Cisco TrustSec Software-Defined Segmentation Release 6.1 System Bulletin

Introduction

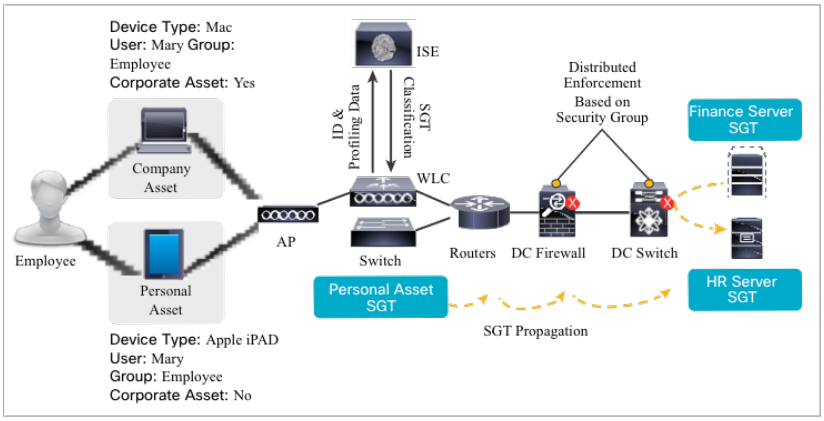
Network segmentation is essential for protecting critical business assets. Cisco TrustSec® Software Defined Segmentation balances the demands for agility and security without the operational complexity and difficulty of deploying into existing environments seen with traditional segmentation. With TrustSec,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

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

network where TrustSec can be quickly enabled.

Summary of New Cisco TrustSec Capabilities

The Cisco TrustSec 6.1 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 6.1

- Applying group-based policies to FlexConnect WLAN users: With the WLC release v8.3, endpoints connected to FlexConnect Access Points can be classified and assigned to Security Groups. The Cisco 2504, 5508, 5520, Flex 7510, 8510, and 8540 WLCs and WiSM2 can then share Security Group membership with other network devices to enable simple group-based access controls to control user access to resources like data center applications. This also enables the use of group-based policies in firewalls, next-gen firewalls, Web Security appliances for FlexConnect users.
- Rapid deployments of campus Software-Defined Segmentation without needing inline tagging: An SXP domain logically groups network devices to which SXP mappings should be exchanged. SXP domain capabilities now allow switches to exchange SFT information directly via ISE avoiding the need to enable inline tagging between network devices. This allows rapid enablement of campus segmentation which work seamlessly even if the distribution and core switches used in the campus network have no TrustSec capabilities. In addition, more granular control of the distribution of mappings is possible through isolation of SXP peers and the bindings learned between them. The feature is supported with ISE 2.1.
- Extending Software-Defined Segmentation capabilities to routers: The software-defined segmentation capabilities widely used on Catalyst and Nexus switches are now available on ISR and ASR routers. With SGACL enforcement capabilities now available, segmentation policies can be dynamically downloaded from ISE or defined locally on routers. Updated policies are downloaded to the router when the SGACL policy is modified on ISE and a Change of Authorization (CoA) instruction is pushed to the router. SGACL Enforcement is now available on ISR 4300 series: 4321/4331/4351, ASR 1000 Series: 1001-X/1002-X/1002-HX, and CSR1000V in IOS XE Everest 16.4.1, which complements the ISR 4431 & 4451, and ASR 1004, 1006, 1013, 1006-X, 1009-X platforms support from IOS XE Denali 16.3.1.
- Monitoring router segmentation policies before enforcing them: SGACL Monitor Mode gives the administrator the ability to test segmentation policies in a monitor-only mode so that policy can be evaluated before it is actively applied. This is supported on ISR 4000 series and ISRv, ASR 1000 series, and CSR 1000V with IOS XE Everest 16.4.1. This complements the ISR 4431 & 4451, and ASR 1004, 1006, 1013, 1006-X, 1009-X platform support from IOS XE Denali 16.3.1.
- Extending group-based policies to Cisco Industrial Security Appliances: The Cisco ISA 3000 running ASA 9.6.1 supports group-based policies to simplify and automate policy management. The ISA 3000 supports SXP speaker listener v3, Remote Access VPN classification, SGToverEthernet (inline tagging), and SGFW enforcement.
- Software-Defined Segmentation with IWAN using IOS XE Denali 16.3.2: Segmentation and micro-

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

segmentation policies are enabled with IWAN. For example, within a store, segmentation restricts the interaction between the various departments in the store or across the WAN to the data center so that PCI compliance, HIPAA compliance, and other business needs are met. Traffic can use inline tagging or SXP and/or NAT over DMVPN.

- SGT Propagation using VXLAN: Catalyst 3650 and Catalyst 3850 support inline tagging using VXLAN in IOS XE Denali 16.3.1. This permits seamless integration of TrustSec with the campus fabric to increase VM mobility and deployment flexibility and retain the benefits of segmentation.
- Catalyst 3850/3650 SGACL Logging: For monitoring and troubleshooting, the SGACL logging capabilities available on other Catalyst and Nexus switches are now available on the Catalyst 3650 & Catalyst 3850. These SGACL fields are logged in the local logs and logs send to remote syslog servers: 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 3.6.6.

Summary of current Cisco TrustSec Features Validated in 6.1

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 ISA3000 Series

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 6.1 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 or Beryllium 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 plane exchange	Cisco ISE 2.1- ACI API
Cisco Application Policy Infrastructure Controller – Data Center	Cisco APIC-DC	APIC-DC 1.3(1g)		
Open Daylight SDN controller	ODL SDN	Lithium, Beryllium	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. 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

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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 2. 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	ISE 3515, 3595, 3415, and 3495 Appliance & VMware	Base Plus for pxGrid	Cisco ISE 2.1, 2.0, ISE 1.4	Cisco ISE 2.0	Dynamic, IP 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* 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-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 3.6.4	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
	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;**** SGT over MACsec	SGACL

© 2016 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 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 3.5.1E	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
	Catalyst 4500 E-Series Supervisor Engine 8-E and 8L-E	IP Base K9 & above Cisco ONE Foundation & above	Cisco IOS XE 3.6.6E	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
	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 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*
	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	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, Listener V4	SGT over Ethernet	SGACL

© 2016 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
Cisco Industrial Ethernet Switches	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, Listener V4	SGT over Ethernet on1G interfaces only	SGACL
Cisco Wireless Con-trollers	5500 Series (5508,5520) 2500 Series (2504)	-	Cisco AireOS 8.3.102.0, 7.6.130.0	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	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
Cisco Nexus® 7000 Series	Nexus 7000 M-Series and F-Series*** modules 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 requires 7.3(0)D1(1) or later	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	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 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	SGACL

© 2016 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
Cisco Integrated Services Router (ISR)	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*
	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*
	4000 Series ISR 4431, 4451-X, 4321, 4331, 4351	IP Services/K9 for classify/ propagate; SEC/K9 for 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*
	ISRv	IP Services/K9 for classify/ propagate; SEC/K9 for enforce-ment	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 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	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*
	Cloud Services Router 1000V Series (CSR)	IP Services/K9 for classify/ propagate; SEC/K9 for 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 IPsec VPN, DMVPN	SGACL

© 2016 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 Aggrega-tion 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 Services/K9 for classify/ propagate; SEC/K9 for enforcement	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*
	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
	ASR 1004, 1006, 1013, 1001-X, 1002-X,1002-HX, 1006-X, and 1009-X	IP Services/K9 for classify/ propagate; SEC/K9 for 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*
Cisco Adaptive Security Appliance (ASA)	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**, 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*

© 2016 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
Cisco Firepower (FP)	FP 4100 FP 9300 Cisco Firepower Threat Defense Firepower 4100 & 9300	- Firepower Threat Defense Base	Cisco FXOS 2.0.1.37 Cisco ASA 9.6.1 Cisco Firepower System 6.1.0	Cisco FXOS 2.0.1.37 Cisco ASA 9.6.1 Cisco Firepower System 6.1.0	Remote Access VPN (IPSec, SSL-VPN) -	Speaker, Listener V3 pxGrid	SGT over Ethernet SGT over Ethernet	SG Firewall SG Firewall
	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	-
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

* Catalyst 2960 S/SF Product management recommends 15.0(2)SE which supports SXP v2.

* 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, and WLC AireOS 8.1. These releases have been 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 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 method is considered a better measure for firewalls. Table 2 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 3k Series (non-stack)	1,000	200,000	
Catalyst 3850 Series / (Stack)	128	12,000	
Catalyst 4500 Supervisor Engine 6-E and 6L-E	1,000	200,000	
Catalyst 4500 Supervisor Engine 7-E	1,000	256,000	
Catalyst 4500 Supervisor Engine 7L-E	1,000	64,000	

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Platform	Maximum SXP connections	Maximum IP-SGT bindings	Comments
Catalyst 4500 Supervisor Engine 8-E	2,000	200,000	
Catalyst 4500-X Series	1000	64,000	
Catalyst 6500 Series Supervisor Engine 2T	500	200,000	
Catalyst 6800 Series	2,000	200,000	
5505 Series Wireless Controller	5		
5760 Series Wireless Controller	128	12,000	
Nexus 7000 M1, M2	980	200,000 (7.2, +) 50,000 (pre 7.2)	
Nexus 7000 F1	980	512	
Nexus 7000 F2/F2e Supervisor	980	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	6,000 per VMS	
ASA 5505	10	250	CPU load method
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 5506-X	2,000	195,000	CPS method
ASA 5555-X	2,000	500,000	CPS method
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
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
2900, 3900 Series ISRG2	250	125	180,000 with unidirectional SXP connections 125,000 with bidirectional
4400 Series ISR	1800	900	135,000
ASR 1000 Series	1800	900	750,000 (IOS XE 3.15, and later) 180,000 (earlier)
Cloud Services Router 1000V Series (CSR)	900	450	135,000

© 2016 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 RBACLs	Notes
Catalyst 3850-SE, 3850-XS	1375 (L3) per system	680 L4 SGACLs. Max # of ACEs in SGACL should be 300 or less due to buffer size limits
Catalyst 4500-X	16K	
Catalyst 6840-X	8K	
Catalyst 6880-X	32K (XL), 8K (LE)	
Nexus 7K F1 Modules	1024	
Nexus 7K F2/F2e Modules, F3 Modules	16K	
Nexus 7K M Modules	128K	
Nexus 1000V	6K	
Nexus 5500	124	124 SGACL TCAM entries available per bank of 8 ports for feature use 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	

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 v6.1c
C96-731479-00 4/17
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.