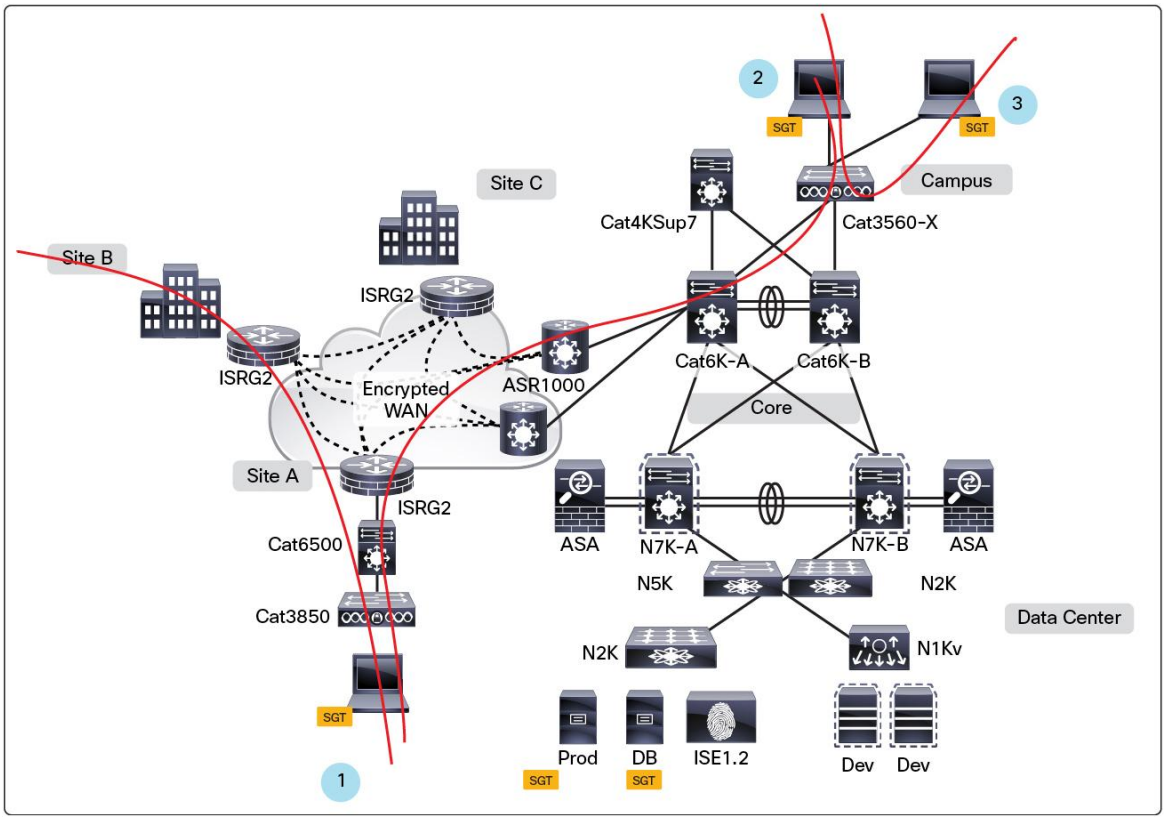
Table 1. Campus and Branch-Office Segmentation Components

Use Case	SGT Classification (at Ingress)	SGT Propagation	SGT Enforcement
Role-based user segmentation	Dynamic, VLAN to SGT	Security Group Exchange Protocol (SXP): Cisco Integrated Services Routers (ISR) Inline tagging: Cisco Catalyst® 3000 Series Routers Cisco Catalyst 6000 Series Supervisor 2T	Security group firewall (SGFW): Cisco ISR and Adaptive Security Appliances Security group ACL: Cisco Catalyst 6000 Series Supervisor 2T and 3500-X Series
Cyber security and malware propagation control	Dynamic	Inline tagging: Cisco Catalyst 3500-X Series	Security group ACL: Cisco Catalyst 3500-X Series

The use cases in Table 1 are illustrated by three major east-to-west traffic flows:

- Site to site: Here we want to block a user at site A from communicating with a user at site B. To accomplish this, the classifications from sites A and B are sent by Security Group Exchange Protocol (SXP) to the headend Cisco Aggregation Services Router (ASR). The Cisco ASR then “reflects” the mappings back to the site-specific Cisco ISRs so that the local firewall can enforce policy.
- Campus to branch office: Users connecting to the campus from a branch-office network need to access resources in the campus and in other branch offices. In this case the branch-office access switch assigns the SGT using identity-based features. These SGTs may be used for local enforcement on a security group firewall (SGFW) module on the Cisco ISR or ASR. Additionally, the local Cisco ISR can propagate SGTs into the campus site over the WAN using various VPN methods: IP Security (IPsec), Dynamic Multipoint VPN (DMVPN), or Group Encrypted Transport VPN (GET VPN). Then by using the SGTs distributed across the WAN, the campus network switches may enforce traffic from the remote branch-officeusers.
- Campus to campus: Within the same Layer 2 domain on the same switch, Cisco TrustSec policies may be used to prevent user-to-user communication. This is a unique method of controlling malware propagation.

Figure 2. Examples of Campus and Branch-Office Segmentation Traffic Flows



Each of these traffic flows illustrates what should be considered in the network design. Table 2 shows the Cisco TrustSec classification, propagation, and enforcement methods supported in Cisco devices. A complete list is available at Cisco.com/go/TrustSec.

Table 2. Cisco 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, and 3495 Appliances and VMware	Cisco ISE Release 1.0	Cisco ISE Release 1.2 Patch 1 (requires Advanced License)	-	-	-	-	-	-
Cisco Catalyst 2000 platform switches	Cisco Catalyst 2960-Plus Series Switches (LAN Base required)	Cisco IOS® Software Release 15.2(1)E	-	Dynamic, IP to SGT, VLAN to SGT	SXP (speaker only)	No	No	No	No
	Cisco Catalyst 2960-C Series Switches (LAN Base required)	Cisco IOS Software Release 15.0(1)SE2	Cisco IOS Software Release15.0(2)SE2	Dynamic, IP to SGT, VLAN to SGT	SXP (speaker only)	No	No	No	No
	Cisco Catalyst 2960-S and 2960-SF Series Switches (LAN Base required)	Cisco IOS Software Release15.0 (1)SE2	Cisco IOS Software Release 15.0(2)SE2	Dynamic, IP to SGT, VLAN to SGT	SXP (speaker only)	No	No	No	No
	Cisco Catalyst 2960-X and 2960-XR Series Switches (LAN Base required)	Cisco IOS Software Release15.0 (2)EX1	-	Dynamic, IP to SGT, VLAN to SGT	SXP (speaker only)	No	No	No	No
Cisco Catalyst 3000 Series Switches	Cisco Catalyst 3560-E and 3750-E Series Switches (IP Base required)	Cisco IOS Software Release15.0 (1)SE2	Cisco IOS Software Release 15.0(2)SE2	Dynamic, IP to SGT, VLAN to SGT	SXP (S, L)	No	No	No	No
	Cisco Catalyst 3560-C Series Switches (IP Base required)	Cisco IOS Software Release15.0 (1)SE2	Cisco IOS Software Release15.0(2)SE2	Dynamic, IP to SGT, VLAN to SGT	SXP (S, L)	No	No	No	No
	Cisco Catalyst 3560-X and 3750-X Series Switches (IP Base required)	Cisco IOS Software Release15.0 (1)SE2	Cisco IOS Software Release15.0(2)SE4	Dynamic, IP to SGT, VLAN to SGT	SXP (S, L)	Yes	Yes (with Cisco Catalyst 3000-X-SM10Gbps)	No	SGACL
	Cisco Catalyst 3850 Series Switches	-	-	No	No	No	No	No	No
Cisco Catalyst 4000 Series Switches	Cisco Catalyst 4500 Supervisor Engines 6-E and 6L-E (IP Base required)	Cisco IOS Software Release15.1.(1)SG	Cisco IOS Software Release15.1(1)SG	Dynamic, IP to SGT, VLAN to SGT	SXP (S, L)	No	No	No	No
	Cisco Catalyst 4500 Supervisor Engines 7-E and 7L-E (IP Base required)	Cisco IOSXE 3.3.0SG	Cisco IOSXE 3.3.0SG	Dynamic, IP to SGT, VLAN to SGT	SXP (S, L)	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 6500 Series Switches	Cisco Catalyst 6500 Series Supervisor Engines 32 and 720 (IP Base required)	Cisco IOS Software Release12.2 (33)SXJ2	Cisco IOS Software Release12.2(33)SXJ2	Dynamic, IP to SGT	SXP (S, L)	No	No	No	No
	Cisco Catalyst 6500 Series Supervisor Engine 2T (IP Base required)	Cisco IOS Software Release15.0 (1)SY1	Cisco IOS Software Release 15.1(1)SY1	Dynamic, IP to SGT, VLAN to SGT, subnet to SGT, Layer 3 interface to SGT	SXP (S, L)	Yes (requires Cisco WS-X6900 Series line cards)	Yes (with Supervisor Engine 2T built-in ports and Cisco WS-X6900 Series line cards)	No	SGACL
Cisco Connected Grid Routers	Cisco 2010 CGR Router	Cisco IOS Software Release15.3 (2)T	Cisco IOS Software Release 15.3(2)T	Dynamic, IP to SGT, VLAN to SGT	SXP (S, L)	No	No	SGT over GETVPN	SGFW
Cisco Industrial Ethernet Switches	Cisco IE 2000	Cisco IOS Software Release 15.0 (2) EB	Cisco IOS Software Release 15.0(2) EB	No	No	No	No	No	No
Cisco Wireless Controllers	Cisco 5500 Series and 2500 Series Wireless Controllers (WLCs), Cisco Wireless Services Module 2 (WiSM2), and Cisco Wireless LAN Controller Module for Integrated Services Routers G2 (WLCM2) **Note:** Cisco 7500 WLC, 8500 WLC, and vWLC do not support Cisco TrustSec functions	Cisco AireOS7.2 MR1	Cisco AireOS7.4.110	Dynamic	SXP (speaker only)	No	No	No	No
	Cisco 5760 Wireless LAN Controller	Cisco IOSXE3.2.1 SE	Cisco IOSXE 3.2.1 SE	No	No	No	No	No	No
Cisco Nexus® 7000 Switches and 2000 Series Fabric Extenders	All Cisco Nexus 7000 Series line cards and chassis	Cisco NX-OS Software Release 6.1(1) (SGT support in Base License in 6.1 and later)	Cisco NX-OS Software Release6.2(2)	Static IP to SGT, Layer 2 interface to SGT, port profile to SGT	SXP (S, L)	Yes	Yes (All line cards except F1 and F2 Series modules)	No	SGACL
Cisco Nexus Series 5000 Switches and 2000 Series Fabric Extenders	Cisco Nexus 5548P and 5596UP Switches	Cisco NX-OS Software Release 5.1(3)N1	Cisco NX-OS Software Release 5.1(3)N2(1c)	Layer 2 interface to SGT	SXP (speaker only)	Yes (no MACsec option)	No	No	SGACL

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 1000V Switches	Cisco Nexus 1000V Switches	Cisco NX-OS Software Release4.2(1) SV2(1.1) with Advanced feature license	Cisco NX-OS Software Release 4.2(1)SV2(1.1) with Advanced feature license	IP to SGT, port profile to SGT	SXP (speaker only)	No	No	No	No
Cisco Integrated Services Routers Generation 2 (ISR G2)	Cisco 890, 1900, 2900, and 3900 Series Integrated Services Routers	Cisco IOS Software Release15.2 (2)T	Cisco IOS Software Release15.3(2)T	Dynamic, IP to SGT	SXP (S, L)	Only on Cisco 2951 and 3945 ISRs	No	SGT over GETV PN	SGFW
Cisco ASR 1000 Series Aggregation Services Routers	Cisco ASR 1000 Series Routers Processor 1 and 2 (RP1andRP2); and Cisco ASR 1001, 1002, 1004, 1006, and 1013 Routers with Encapsulating Security Payload (ESP) (10, 20, and 40 Gbps) and Shared Port Adapter Interface Processor (SIP) (10 and 40)	Cisco IOSXE 3.5	Cisco IOSXE 3.9	Static IP to SGT	SXP (S, L)	Yes	No	SGT over GETV PN	SGFW
Cisco ASA 5500 and 5500-X Series firewalls	Cisco ASA 5505, 5510, 5520, 5540, 5550, 5580, 5585-X, 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X service modules and firewalls	Cisco ASA 9.0.1 and Cisco ASDM 7.0.1	Cisco ASA 9.1 and Cisco ASDM 7.0.1	-	SXP (S, L)	No	No	No	SGFW

Notes:

For SXP roles, S represents Speaker and L represents Listener.

The Cisco IP Base-K9 license is required for the Cisco Catalyst 3560, 3560-C, 3560-E, 3560-X, 3750, 3750-E, and 3750-X Series Switches; Cisco Catalyst 4500 Supervisor Engine 6-E and Supervisor Engine 6L-E, Cisco Catalyst 4500 Supervisor Engine 7-E and Supervisor Engine 7L-E, Cisco Catalyst 6500 Series Supervisor Engine 720, and Cisco Catalyst 6500 Series Supervisor Engine 2T.

The Cisco ISR Base-K9 license is required for Cisco Secure Access features. For Cisco TrustSec classification, propagation, and enforcement functions, the Cisco ISR SEC-K9 license is required.

The Cisco ASR1000 SEC-FW license is required for Cisco ASR 1000 Series Aggregation Services Routers for all Cisco TrustSec functions.

Design Considerations: Classification

In this phase, users (for example, engineers) and servers (for example, development servers) are placed into logical groups. These groups can be manually defined, or they can be predefined from Active Directory or Lightweight Directory Access Protocol (LDAP) servers. The groups are each represented by an SGT.

The SGT is a unique number that is used to represent the role (or group) 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 the security group name "employee." When Cisco TrustSec devices receive traffic tagged "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 the Cisco ISE periodically for these SGT-to-role mappings. After 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 authentication method such as IEEE 802.1X, MAC Authentication Bypass (MAB), or Web authentication (WebAuth) to provide user-specific control. After authentication, the Cisco ISE evaluates the policy, classifies the user, and assigns an SGT that is 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 the SGT represents the classification of all of the devices within that VLAN.

Note: The capability to enforce access policies that are based on user identities is lost with VLAN-to-SGT classifications.

For networks with third-party devices or switches that do not support Cisco TrustSec functions, 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.

Platform-Specific Considerations

The Cisco Catalyst switches assign SGTs differently:

- Cisco Catalyst 3560-X and 3750-X Series Switches:
  - IP Device Tracking (IPDT) must be enabled before you can tag and filter traffic. When IEEE 802.1X, MAB or WebAuth authentication methods 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** (the maximum value for "xx" is 10).
  - Cat 3K-X can have Layer 2 adjacent hosts (small WLCs) trunked to Cat3K-X. This is useful in the case where the Cisco Wireless LAN Controller that does not have TrustSec support (pre 7.2 WLC code) You can assign a SGT to the trunked VLAN at the switch.

Note: Cisco TrustSec enforcement is supported on only eight or fewer VLANs on a VLAN-trunk link. If more than eight VLANs are 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 map only 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: Please consult the Cisco TrustSec Switch Configuration Guide for notes about the Catalyst 4500 Series Switches (http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/appb_cat4k.html).

Design Considerations: Propagation

Inline Tagging Compared with SXP

Which SGT-propagation method is used depends on the platforms in the path. Not all devices are capable of inline SGT, but some devices support both inline tagging and SXP. Inline SGT is better from an operational perspective. Inline SGT occurs within the data plane, so there is no maintenance required.

SXP Scalability

With SXP, you are building a peering connection that requires maintenance. Unlike inline SGT, SXP also limitsthe number of IP-to-SGT mappings that can be maintained. Please refer to the SXP scalability chart on the Cisco TrustSec home page (http://www.cisco.com/go/trustsec) for additional information.

Platform-Specific Considerations

The Cisco Catalyst switches and wireless controllers propagate SGTs differently:

- Cisco Catalyst 3560-X and 3750-X Switches:
  - These switches can be SXP listeners for Layer 2-adjacent traffic only. They cannot be listeners for peers sending aggregated IP-to-SGT bindings, and they cannot take IP-to-SGT bindings from multihop SXP connections.
- Cisco Wireless Controllers:
  - To have the Cisco Wireless LAN Controller peer with the Cisco Nexus 7000 Series Switch, the Cisco WLC Release 7.4 or later is required.
  - To have the Cisco Wireless LAN Controller peer with a Cisco ASA, Cisco WLC Release 7.4 or later is required.
  - Cisco wireless access points do not support SXP. Therefore, if you are using a Cisco FlexConnect™ solution where the data traffic is switched locally, the local switch must use VLAN -to-SGT mapping for classification.

Design Considerations: Enforcement

A general guideline for enforcing policies is to use the device closest to the resources that are being protected. However, in some cases, the closest enforcement device may not be the best choice because of the way the device learned the SGTs, because of device-specific limitations, or because of compliance policies. The traffic flow design section will outline these limitations and list some useful features that may influence where enforcement should occur.

Unknown SGT (SGT=0)

It is unrealistic to have all the users and servers mapped to an SGT on the first day. To address this, packets that arrive untagged are tagged “SGT=0,” 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, security group ACLs (SGACLs) implemented on a switching platform have an implicit permit to Unknown or an implicit permit to all. This policy is not enforcedon the Cisco ASA firewall or the Cisco IOS zone-based firewall acting as an SGFW, where an implicit deny is still maintained. On a switch, if no specific tag value is assigned to a server, the destination is considered Unknown and the packet is forwarded by default.

A common error is to create a rule to deny the IP address of the Unknown tag. This, however, means that every packet with an Unknown destination tag will be dropped. It is best to omit a 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-to-SGT mapping configured.
2. Command-line interface (CLI): Address bindings configured using the IP-to-SGT form of the Cisco TrustSec role-based SGT-map global configuration command.
3. Layer 3 Interface (L3IF): Bindings added using Forwarding Information Base (FIB) entries that have paths through one or more interfaces with consistent L3IF-to-SGT mapping or with identity port mapping on routed ports.
4. SXP: Bindings learned from SXP peers.
5. IPARP: Bindings learned when tagged ARP packets are received on a Cisco TrustSec capable link.
6. Local: Bindings of authenticated hosts that are learned by means of Cisco Enterprise Policy Manager and device tracking. This type of binding also includes individual hosts that are learned by means of ARP snooping on Layer 2 ports that are configured forportmirroring.
7. Internal: Bindings between locally configured IP addresses and the device’s own SGT.

Platform-Specific Considerations

The Cisco ASR and ISR routers treat SGTs differently:

- Cisco ASR 1000 Series routers: SGTs can be used for the source and destination values in a firewall rule.
- Cisco ISR G2: SGTs can be used for the source values only in a firewall rule.

Traffic Flow Design

This section examines each flow in Figure 1 to determine how classification is performed, how the SGT is propagated, and what device provides the enforcement.

Traffic flow 1: Site-to-Site Segmentation

In site-to-site segmentation, the source classification is done at Site A and the SGT is propagated to a Cisco ISR using inline tagging or SXP depending upon what the distribution layer device supports (Figure 3). The Cisco ISR at site A can perform SGFW enforcement with SGTs for source and destination so that traffic destined to Site B does not need to traverse the WAN. In order for Site A Cisco ISR to provide this enforcement, the SGTs from Site B must be propagated to Site A via SXP or by some vpn method.

Please note that if there are multiple sites and if SXP is necessary, the Cisco ISR and ASR both support SXPv4. SXPv4 supports loop detection. Therefore, SXP peering can be done just between the Cisco ISRs and ASRs. You do not have to create an SXP mesh between ISRs.

Table 3 shows the classification, SGT propagation, and enforcement for each device in site-to-site segmentation.

Figure 3. Site-to-Site Segmentation

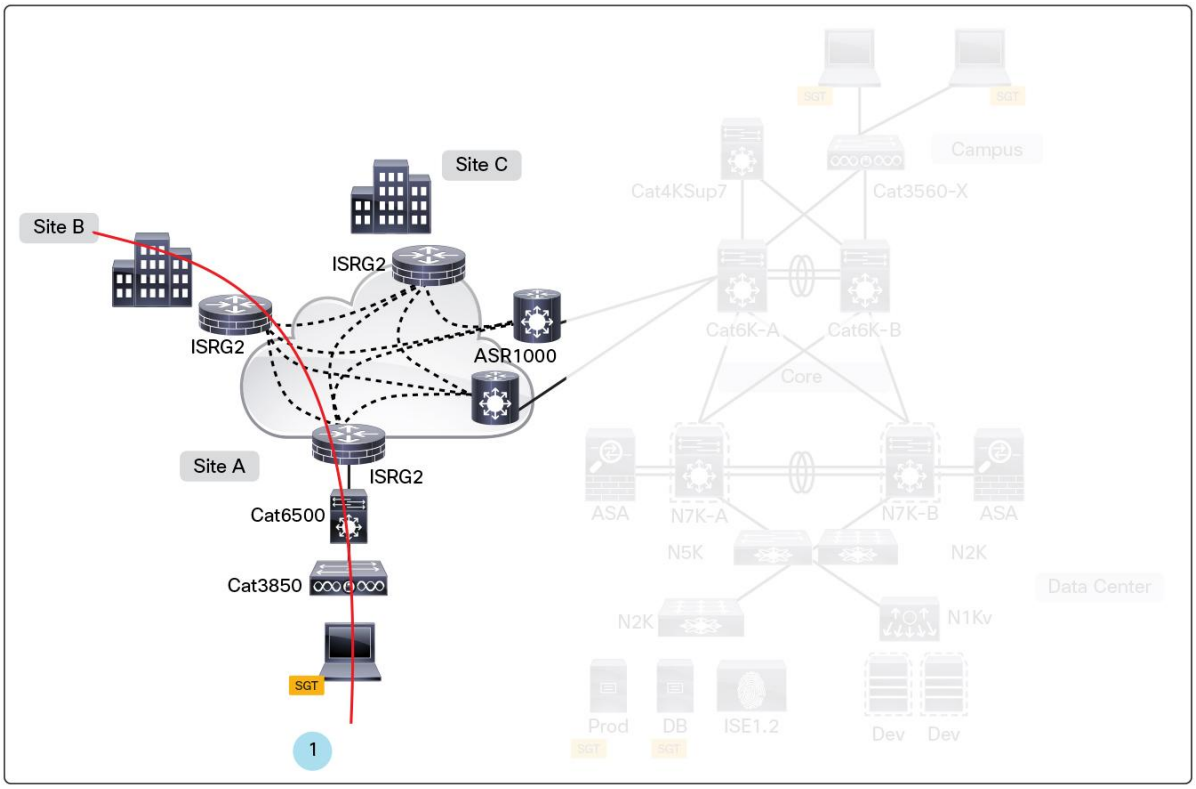


Table 3. Classification, SGT Propagation, and Enforcement Methods for Site-to-Site Segmentation

Classification

Device	SGT Classification	Notes
Access Layer		
Cisco Catalyst 3850Series Switches	dynamic	

Propagation

Device	SGT Propagation	Notes
From Site A		
Cisco Catalyst 6500 Series with SUP2T to site A Cisco ISR G2	inline	
Cisco Catalyst 6500 Series with SUP720 to site A Cisco ISR G2	SXP	

Enforcement

Device	SGT Enforcement	Notes
Site A ISR	SGFW	Zone based firewall rules can only use SGTs as the source of the traffic flow. Cisco ASR is required to provide SGT based source and destination rules.

Traffic Flow 2: Campus to Branch Office

In campus-to-branch-office segmentation enforcement is possible at the core or at the branch office (Figure 4). The user is dynamically classified on the Cisco Catalyst 3560-X Series Switch. This classification is then communicated to the Cisco Catalyst 6500 Series Supervisor 2T using inline tagging. The Cisco Catalyst 6500 can propagate the SGT to the Cisco ASR using inline tagging. The Cisco ASR may perform enforcement based on SGFW rules, or it can propagate the tags using SGTover DMVPN, SGT over GETVPN, or SXP to the Cisco Catalyst 6500 in the destination branch office for enforcement. Table 4 shows the classification, SGT propagation, and enforcement method for each device.

Figure 4. Campus-to-Branch-Office Segmentation

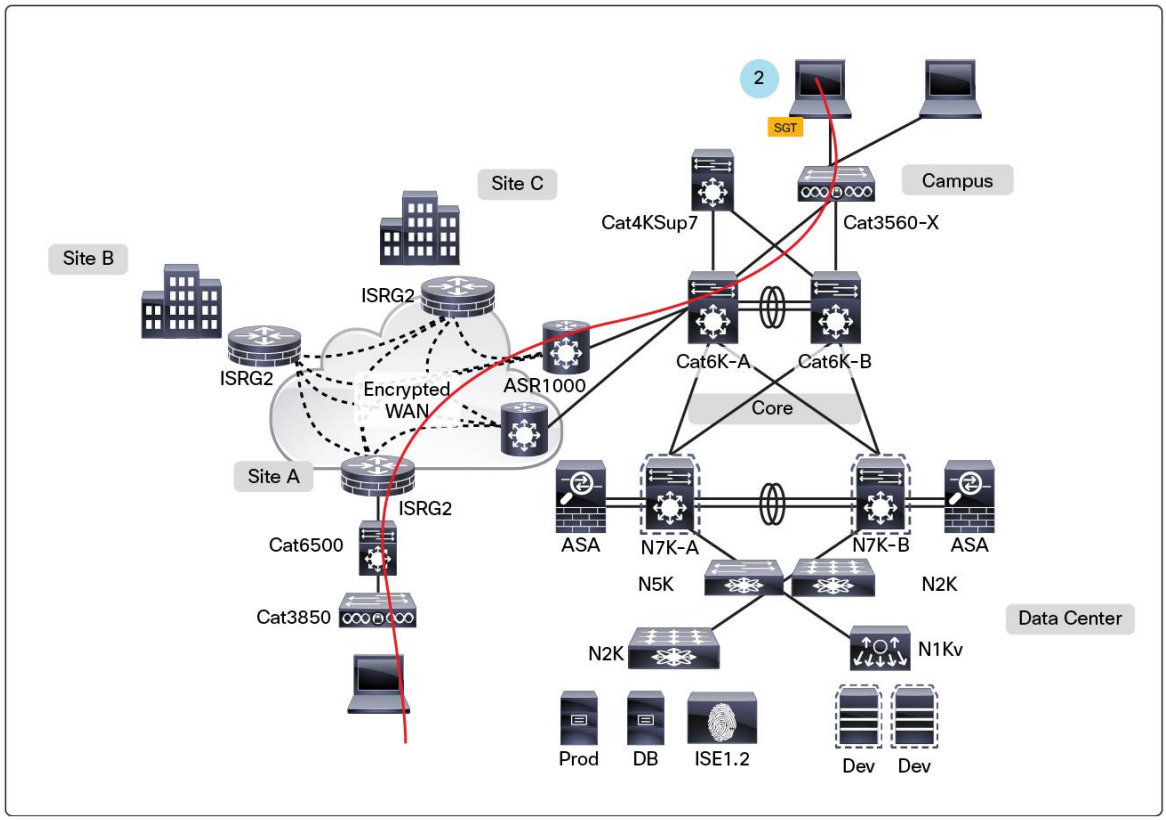


Table 4. Classification, SGT Propagation, and Enforcement Methods for Campus-to-Branch-Office Segmentation

Classification

Device	SGT Classification	Notes
Campus Access Layer		
Cisco Catalyst 3500-X Series Switches	Dynamic	
Branch-Office Access Layer		
Cisco Catalyst 3850 Series Switch	Dynamic	

Propagation

Device	SGT Propagation	Notes
From the Campus Access Layer Toward the Branch Office		
Cisco Catalyst 3560-X to Catalyst 6500 Series Switches with SUP2T to Cisco ASR **Cisco Catalyst 3560-X to Catalyst 6500 Series Switches with SUP720 to Cisco ASR**	Inline SXP	
From the Branch-Office Access LayerToward the Campus		
Cisco Catalyst 3850 to Cisco Catalyst 6500 Series Switches with SUP 2T to Cisco ISR	Inline	

Enforcement

Device	SGT Enforcement	Notes
Cisco ASR	SGFW enforcement	
Cisco Catalyst 6500 Series Switches	SGACL	Enforcement provided here if traffic originates from Site A.

Traffic Flow 3: Campus to Campus

In campus-to-campus segmentation you have two users connected to the Layer 2 switch (Figure 5). These users can be connected to the same VLAN or to different ones. You can use SGTs to tag each user and use SGACLs, rather than ACLs, to enforce traffic between them (Figure 5). Table 5 shows the classification, SGT propagation, and enforcement method for each device.

Figure 5. Campus-to-Campus Segmentation

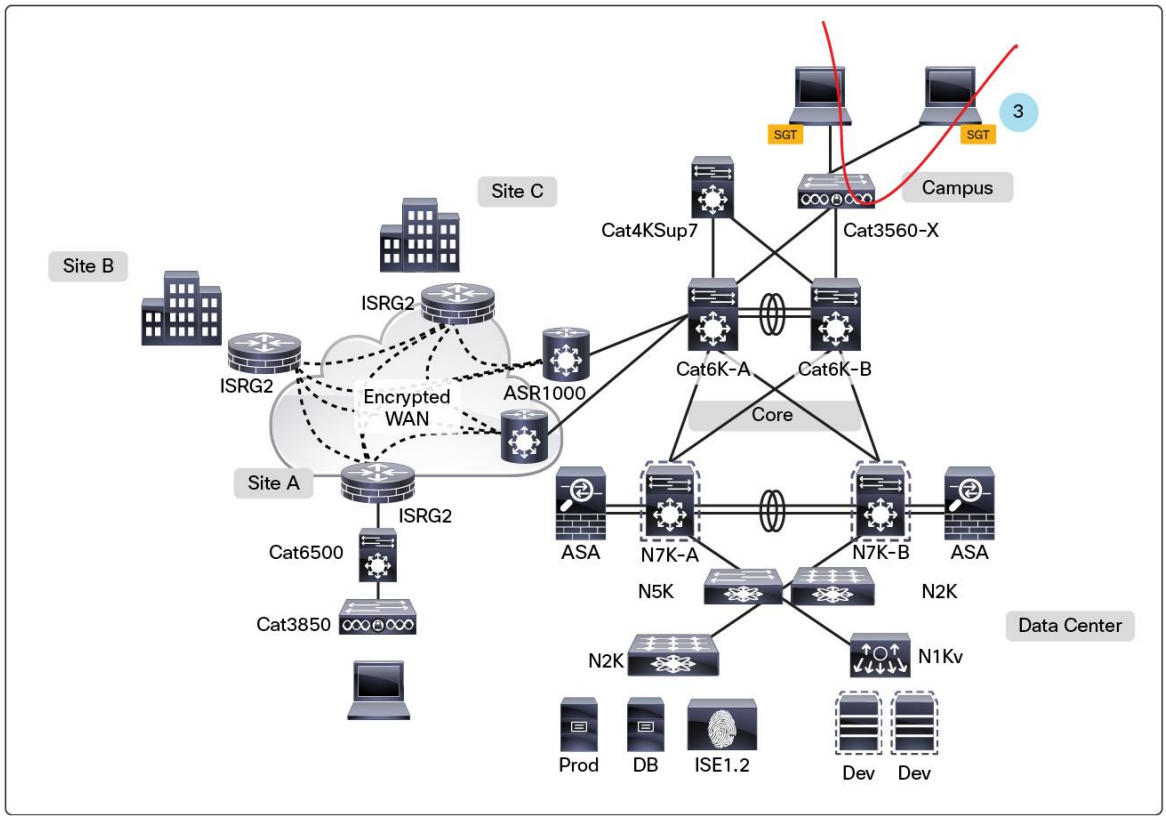


Table 5. Classification, SGT Propagation, and Enforcement Methods for Campus-to-Campus Segmentation

Classification

Device	SGT Classification	Notes
Campus Access Layer		
Cisco Catalyst 3560-X Series Switches	Dynamic	

Device	SGT Propagation	Notes
Cisco Catalyst 3500-X to Catalyst 3500-X Series Switch	None	No need to propagate the SGT since enforcement is possible

Enforcement

Device	SGT Enforcement	Notes
Cisco Catalyst 3500-X Series Switches	SGACL	

Note: In this example, a Cisco 3500-X Series Switch was used. You can also achieve this type of segmentation with other Catalyst switches that don't support enforcement by using private VLANs to force the traffic to a distribution switch that performs SGACL enforcement.

It is also possible to provide peer to peer segmentation with a Cisco 3850 Series Switch. The Cisco 3850 with TrustSec uniquely provide segmentation between wired and wireless users.

For More Information

Please reference http://www.cisco.com/go/trustsec.

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 C07-730150-00 11/13