Cisco TrustSec Software-Defined Segmentation Release 6.3 System Bulletin

Introduction

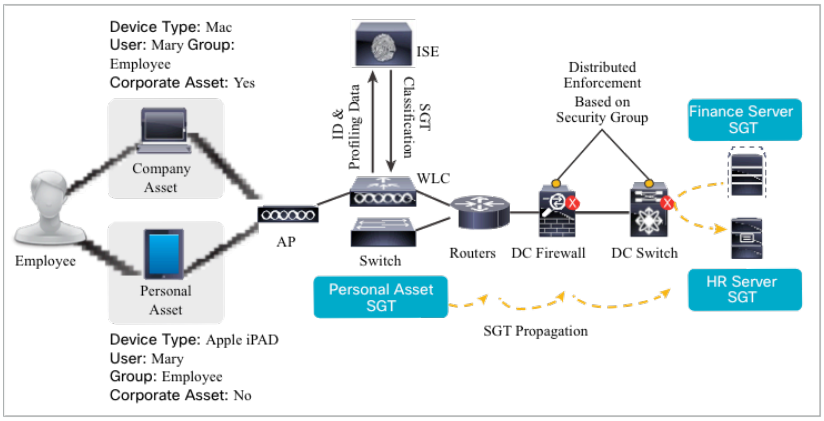
Network segmentation is essential for protecting critical business assets. Cisco TrustSec® Software Defined Segmentation balances the demands for agility and security without the operational complexity and difficulty of deploying into existing environments seen with traditional segmentation. With TrustSec, 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

© 2017 Cisco and/or affiliates. All rights reserved. This document is Cisco Public Information.

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 6.3 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 logical boundaries, such as VLAN or subnet, along with static access control lists.
- Data Center segmentation and micro-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 6.3

- Cisco Active Advisor's TrustSec Readiness Assessment allows users to quickly analyze network TrustSec compatibility. The readiness assessment compares Product ID, Software Version, and License information against the Cisco TrustSec Software-Defined Segmentation Platform and Capability Matrix for Release 6.2 with the 6.3 update to follow. The easy-to-read recommendations are exportable and immediately available at www.ciscoactiveadvisor.com.
- In some designs, it is desirable to centralize SXP advertisements within the data center. An ASR 1000 Series router may be used as the centralized peering point or “SXP Reflector” to which all SXP advertisements are aggregated with a single peering extending from the router to an ASA or the campus. An HA pair of ASR 1006 RP2 was tested to determine the scaling characteristics as an SXP reflector.
- The Nexus 7700 M3 line card NX-OS 8.1(1) includes the new command **no propagate-sgt l2-control** to exempt the SGT tagging of the L2 control plane protocols for an interface. Nexus 7k M3 modules, Catalyst switches, and Cisco routers include the null SGT tag in the L2 control plane protocols. The Nexus F series modules do not handle null SGT in L2 control packets. When the Cisco M3 series module interoperates with the Cisco F3 series module over a Cisco TrustSec-enabled link, this command must be enabled for the M3 series module to ensure that the control packets are accepted by the Cisco F3 series module.
- With NX-OS 8.0(1), SXP contributions are maintained in a new SXP Contributor Database for improved resiliency. The best advertisement for each IP-SGT binding is selected from the possible multiple sources and then stored in the Role-Based Manager Database (RBM). If the best binding source goes down, the next best binding is installed in the RBM.
- The IE 4000 and IE 5000 platforms perform similarly to the Catalyst 3560-X and 3750-X platforms in the reliance on IP Address, MAC Address, and physical port/VLAN of the device, learned via dot1x or MAB or IP Device Tracking (IPDT). These devices cannot use information learned via SXP as the device is not directly attached and so they can’t use SXP information for neither enforcement nor tag propagation. SXP v4 is supported in Speaker mode only.
- With Cisco IOS 3.6.7 on the Catalyst 4500, the TCAM label sharing is optimized. This allows QoS and TrustSec to more efficiently share the TCAM space with reduced likelihood of TCAM exhaustion (resolution of CSCvc88353).
- Some environments require a whitelist approach where only specified access is granted. In these situations, the default permission is set to Deny in the ISE policy matrix. Additional validation of ‘Default Deny’ for unknown tag and known tag combinations was tested with the Cat 3850 - IOS XE 3.6.7 and Cat

© 2017 Cisco and/or affiliates. All rights reserved. This document is Cisco Public Information.

6k – 15.2(1)SY2 receiving the SGACL information from ISE. The results were successful for non-VRF; VRF environments encountered an issue on the Catalyst 3850 (CSCvg69769).

- In some situations, customers experienced Cat6k CPU HOG messages and Watchdog timeouts with SXP v1, v2, and v3 to WLC (CSCvd63786). Cisco IOS Cat 6500 releases 15.2(01)SY05 and 15.4(01)SY01 resolve this issue.

Summary of current Cisco TrustSec Features Validated in 6.3

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
- monitoring and troubleshooting
- HA operations
- device management with NDAC, Environment data and policy download
- unknown SGT support

These new platforms were tested in this release:

- Cisco Catalyst 9300 Series with scale testing
- Cisco Catalyst 9500 Series with scale testing
- Cisco Catalyst 6816-X-LE (6840-X Series)
- Cisco Firepower 2100
- Cisco Firepower Threat Defense Virtual

Product Components and Features

Tables 1 and 2 summarize 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 6.3 validation program.
Table 1 provides cross-platform group-based policy exchange interoperability testing results. Application Centric Infrastructure (ACI) and TrustSec integration enables customers to apply consistent security policy across the enterprise- leveraging user roles and device type together with application context. The validated Open Source Open Daylight SDN use case included Nexus 7k SXPv3, ASA SXPv3, and OpenDaylight SXPv4 (Lithium, Beryllium, or Carbon release) working together in the Data Center.

Table 1. TrustSec Group-Based Policy (GBP) Interoperability

System Component	Platform	Solution-Level Validated Version	Group Information Exchange	Interoperability Platform & Propagation method
Cisco Nexus 9000 Series Switches	Cisco 9000 Series: Spine & Leaf	NX-OS 11.3(2f)	EndPoint Group – Security Group Mappings via TrustSec-ACI policy and data plane exchange	Cisco ISE 2.1, 2.2- ACI API
Cisco Application Policy Infrastructure Controller – Data Center	Cisco APIC-DC	APIC-DC 2.3 Data Plane APIC-DC 1.3(1g) Policy plane;		
Open Daylight SDN controller	ODL SDN	Lithium, Beryllium, Carbon	SGT via SXP v4	Cisco ISE 2.1- SXP v4 Nexus 7000 7.3- SXP v3 ASA 9.6.1- SXP v3

In Table 2 Cisco Platform Support Matrix, Dynamic classification includes IEEE 802.1X, MAC Authentication Bypass (MAB), Web Authentication (Web Auth), and Easy Connect. 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. 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.
Solution-level validated versions listed in Table 2 may not always represent the latest available platform version and feature set. Releases may encounter issues in other subsystems and be deferred. For latest

© 2017 Cisco and/or affiliates. All rights reserved. This document is Cisco Public Information.

platform firmware version and feature set, refer to product release notes.

Table 3. Cisco TrustSec Platform Support Matrix - Classic

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	ISE 3515, 3595, 3415, and 3495 Appliance & Vmware	Base Plus for pxGrid	Cisco ISE 2.3P1, 2.2, 2.1, 2.0, 1.4	Cisco ISE 2.2	Dynamic, IP to SGT, Subnet to SGT	Speaker, Listener V4 pxGrid	–	–
Cisco Catalyst® 2000 Series	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
	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
	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
	Catalyst 2960-S and 2960-SF Series	LAN Base K9	Cisco IOS 15.0(2)SE[Note1] 15.2(2)E	Cisco IOS 15.2(2)E3	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT	Speaker V4 [Note1]	No	No
	Catalyst 2960-X 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
	Catalyst 2960-XR Series	IP Lite 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	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
	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
	Catalyst 3560-CX Series	IP Base K9	Cisco IOS 15.2(3)E	Cisco IOS 15.2(4)E	Dynamic, IP to SGT (v4, v6), VLAN to SGT, Subnet to SGT	Speaker, Listener V4	No	SGACL
	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); SGT over VXLAN	SGACL (maximum of 8 VLANs on a VLAN-trunk link)
	Catalyst 3650 and 3850 Series	IP Base K9 & above Cisco ONE Foundation & above	Cisco IOS XE 3.6.7, 3.7.1E	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 *SGT Netflow v9*
	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; SGT over VXLAN	SGACL
	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 [Note5]; SGT over MACsec	SGACL

© 2017 Cisco and/or affiliates. All rights reserved. This document is Cisco Public Information.

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	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
	Catalyst 4500 E-Series Supervisor Engine 7-E and 7L-E	IP Base K9 & above Cisco ONE Foundation & above	Cisco IOS XE 3.7.1E	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 note 2 for supported line cards)	SGACL *SGT Netflow v9*
	Catalyst 4500 E-Series Supervisor Engine 8-E and 8L-E	IP Base K9 & above Cisco ONE Foundation & above	Cisco IOS XE 3.7.1E	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 note 2 for supported line cards)	SGACL *SGT Netflow v9*
	Catalyst 4500-X Series	IP Base K9 & above Cisco ONE Foundation & above	Cisco IOS XE 3.6.6	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	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
	Catalyst 6500 Series Supervisor Engine 2T & Supervisor 6T Catalyst 6807-XL	2T: IP Base K9 6T: IP Services K9	Cisco IOS 15.2(1)SY05 15.2(1)SY0a Sup 6T Cisco IOS 15.4(1)SY1	Cisco IOS 15.2(1)SY0a Sup 6T Cisco IOS 15.4(1)SY1	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* *SGT Netflow v9*
	Catalyst 6880-X, 6840-X (incl 6816-X-LE), and 6800ia	IP Base K9 & above Cisco ONE Foundation & above	Cisco IOS 15.2(2)SY2, 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* *SGT Netflow v9*
Cisco Catalyst 9300 Series	Catalyst 9300 Series	DNA Advantage	Cisco IOS XE Everest 16.6.2 SMU	Cisco IOS XE Everest 16.6.2 SMU (Note 10)	Dynamic, IP to SGT, VLAN to SGT, Port to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4	SGT over Ethernet SGT over VXLAN	SGACL
Cisco Catalyst 9500 Series	Catalyst 9500 Series	DNA Advantage	Cisco IOS XE Everest 16.6.2 SMU	Cisco IOS XE Everest 16.6.2 SMU (Note 10)	Dynamic, IP to SGT, VLAN to SGT, Port to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4	SGT over Ethernet SGT over VXLAN	SGACL *SGT Caching* *SGT Netflow v9*

© 2017 Cisco and/or affiliates. All rights reserved. This document is Cisco Public Information.

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 Connected Grid Routers and Switches	CGR 2010 Series	-	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, SGT over IPsec VPN	SG Firewall
	CGS 2500 Series	-	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	IE 2000 & 2000U Series 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
	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)E	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT	Speaker V4	SGT over Ethernet	SGACL
	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)E	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT	Speaker V4	SGT over Ethernet on1G interfaces only	SGACL
Cisco Access Points	1700, 2700, 3700, AP Series (Wave 1)	-	Cisco AireOS 8.4	Cisco AireOS 8.4	Dynamic	Speaker, Listener V4[Note6]	SGT over Ethernet[Note6]	SGACL
	1815, 1830, 1850, 2800, 3800 AP Series (Wave 2)	-	Cisco AireOS 8.4	Cisco AireOS 8.4	Dynamic	Speaker, Listener V4[Note6]	SGT over Ethernet[Note6]	SGACL
Cisco Wireless Controllers	5500 Series (5508,5520) 2500 Series (2504)	-	Cisco AireOS 8.3.102.0, 7.6.130.0	Cisco AireOS 7.6.130.0	Dynamic	Speaker V2	No	No
	Wireless Services Module 2 (WiSM2)	-	Cisco AireOS 8.3.102.0, 7.6.130.0	Cisco AireOS 7.6.130.0	Dynamic	Speaker V2	No	No
	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
	Flex 7500 Series Wireless Controller	-	Cisco AireOS 8.3.102.0, 7.6.130.0	Cisco AireOS 8.3	Dynamic	Speaker V2	No	No
	8500 Series Wireless Controller (8540,8510)	-	Cisco AireOS 8.3.102.0	Cisco AireOS 8.1	Dynamic	Speaker V2	No	No
	8540 Series Wireless Controller 5520 Series Wireless Controller		Cisco AireOS 8.4	Cisco AireOS 8.4	Dynamic	Speaker v2	SGT over Ethernet	No

© 2017 Cisco and/or affiliates. All rights reserved. This document is Cisco Public Information.

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 Nexus® 7000 Series	Nexus 7000 with M3-Series modules	Base License NX-OS 6.1 and later	Cisco NX-OS 8.1(1), 8.0(1) 7.3(0)D1(1), 7.2(0)D1(1)	Cisco NX-OS 8.0(1)	IP to SGT[1], Port Profile to SGT, VLAN to SGT[2], Port to SGT[2] Subnet to SGT[5]	Speaker, Listener V4	SGT over Ethernet[5]; SGT over MACsec [5]: F3 interoperability requires M3 'no propagate-sgt l2 control' command	SGACL
	Nexus 7000 with M2-Series modules	Base License NX-OS 6.1 and later	Cisco NX-OS 8.1(1), 8.0(1) 7.3(0)D1(1), 7.2(0)D1(1)	Cisco NX-OS 8.0(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 requires 7.3(0)D1(1) or later	Speaker, Listener V4	SGT over Ethernet[5]; SGT over MACsec [5]: M2 cannot link to F3 module.	SGACL
	Nexus 7700 F-Series[Note4] modules F3 modules do not support SGT tagging with other Cisco products unless these products support the SGT tagging exemption feature for Layer 2 protocols. M3 series support this by enabling 'no propagate-sgt l2-control' command.	Base License NX-OS 6.1 and later	Cisco NX-OS 8.1(1), 8.0(1) 7.3(0)D1(1), 7.2(0)D1(1)	Cisco NX-OS 8.0(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 requires 7.3(0)D1(1) or later	Speaker, Listener V4	SGT over Ethernet[35]; SGT over MACsec[4] [3]: F3 interfaces (L2 or L3) require 802.1Q or FabricPath [4]: F2e (Copper) all ports; F2e (SFP) & F3 (10G)- last 8 ports; All others- no support [5]: Not supported between F3 and either M2 or F2e	SGACL
Cisco Nexus 1000 Series	Nexus 1000V for VMware vSphere	Ad-vanced license for SGToE/ 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[Note9]	SGACL

© 2017 Cisco and/or affiliates. All rights reserved. This document is Cisco Public Information.

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 Nexus 5000, 6000 Series	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
	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 Integrated Services Router (ISR)	890, 1900, 2900, 3900 Series	IP Base/K9 for classify/ propagate; Security/K9 for SG FW enforcement	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*
	4000 Series (ISR 4451-X validated)	IP Base/K9 for classify/ propagate; Security/K9 for SG FW enforcement	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* *SGT Netflow v9*
	4000 Series ISR 4431, 4451-X, 4321, 4331, 4351	IP Base/K9 for classify/ propagate, SGACL; Security/K9 for SG FW enforcement	Cisco IOS XE Denali 16.3.2, Everest 16.4.1	Cisco IOS XE Denali 16.3.2	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*
	ISRv	IP Base/K9 for classify/ propagate, SGACL	Cisco IOS XE Denali 16.3.2	Cisco IOS XE Denali 16.3.2	IP to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4	SGT over Ethernet, SGT over IPsec VPN, DMVPN	SGACL
	SM-X Layer 2/3 EtherSwitch Module	IP Services/K9	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	Cloud Services Router 1000V Series (CSR)	IP Base/K9 for classify/ propagate; Security/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* *SGT Netflow v9*
	Cloud Services Router 1000V Series (CSR)	IP Base/K9 for classify/ propagate, SGACL;	Cisco IOS XE Denali 16.3.2, Everest 16.4.1	Cisco IOS XE Denali 16.3.2	IP to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4	SGT over Ethernet, SGT over IPsec VPN, DMVPN	SGACL

© 2017 Cisco and/or affiliates. All rights reserved. This document is Cisco Public Information.

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 Aggreg-ation Services Router (ASR)	ASR 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 Base/K9 for classify/ propagate; Security/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* *SGT Netflow v9*
	ASR 1001-X and 1002-X	IP Base/K9 for classify/ propagate; Security/K9 for enforce-ment	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 *SGT Netflow v9*
	ASR 1004, 1006, 1013, 1001-X, 1002-X,1002-HX, 1006-X, and 1009-X	IP Base/K9 for classify/ propagate, SGACL; Security/K9 for SGFW enforce-ment	Cisco IOS XE Denali 16.3.2, Everest 16.4.1	Cisco IOS XE Denali 16.3.2	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 Adaptive Security Appliance	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
	ASA 5505[Note3], 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*
	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*
	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*
	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*

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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 Firepower (FP)	Cisco Firepower 2100 FP 4100 FP 9300 Cisco Firepower Threat Defense Firepower 4100 & 9300	Firepower Threat Defense Base - Firepower Threat Defense Base	Cisco Firepower System 6.2.1 Cisco FXOS 2.0.1.37 Cisco ASA 9.6.1 Cisco Firepower System 6.1.0	Cisco Firepower System 6.2.1 Cisco FXOS 2.0.1.37 Cisco ASA 9.6.1 Cisco Firepower System 6.1.0	- Remote Access VPN (IPsec, SSL-VPN) -	pxGrid Speaker, Listener V3 pxGrid	SGT over Ethernet SGT over Ethernet SGT over Ethernet	SG Firewall SG Firewall SG Firewall
	FirePOWER 7000 and 8000 Series	Threat & Apps (TA)	Cisco FireSIGHT 5.4.0.6, 5.4.1.5, 6.0.1.1, 6.2	Cisco FireSIGHT 5.4.0.6, 5.4.1.5, 6.0.1.1	-	-	SGT over Ethernet	-
	FTDv	Threat & Apps (TA)	Cisco Firepower System 6.2.0.2	Cisco Firepower System 6.2.0.2	-	pxGrid	SGT over Ethernet	SG Firewall
Cisco Industrial Security Appliance 3000	ISA 3000 Series	-	Cisco ASA 9.6.1	Cisco ASA 9.6.1	Remote Access VPN (IPsec, SSL-VPN)	Speaker, Listener V3	SGT over Ethernet	SG Firewall (IPv4, IPv6) ——— *SGT based PBR*

Notes

1: Catalyst 2960 S/SF Product management recommends 15.0(2)SE which supports SXP v2.
2: 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.
3: Cisco ASA 5505 does not support releases after 9.2.
4: Cisco Nexus 7000 F1-Series modules do not support Cisco TrustSec.
5: Use of inline tagging with LACP requires future IOS XE Denali or IOS 3.7 release (CSCva22545)
6: For SXP support, AP must run in FlexConnect Mode
7: With IPv6 support, DGT can be IPv4.
8: Prior versions of this document listed Cisco Catalyst 3750-X validated version, IOS 12.2(3)E1, and WLC AireOS 8.1. These releases have been deferred.
9: When TrustSec inline tagging (SGToE) is enabled with the VIC 12xx and VIC 13xx, packet processing is handled at the processor level which will attribute to lower network I/O performance. An alternative solution is to use Intel adaptors.
10: IOS XE Everest 16.6.2 SMU is required for ISE BYOD, Guest, and Posture features. See ISE Compatibility Matrix: https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-device-support-tables-list.html

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 3 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

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

method is considered a better measure for firewalls. Table 3 show switch, wireless, and security products and Table 4 shows router product scalability. Table 5 lists select platform maximum number of supported SGACLs.

Table 3. Cisco TrustSec Platform Scalability of Switch, Wireless, and Security Products

Platform	Maximum SXP connections	Maximum IP-SGT bindings	Comments
Catalyst 2960-S Series	1,000	1,000	
Catalyst 2960-X & 2960-XR Series	1,000	1,000	
Catalyst 3750-X & 3560-X Series (non-stack)	1,000 (500 Bidirectional)	200,000	
Catalyst 3650 & 3850 Series / (Stack)	~~128~~ 256 (128 Bidirectional)	12,000	
Catalyst 4500 Supervisor Engine 6-E	1,000 (900 Bidirectional)	100,000 routed/L3 2,000 Switched/L2	
Catalyst 4500 Supervisor Engine 7-E, 8-E	~~1,000~~ 1,800 (900 Bidirectional)	128,000 routed/L3 2,000 Switched/L2	
Catalyst 4500 Supervisor Engine 7L-E, 8L-E	~~1,000~~ 1,800 (900 Bidirectional)	32,000 routed/L3 2,000 Switched/L2	
Catalyst 4500-X Series	1000	32,000 routed/L3 2,000 Switched/L2	
Catalyst 6500 Series Supervisor Engine 720	2000 (1,000 Bidirectional)	200,000	
Catalyst 6500 Series Supervisor Engine 2T and 6T	2000 (1,000 Bidirectional)	256,000	
Catalyst 6800 Series	2,000 (1,000 Bidirectional)	256,000	
Catalyst 9300 Series	256 (130 Bidirectional)	10,000	
Catalyst 9500 Series	256	10,000	
1700, 2700, 2800, 3700, AP Series (Wave 1) 1815, 1830, 1850, 2800, 3800 AP Series (Wave 2)	5	50	
WLC 8540, 8510 Series		64,000	
WLC 5520		20,000	
WLC 5508		7,000	
WLC 5505 Series	5	2,500	
WLC 5760 Series	128	12,000	
WISM2		20,000	
Nexus 7000 M1 XL, M2, M3	980 (450 Bidirectional)	200,000 (7.2, +) 50,000 (pre 7.2)	
Nexus 7000 M1 (non-XL)	980 (450 Bidirectional)	128,000	
Nexus 7000 F2, F2e	980 (450 Bidirectional)	32,000	Recommend 25,000 for planning purposes
Nexus 7000 F3	980	64,000	Recommend 50,000 for planning purposes
Nexus 6000, 5600, 5500	4 per VRF	2,000 per SXP connection	Max of 4 VRF
Nexus 1000v	64 (32* Bidirectional connections)	6,000 per VSM	*: Bidirectional max not tested; SGACL & IP-SGT mappings pushed from ISE via SSH
ASA 5505	10	250	CPU load method

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Platform	Maximum SXP connections	Maximum IP-SGT bindings	Comments
ASA 5510	25	1,000	CPU load method
ASA 5520	50	2,500	CPU load method
ASA 5540	100	5,000	CPU load method
ASA 5550	150	75,000	CPU load method
ASA 5580-20	250	10,000	CPU load method
ASA 5580-40	500	20,000	CPU load method
ASA 5585-SSP10	150	18,750	CPU load method
ASA 5585-SSP20	250	20,000	CPU load method
ASA 5585-SSP40	500	50,000	CPU load method
ASA 5585-SSP60	2,000	500,000	CPS method
ASA 5506-X	2,000	195,000	CPS method
ASA 5555-X	2,000	500,000	CPS method
FP-4110	2,000	1M	CPS method
FP-9300 SM-36	2,000	1M	CPS method
ISE 3495 ISE 2.0	20	100,000	
ISE 2.1 with single SXPN	100	250,000	
ISE 2.1 with 2 SXPN	200	500,000	

Table 4. Cisco TrustSec Platform Scalability of Router Products

Platform	Maximum Unidirectional SXP Connections (Speaker only/ Listener only)	Maximum Bidirectional SXP Connections	Maximum IP SGT Bindings
890 Series Routers	100		1,000
1900 Series Routers	500	250	100,000 with unidirectional SXP connections 25,000 with bidirectional SXP connections
2900, 3900 Series ISRG2	250	125	180,000 with unidirectional SXP connections 125,000 with bidirectional SXP connections
4400 Series ISR	1800	900	750,000 (IOS XE 3.15 and 3.16) 135,000 (IOS XE earlier than 3.15)
ASR 1000 Series	1800	900	750,000 uni-directional (IOS XE 3.15 and 3.16) 180,000 (IOS XE earlier than 3.15)
ASR 1006 RP2 as SXP Reflector		250 with 100 bindings, 126 with 500 bindings	
Cloud Services Router 1000V Series (CSR)	900	450	750,000 (IOS XE 3.15 and 3.16) 135,000 (IOS XE earlier than 3.15)

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Table 5. Cisco TrustSec Platform Scalability of SGACLs

Platform	Maximum number of SG ACEs	Notes
Catalyst 3750-X & 3560-X	~~48~~	1015 maximum unique cells
Catalyst 3650 Catalyst 3850-SE, 3850-XS Catalyst 3850	~~1375 (L3) per system~~ 680 L4 per system	Max # of ACEs in SGACL should be 300 or less due to buffer size limits 256 Source/Destination Groups
Catalyst 4500-X, Catalyst 4500 Sup 7-E/7L-E/8-E/8L-E	64,000	Ranges between 64k ACEs in 1 SGACL to 1 ACE in 64k SGACLs
Catalyst 6500 Series Supervisor Engine 2T and 6T	16,000	
Catalyst 6840-X	16K	
Catalyst 6880-X	64K (XL), 16K (LE)	
Catalyst 9300	5,000	256 Source/Destination Groups
Catalyst 9500	5,000	
AP Wave 1 & Wave 2	256 ACEs per SGACL	400 unique SGACLs, 50 SGTs
WLC 8540, 5520, 3504	256 ACEs per SGACL	8,000 unique SGACLs, 512 SGTs
Nexus 7K M3, M2, M1 Modules	128,000	
Nexus 7K F3, F2, F2e Modules,	16,000	
Nexus 7K F1 Modules	1024	
Nexus 1000V	6,000	
Nexus 5500	124	124 SGACL TCAM entries available per bank of 8 ports for feature use (4 of 128 are default entries) Sum of SGACL entries per 8 port bank cannot contain more than 124 permissions in total SGACL can be reused extensively; Over 2000 SGT, DGT combinations possible from reusing 124 lines of permissions
Nexus 5600, 6000	1148	
ASR 1000	4,096 per cell	62,500 maximum number of unique cells

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA v6.3b C96-731479-00 12/17

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.