Cisco TrustSec Software-Defined Segmentation Release 6.0 System Bulletin

Introduction

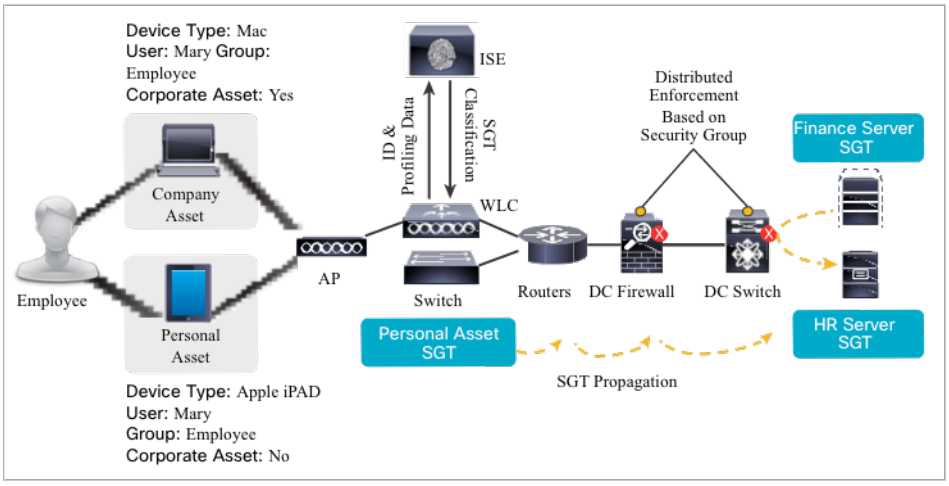
Network segmentation is essential for protecting critical business assets. Cisco TrustSec® Software Defined Segmentation balances the demands for agility and security without the operational complexity and difficulty of deploying into existing environments seen with traditional segmentation. With TrustSec, endpoints are classified into groups that can be used anywhere on the network. This allows us to decouple the segmentation policies from the underlying network infrastructure. Software-defined segmentation is much easier to enable and manage than VLAN-based segmentation and avoids the associated processing impact on network devices.

By classifying systems using human-friendly logical groups, security rules can be defined using these groups, not IP addresses. Controls using these endpoint roles are more flexible and much easier to manage than using IP address-based controls. TrustSec Security Groups can indicate the role of the system or person, the type of application a server hosts, the purpose of an IoT device, or the threat-state of a system, which IP addresses alone cannot. These security groups can simplify firewall and next-gen firewall rules, Web Security Appliance policies and the access control lists used in switches, WLAN controllers, and routers.

Cisco's Identity Services Engine (ISE) acts as the controller for software-defined segmentation groups and policies, providing a layer of policy abstraction and centralized administration. ISE allows segmentation policies to be applied to networks of any size using a simple and clear policy matrix. ISE is able to share group information with other group-based policy schemes used in Cisco's Application-Centric Infrastructure and in Open Daylight, the open source SDN controller, to simplify security policy management across domains.

TrustSec embedded technology is embedded in Cisco switches, routers, wireless LAN and security products and is the foundation for using a Network as an Enforcer. TrustSec enforcement capabilities mitigate risk by reducing attack surface through better segmentation, whilst also increasing operational efficiency and making compliance goals easier to achieve.

Figure 1. Example of Cisco TrustSec in the Network



To help smooth customer deployments of the complete solution, Cisco has developed a rigorous validation process that encompasses component-level and end-to-end interoperability, scalability and performance tests. The validated platform list is intended to make it easy to assess an existing network to understand the areas of the network where TrustSec can be quickly enabled.

Summary of New Cisco TrustSec Capabilities

The Cisco TrustSec 6.0 release continues to validate three major deployment scenarios. All three of these TrustSec deployment scenarios can be used to help achieve regulatory compliance and have been validated by Verizon Business as a means to reduce the audit scope for Payment Card Industry Data Security Standard (PCI- DSS) regulatory requirements.

- Controlling access to data centers, to help organizations gain visibility into and effective control over mobile devices, whether managed or unmanaged, accessing network services and company data.
- Campus and Branch network segmentation, to allow organizations to set access policies based on the user or device role, instead of using logical boundaries, such as VLAN or subnet, along with static access control lists.
- Data Center segmentation and micro-segmentation. Segmentation of any combination of virtual and physical servers, allows organizations to reduce attack surface and accelerate security provisioning, while maintaining security policy more easily.

New Cisco TrustSec Deployment Scenarios Validated in Release 6.0

- TrustSec – Application Centric Infrastructure (ACI) integration. ISE 2.1 enables sharing of policy groups between TrustSec and ACI environments so that TrustSec security groups can be reused in ACI policies in ACI-enabled data centers and ACI EndPoint Groups can be reused in TrustSec policies elsewhere in an enterprise network or cloud environment. Groups and group membership information is automatically shared between ACI and TrustSec environments to enable consistent security policies to be used across the Enterprise network.
- ISE 2.1 Easy Connect with TrustSec. Easy Connect enables the authorization of users from a Windows based endpoint without requiring the use of 802.1X being required on the endpoint. Cisco ISE collects user authentication information from the Active Directory (AD) Domain Controller. With Easy Connect, Cisco ISE can issue a CoA (change of authorization) to the network access device (NAD) after the user is authenticated by Active Directory to classify the user's endpoint with an SGT. Authenticated users are then shown in the Cisco ISE live sessions view, and can be queried from the session directory. SXP functions on ISE can also propagate the SGT information to other SXP peers and share the SGT information over pxGrid.
- ISE 2.1 TrustSec Staging Matrix Enhancements. A Staging Matrix feature can be used to roll out new policy changes in a phased manner. This feature includes an approval workflow, where the staging policy cannot be deployed until it is approved. After approval, the staging matrix can be deployed on a limited set of devices. This is useful for evaluating the policy before full deployment. The staging matrix can be edited, if required. The deployment can continue on to the next set of devices or to all devices. Once the staging matrix is fully deployed, the staging matrix policies can be adopted as the new production matrix.
- ISE 2.1 TrustSec Matrix import/export enhancements. Cisco ISE allows the admin to import and export the TrustSec policies in CSV format. With ISE 2.1, empty cells (which do not have any SGACL configured) can now be included in the exported file. When this option is enabled, the whole matrix is exported and the empty cells are marked with the "Empty" keyword in the SGACL column. While importing the egress policy, the admin can now overwrite the existing policy with the one that is imported. If empty cells are included in the imported file, the existing policy in the corresponding matrix cells will be deleted.
- Cisco IE 4000 and IE5000 support Inline Tagging and SGACL enforcement. 1Gig Interfaces support inline tagging on the IE 4000 and IE 5000 with IOS 15.2(5)E. With SGACL enforcement, policy can be static

(through CLI) and/or dynamic policy (through ISE).

- Path Selection based on SGT for ASR1000, CSR1000v, ISR4000, running either IOS-XE 3.17S or IOS-XE Denali 16.3, and ASA running 9.6.1. The ability to make routing decisions based upon Security Group Tags enhances security analysis and delivers operational efficiencies in a number of ways. When hosts are added to a suspicious group, a different forwarding path can now be applied, allowing traffic to be routed via centralized security inspection or centralized packet capture for analysis. Policy routing based upon the SGT can also enable some organizations to more easily share infrastructure and services, delivering cost and efficiency benefits.
- Catalyst 3850/3650 SGACL Logging: For ease of deployment, these SGACL fields are logged in the local logs and the remote syslog server: Source IP address, Destination IP address, Source Port, Destination port, Protocol information, Source Security Group Tag (SGT), Destination Security Group Tag (SGT), Security Group ACL Name, and Security Group ACL Action (permit/deny). This is supported on IOS XE Denali 16.3.1.
- Catalyst 3850/3650 SGACL Monitor Mode. Monitor Mode gives the administrator visibility into who and what is connecting to the network. It ensures all devices are authenticating correctly without impacting connectivity. Policy can be evaluated before it is actively applied. This is supported on IOS XE Denali 16.3.1.
- SGACL Enforcement on ISR: 4431 & 4451, ASR: 1004, 1006, 1013, 1006-X, 1009-X in IOS XE Denali 16.3.1. Updated policy is downloaded to the router when the SGACL policy is modified on ISE and a Change of Authorization (CoA) is pushed to the router.
- FirePOWER 7000 and 8000 Series propagate SGT. Firepower 6.0.1, and FireSIGHT 5.4.0.6 and 5.4.1.5 support the propagation of SGT tagged traffic through IPS appliances (Resolution of CSCze94478).
- With the support of Subnet to SGT mapping in Nexus 7000 NX-OS 7.3, 0.0.0.0/ can be mapped to a SGT. In extranet use-cases this can be used to allow traffic to be classified from an unknown network, for example the Internet or a business partner network connection

Summary of current Cisco TrustSec Features Validated in 6.0

In addition to validating new functionality, validation of existing functionality is performed. Functionality includes

- dynamic and static classification;
- propagation via SXP, or inline tagging over Ethernet or VPN;
- enforcement via SGACL, SGFW;
- HA operations;
- unknown SGT support;
- device management with NDAC, Environment data and policy download
- monitoring and troubleshooting.

These new platforms were tested in this release:

- Catalyst 3850-XS Series
- Cisco IE2000U Series
- Cisco IE5000 Series

Product Components and Features

Table 1 summarizes the platforms and features that are validated in Cisco TrustSec testing. The list is also available at: cisco.com/go/TrustSec. It is current with the TrustSec 6.0 validation program.
Dynamic classification includes IEEE 802.1X, MAC Authentication Bypass (MAB), and Web Authentication (Web Auth). IP to SGT, VLAN to SGT, subnet to SGT, port profile to SGT, L2IF to SGT, and L3IF to SGT use the static classification method. Solution-level validated versions may not always represent the latest available platform version and feature set. For latest platform firmware version and feature set, refer to product release notes.

Cisco ONE for Access is a simple and economical solution for deploying branch and campus switches and wireless access points. It offers an uncompromised user experience in a highly secure and feature-rich access infrastructure and simplifies the licensing requirements for TrustSec deployment.

Table 1. Cisco TrustSec Platform Support Matrix

System Component	Platform	License	Solution-Level Validated Version	Minimum version for all features	Security Group Tag (SGT) Classification	SGT Exchange Protocol (SXP) Support and Version	Inline SGT Tagging	SGT Enforcement
Cisco Identity Services Engine	Cisco ISE 3515, 3595, 3415, and 3495 Appliance & VMware	Base	Cisco ISE 2.1, 2.0, ISE 1.4	Cisco ISE 2.0	Dynamic, IP to SGT	Speaker, Listener V4	–	–
Cisco Catalyst® 2000 Series	Cisco Catalyst 2960-Plus Series Switches	LAN Base K9	-	Cisco IOS 15.2(2)E3	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT	Speaker V4	No	No
	Cisco Catalyst 2960-C Series	LAN Base K9	-	Cisco IOS 15.2(2)E3	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT	Speaker V4	No	No
	Cisco Catalyst 2960-CX Series	LAN Base K9	-	Cisco IOS 15.2(3)E	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT	Speaker V4	No	No
	Cisco Catalyst 2960-S and 2960-SF Series	LAN Base K9	Cisco IOS 15.2(2)E	Cisco IOS 15.2(2)E3	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT	Speaker V4	No	No
	Cisco Catalyst 2960-X and 2960-XR Series	LAN Base K9	Cisco IOS 15.2(2)E	Cisco IOS 15.2(2)E3	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT	Speaker V4	No	No
Cisco Catalyst 3000 Series	Cisco Catalyst 3560-E and 3750-E Series	IP Base K9	Cisco IOS 15.0(2)SE5	Cisco IOS 15.0(2)SE5	Dynamic, IP to SGT, VLAN to SGT	Speaker, Listener V2	No	No
	Cisco Catalyst 3560-C/CG Series	IP Base K9	Cisco IOS 15.0(1)SE2	Cisco IOS 15.2(2)E	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT	Speaker, Listener V4	No	No
	Cisco Catalyst 3560-CX Series	IP Base K9	Cisco IOS 15.2(3)E	Cisco IOS 15.2(3)E	Dynamic, IP to SGT (v4, v6), VLAN to SGT, Subnet to SGT	Speaker, Listener V4	No	No
	Cisco Catalyst 3560-X and 3750-X Series	IP Base K9	Cisco IOS 15.2(2)E3	Cisco IOS 15.2(2)E1	Dynamic, IP to SGT (prefix must be 32), VLAN to SGT, Port to SGT (only on switch to switch links)	Speaker V4	SGT over Ethernet; SGT over MACsec (with C3KX-SM- 10G uplink)	SGACL (maximum of 8 VLANs on a VLAN-trunk link)
	Cisco Catalyst 3650 and 3850 Series	IP Base K9 & above Cisco ONE Foundation & above	Cisco IOS XE 3.6.4	Cisco IOS XE 3.6.0SE	Dynamic, IP to SGT (v4,v6), VLAN to SGT, Port to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4	SGT over Ethernet; SGT over MACsec (3650 requires 3.7.1)	SGACL
	Cisco Catalyst 3650 and 3850 Series	IP Base K9 & above Cisco ONE Foundation & above	Cisco IOS XE Denali 16.3.1	Cisco IOS XE Denali 16.3.1	Dynamic, IP to SGT (v4,v6), VLAN to SGT, Port to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4	SGT over Ethernet; SGT over MACsec (3650 requires 3.7.1)	SGACL
	Cisco Catalyst 3850-XS Series	IP Base K9 & above Cisco ONE Foundation & above	Cisco IOS XE 3.7.4	Cisco IOS XE 3.7.4	Dynamic, IP to SGT, VLAN to SGT, Port to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4	SGT over Ethernet;**** SGT over MACsec	SGACL

System Component	Platform	License	Solution-Level Validated Version	Minimum version for all features	Security Group Tag (SGT) Classification	SGT Exchange Protocol (SXP) Support and Version	Inline SGT Tagging	SGT Enforcement *Services*
Cisco Catalyst 4500 Series	Cisco Catalyst 4500 E-Series Supervisor Engine 6-E and 6L-E ; Cisco Catalyst 4948 Series	IP Base K9	Cisco IOS 15.1(1)SG	Cisco IOS 15.1(1)SG	Dynamic, IP to SGT	Speaker, Listener V4	No	No
	Cisco Catalyst 4500 E-Series Supervisor Engine 7-E and 7L-E	IP Base K9 & above Cisco ONE Foundation & above	Cisco IOS XE 3.5.1E	Cisco IOS XE 3.5.1E	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT, L3IF to SGT, Port to SGT	Speaker, Listener V4	SGT over Ethernet; SGT over MACsec (See footnote for supported line cards)	SGACL
	Cisco Catalyst 4500 E-Series Supervisor Engine 8-E and 8L-E	IP Base K9 & above Cisco ONE Foundation & above	Cisco IOS XE 3.6.3E	Cisco IOS XE 3.6.0E	Dynamic, IP to SGT (v4, v6), VLAN to SGT, Port to SGT, Subnet to SGT (Src & Dst), L3IF to SGT	Speaker, Listener V4	SGT over Ethernet; SGT over MACsec (See footnote for supported line cards)	SGACL
	Cisco Catalyst 4500-X Series	IP Base K9 & above Cisco ONE Foundation & above	Cisco IOS XE 3.6.3	Cisco IOS XE 3.5.1E	Dynamic, IP to SGT (v4,v6), VLAN to SGT, Port to SGT, Subnet to SGT (Src & Dst), L3IF to SGT	Speaker, Listener V4	SGT over Ethernet; SGT over MACsec	SGACL
Cisco Catalyst 6500 Series	Cisco Catalyst 6500 Series Supervisor Engine 32 and 720	IP Base K9	Cisco IOS 12.2(33)SXJ2	Cisco IOS 15.1(2)SY1	Dynamic, IP to SGT	Speaker, Listener V4	No	No
	Cisco Catalyst 6500 Series Supervisor Engine 2T Cisco Catalyst 6807-XL	IP Base K9	Cisco IOS 15.2(1)SY0a	Cisco IOS 15.2(1)SY0a	Dynamic, IP to SGT (v4, v6), VLAN to SGT, Port to SGT, Subnet to SGT (v4,v6), L3IF-to- SGT (v4,v6)	Speaker, Listener V4 (IPv4, IPv6)	SGT over Ethernet & SGT over MACsec supported on: WS-X69xx modules, C6800 32P10G/G-XL, C6800-16P10G/G-XL, C6800-8P10G/G-XL	SGACL (IPv4, IPv6) *SGT Caching*
	Cisco Catalyst 6880-X, 6840-X, and 6800ia	IP Base K9 & above Cisco ONE Foundation & above	Cisco IOS 15.2(1)SY0a, 15.2(3a)E	Cisco IOS 15.2(1)SY0a	Dynamic, IP to SGT (v4, v6), VLAN to SGT, Port to SGT, Subnet to SGT (v4,v6), L3IF-to-SGT (v4,v6)	Speaker, Listener V4 (IPv4, IPv6)	SGT over Ethernet; SGT over MACsec	SGACL (IPv4, IPv6) *SGT Caching*
Cisco Con-nected Grid Routers and Switches	Cisco 2010 Connected Grid Routers	-	Cisco IOS 15.5(2)T	Cisco IOS 15.4(1)T	Dynamic, IP to SGT, VLAN to SGT	Speaker, Listener V4	SGT over GETVPN or IPsec VPN	SG Firewall
	Cisco 2500 Series Connected Grid Switches	-	Cisco IOS 15.2(3)EA	Cisco IOS 15.0(2)EK1	Dynamic, IP to SGT, VLAN to SGT, Port to SGT, Subnet to SGT	Speaker, Listener V3	No	No
Cisco Industrial Ethernet Switches	Cisco IE 2000 & 2000U Series Cisco IE 3000 Series	LAN Base	Cisco IOS 15.2(3)EA IE2000U: IOS 15.2(3)E3	Cisco IOS 15.2(1)EY IE2000U: IOS 15.2(3)E3	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT	Speaker, Listener V4	No	No
	Cisco IE 4000 Series	LAN Base; IP Services for SGToE & SGACL	Cisco IOS 15.2(4)EA, 15.2(5)E	Cisco IOS 15.2(5)EA	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT	Speaker, Listener V4	SGT over Ethernet	SGACL

System Component	Platform	License	Solution-Level Validated Version	Minimum version for all features	Security Group Tag (SGT) Classification	SGT Exchange Protocol (SXP) Support and Version	Inline SGT Tagging	SGT Enforcement
Cisco Industrial Ethernet Switches	Cisco IE 5000 Series	LAN Base; IP Services for SGToE & SGACL	Cisco IOS 15.2(2)EB1, 15.2(5)E	Cisco IOS 15.2(5)EA	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT	Speaker, Listener V4	SGT over Ethernet on1G interfaces only	SGACL
Cisco Wireless Con-trollers	Cisco 5500 Series (5508,5520) Cisco 2500 Series (2504)	-	Cisco AireOS 8.1	AireOS 7.6.130.0	Dynamic	Speaker V2	No	No
	Cisco Wireless Services Module 2 (WiSM2)	-	Cisco AireOS 8.1	AireOS 7.6.130.0	Dynamic	Speaker V2	No	No
	Cisco 5760 Wireless Controller Series	IP Base K9	Cisco IOS XE 3.7.1E	Cisco IOS XE 3.3.1SE	Dynamic, IP to SGT, VLAN to SGT, Port to SGT, Subnet to SGT	Speaker, Listener V4	SGT over Ethernet	SGACL
	Cisco 8500 Wireless Controller Series (8540,8510)	-	Cisco AireOS 8.1	Cisco AireOS 8.1	Dynamic	Speaker V2	No	No
Cisco Nexus® 7000 Series	Cisco Nexus 7000 M-Series and F-Series*** modules Cisco Nexus 7700 F-Series*** modules	Base License NX-OS 6.1 and later	Cisco NX-OS 7.3(0)D1(1), 7.2(0)D1(1)	Cisco NX-OS 7.3(0)D1(1)	IP to SGT[1], Port Profile to SGT, VLAN to SGT[2], Port to SGT[2] Subnet to SGT[5] [1]:FabricPath support requires 6.2(10) or later [2] VPC/VPC+ support requires 7.2(0)D1(1) or later [5] Subnet to SGT	Speaker, Listener V3	SGT over Ethernet[3]; SGT over MACsec[4] [3]: F3 interfaces (L2 or L3) require 802.1Q or FabricPath [4]: M & F2e (Copper-) all ports; F2e (SFP) & F3 (10G)- last 8 ports; All others- no support	SGACL
Cisco Nexus 5000, 6000 Series	Cisco Nexus 6000/5600 Series	-	Cisco NX-OS 7.1(0)N1(1a)	Cisco NX-OS 7.0(1)N1(1)	Port to SGT	Speaker V1	SGT over Ethernet	SGACL
	Cisco Nexus 5548P, 5548UP, and 5596UP (Note: No support for 5010 or 5020)	-	Cisco NX-OS 7.0(5)N1(1)	Cisco NX-OS 6.0(2)N2(6)	Port to SGT	Speaker V1 [1] [1]: FabricPath	SGT over Ethernet	SGACL
Cisco Nexus 1000 Series	Cisco Nexus 1000V for VMware vSphere	Ad-vanced license for SGT/ SGACL support	Cisco NX-OS 5.2(1)SV3(1.3)	Cisco NX-OS 5.2(1)SV3 (1.1)	IP to SGT, Port Profile to SGT	Speaker, Listener v1	SGT over Ethernet	SGACL

System Component	Platform	License	Solution-Level Validated Version	Minimum version for all features	Security Group Tag (SGT) Classification	SGT Exchange Protocol (SXP) Support and Version	Inline SGT Tagging	SGT Enforcement
Cisco Integrated Services Router (ISR)	Cisco 890, 1900, 2900, 3900 Series	IP Services/K9 for classify/ propagate; SEC/K9 for enforce-ment	890: Cisco IOS 15.4(1)T1 *IOS 15.4(3)M* 1900/2900/3900:Cisco IOS 15.5(1)20T *IOS 15.4(3)M*	890: Cisco IOS 15.4(3)M 1900/2900/3900: Cisco IOS 15.6(1)T	IP to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4	SGT over Ethernet (no support on ISR G2-Cisco 800 Series), SGT over GETVPN, DMVPN, or IPsec VPN	SG Firewall (890:No services) *SGT based PBR* *SGT Caching* *SGT based QoS*
	Cisco 4000 Series (ISR 4451-X validated)	IP Services/K9 for classify/ propagate; SEC/K9 for enforce-ment	Cisco IOS XE 3.15.01S	Cisco IOS XE 3.17.0S	IP to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4	SGT over Ethernet, SGT over GETVPN, DMVPN, or IPsec VPN,	SG Firewall *SGT based PBR* *SGT Caching* *SGT based QoS*
	Cisco 4000 Series ISR 4431, and 4451-X	IP Services/K9 for classify/ propa-gate; SEC/K9 for enforce-ment	Cisco IOS XE Denali 16.3.1	Cisco IOS XE Denali 16.3.1	IP to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4	SGT over Ethernet, SGT over GETVPN, DMVPN, or IPsec VPN	SGACL SG Firewall *SGT based PBR* *SGT Caching* *SGT based QoS*
	Cisco SM-X Layer 2/3 EtherSwitch Module	IP Services/K9 for classify/ propagate; SEC/K9 for enforce-ment	Cisco IOS 15.5.2T	Cisco IOS 15.2(2)E	Dynamic, IP to SGT, VLAN to SGT	Speaker, Listener V4	SGT over Ethernet; SGT over MACsec	SGACL
Cisco Cloud Services Router	Cisco Cloud Services Router 1000V Series (CSR)	IP Services/K9 for classify/ propagate; SEC/K9 for enforce-ment	Cisco IOS XE 3.15.01S	Cisco IOS XE 3.11.0S	IP to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4	SGT over Ethernet, SGT over IPsec VPN, DMVPN	SG Firewall *SGT based PBR* *SGT Caching*
Cisco Aggrega-tion Services Router (ASR)	Cisco 1000 Series Router Processor 1 or 2 (RP1, RP2); ASR 1001, 1002,1004, 1006 and 1013 with ESP (10,20, 40, 100, 200) and SIP (10/40)	IP Services/K9 for classify/ propagate; SEC/K9 for enforce-ment	Cisco IOS XE 3.15.0S	Cisco IOS 3.17.0S	IP to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4	SGT over Ethernet, SGT over GETVPN, IPsec VPN, or DMVPN	SG Firewall *SGT based PBR (1000 RP2)* *SGT based QoS* *SGT Caching*
	Cisco ASR 1001-X and 1002-X	IP Services /K9 for classify/ propagate; SEC/K9 for enforcement	Cisco IOS XE 3.13.0S	Cisco IOS XE 3.17.0S	IP to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4	SGT over Ethernet, SGT over GETVPN, IPsec VPN, DMVPN	SG Firewall SGT based PBR SGT based QoS SGT Caching
	Cisco ASR 1004, 1006, 1013, 1006-X, and 1009-X	IP Services/K9 for classify/ propagate; SEC/K9 for enforce-ment	Cisco IOS XE Denali 16.3.1	Cisco IOS XE Denali 16.3.1	IP to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4	SGT over Ethernet, SGT over GETVPN, DMVPN, or IPsec VPN	SGACL SG Firewall *SGT based PBR* *SGT Caching* *SGT based QoS*

System Component	Platform	License	Solution-Level Validated Version	Minimum version for all features	Security Group Tag (SGT) Classification	SGT Exchange Protocol (SXP) Support and Version	Inline SGT Tagging	SGT Enforcement Services
Cisco Adaptive Security Appliance (ASA)	Cisco ASA 5510, 5520, 5540, 5550, 5580	-	Cisco ASA 9.0.1, ASDM 7.1.6	Cisco ASA 9.0.1, ASDM 7.1.6		Speaker, Listener v2		SG Firewall
	Cisco ASA 5505**, 5512, 5515, 5525, 5545, 5555, 5585	-	ASA 9.3.1, ASDM 7.3.1, CSM 4.8	Cisco ASA 9.3.1, ASDM 7.3.1, CSM 4.8	Remote Access VPN (IPSec, SSL-VPN)	Speaker, Listener V2 (IPv4, IPv6)	SGT over Ethernet	SG Firewall (IPv4, IPv6) *SGT based PBR*
	Cisco ASA 5506-X, 5506H-X, 5506W-X, 5508-X, 5516-X	-	Cisco ASA 9.6.1, ASDM 7.6.1	Cisco ASA 9.6.1, ASDM 7.6.1	Remote Access VPN (IPSec, SSL-VPN)	Speaker, Listener V3	SGT over Ethernet	SG Firewall (IPv4, IPv6) *SGT based PBR*
	Cisco ASA 5512-X, 5515-X, 5525-X, 5545-X, 5555-X, 5585-X with FirePower Services	-	Cisco ASA 9.6.1, ASDM 7.6.1	Cisco ASA 9.6.1, ASDM 7.6.1	Remote Access VPN (IPSec, SSL-VPN)	Speaker, Listener V3	SGT over Ethernet	SG Firewall (IPv4, IPv6) *SGT based PBR*
	Cisco ASAv	-	Cisco ASA 9.3.1 ADSM 7.1.6	Cisco ASA 9.6.1 ASDM 7.6.1	Remote Access VPN (IPSec, SSL-VPN)	Speaker, Listener V3	SGT over Ethernet	SG Firewall *SGT based PBR*
Cisco Firepower (FP)	Cisco FP 4100 Cisco FP 9300	Firepower Threat Defense Base	Cisco FXOS 2.0(1) Cisco ASA 9.6.1	Cisco FXOS 2.0(1) Cisco ASA 9.6.1	Remote Access VPN (IPSec, SSL-VPN)	Speaker, Listener V3	SGT over Ethernet	SG Firewall
	Cisco FirePOWER 7000 and 8000 Series	-	Cisco FireSIGHT 5.4.0.6, 5.4.1.5, 6.0.1.1	Cisco FireSIGHT 5.4.0.6, 5.4.1.5, 6.0.1.1	-	-	SGT over Ethernet	-

Notes

Dynamic classification includes IEEE 802.1X, MAC Authentication Bypass (MAB), and Web Authentication (Web Auth).

IP to SGT, VLAN to SGT, subnet to SGT, port profile to SGT, L2IF to SGT, and L3IF to SGT use the static classification method.

Solution-level validated versions may not always represent the latest available platform version and feature set. For latest platform firmware version and feature set, refer to product release notes.

Notes

* Product part numbers of supported line cards for SGT over Ethernet and SGT over MACsec on the Cisco Catalyst 4500 Supervisor Engine 7-E, 7L-E, 8-E, and 8L-E include the following: WS-X4712-SFP+E, WS-X4712-SFP-E, WS-X4748-UPOE+E, WS-X4748-RJ45V+E, WS-X4748-RJ45- E, WS-X4724-SFP-E, WS-X4748-SFP-E, and WS-X4748-12X48U+E.

** Cisco ASA 5505 does not support releases after 9.2.

*** Cisco Nexus 7000 F1-Series modules do not support Cisco TrustSec.

****Use of inline tagging with LACP requires future IOS XE Denali or IOS 3.7 release (CSCva22545)

- With IPv6 support, DGT can be IPv4.

- Cisco vWLC does not support Cisco TrustSec.

- Prior versions of this document listed Cisco Catalyst 3750-X validated version, IOS 12.2(3)E1. It has a TrustSec defect and was deferred.

Product Scalability

Cisco TrustSec® scalability is platform dependent. The tables below provide insight into the SXP maximum number of connections (peers) a platform is able to support along with the maximum number of IP-SGT bindings that can be managed. Table 2 results use a CPU load method, except for newer ASA and Firepower results which use a CPS (connections per second) traffic load with a maximum performance degradation of 5%. The CPS method is considered a better measure for firewalls. Table 2 show switch, wireless, and security products and Table 3 shows router product scalability.

Table 2. Cisco TrustSec Platform Scalability of Switch, Wireless, and Security Products

Platform	Maximum SXP connections	Maximum IP-SGT bindings	Comments
Cisco Catalyst 2960-S Series	1,000	1,000	
Cisco Catalyst 2960-X & 2960-XR Series	1,000	1,000	
Cisco Catalyst 3k Series (non-stack)	1,000	200,000	
Cisco Catalyst 3850 Series / 3650 Series (Stack)	128	12,000	
Cisco Catalyst 4500 Supervisor Engine 6-E and 6L-E	1,000	200,000	
Cisco Catalyst 4500 Supervisor Engine 7-E	1,000	256,000	
Cisco Catalyst 4500 Supervisor Engine 7L-E	1,000	64,000	
Cisco Catalyst 4500 Supervisor Engine 8-E	2,000	200,000	
Cisco Catalyst 4500-X Series	1000	64,000	
Cisco Catalyst 6500 Series Supervisor Engine 2T	2,000	200,000	
Cisco Catalyst 6800 Series	2,000	200,000	
Cisco 5505 Wireless Controller Series	5		
Cisco 5760 Wireless Controller Series	128	12,000	
Cisco Nexus 7000 M1, M2	980	200,000 (7.2, +) 50,000 (pre 7.2)	
Cisco Nexus 7000 F1	980	512	
Cisco Nexus 7000 F2/F2e Supervisor	980	32,000	Recommend 25,000 for planning purposes
Cisco Nexus 7000 F3	980	64,000	Recommend 50,000 for planning purposes
Cisco Nexus 6000, 5600, 5500	4 per VRF	2,000 per SXP connection	Max of 4 VRF
Cisco Nexus 1000v	64	6,000 per VMS	
Cisco ASA 5505	10	250	CPU load method
Cisco ASA 5510	25	1,000	CPU load method
Cisco ASA 5520	50	2,500	CPU load method
Cisco ASA 5540	100	5,000	CPU load method
Cisco ASA 5550	150	75,000	CPU load method
Cisco ASA 5580-20	250	10,000	CPU load method
Cisco ASA 5580-40	500	20,000	CPU load method
Cisco ASA 5585-SSP10	150	18,750	CPU load method
Cisco ASA 5585-SSP20	250	20,000	CPU load method
Cisco ASA 5585-SSP40	500	50,000	CPU load method
Cisco ASA 5506-X	2,000	195,000	CPS method
Cisco ASA 5555-X	2,000	500,000	CPS method
Cisco ASA 5585-SSP60	2,000	500,000	CPS method
FP-4110	2,000	1M	CPS method
FP-9300 SM-36	2,000	1M	CPS method
Cisco ISE 3495	20	100,000	

Table 3. Cisco TrustSec Platform Scalability of Router Products

Platform	Maximum Unidirectional SXP Connections (Speaker only/ Listener only)	Maximum Bidirectional SXP Connections	Maximum IP SGT Bindings
Cisco 890 Series	100		1,000
Cisco 2900, 3900 Series ISRG2	250	125	180,000 with unidirectional SXP connections 125,000 with bidirectional
Cisco 4400 Series ISR	1800	900	135,000
Cisco ASR 1000 Series	1800	900	750,000 (IOS XE 3.15, and later) 180,000 (earlier)
Cisco Cloud Services Router 1000V Series (CSR)	900	450	135,000

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 v6.0a C96-731479-00 11/16