Cisco TrustSec Release 5.3 System Bulletin

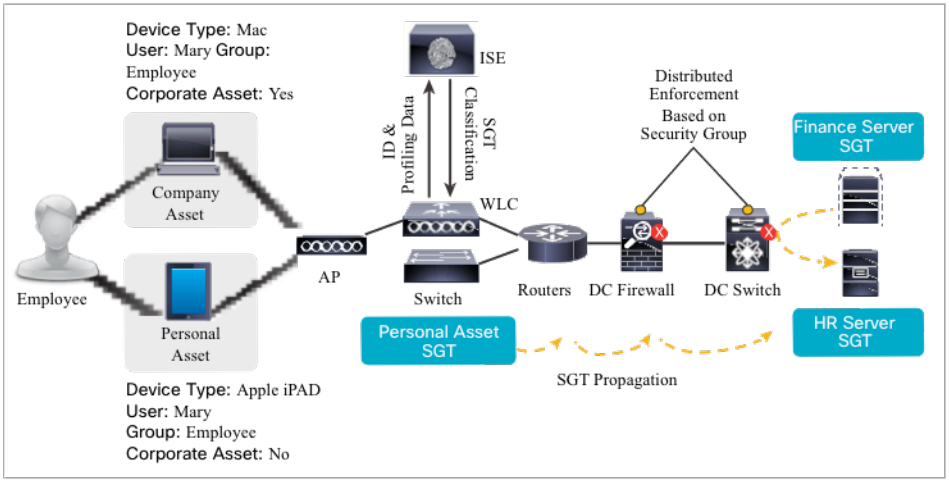
Introduction

Cisco TrustSec® technology uses software-defined segmentation to simplify the provisioning of security policies, to accelerate security operations, and to consistently enforce policy anywhere in the network. TrustSec is embedded technology in Cisco switches, routers, wireless, and security devices. It is a secure network architecture that extends security across the network from campus to branch to data center. TrustSec is the foundation for using the Network as an Enforcer and mitigates risk by reducing attack surface through better segmentation, whilst also increasing operational efficiency and making compliance goals easier to achieve.

TrustSec works with the Cisco Identity Services Engine (ISE), Cisco's market-leading policy management platform. Cisco ISE gathers advanced contextual data about who and what is accessing the network. It then defines role-based access using Cisco TrustSec to permit or constrain access to data and applications through segmentation of the network and enforcement of policy decisions across the network.

Cisco TrustSec® technology simplifies the provisioning of access controls and segmentation functions through the use of logical identifiers called Security Group Tags (SGTs). The tag represents a set of network endpoints or servers with common entitlements. The tag provides a layer of policy abstraction which works independently of the underlying IP address-based or VLAN mechanisms traditionally used for access control. Policies for wired, wireless, or VPN remote access can be managed consistently and centrally to avoid the operational cost associated with topology-based policy management. Figure 1 is an example of Cisco TrustSec® in a network.

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 5.3 release continues to validate three major deployment scenarios:

- 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.

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.

New Cisco TrustSec Deployment Scenarios Validated in Release 5.3

- Restricting lateral movement of threats, also known as East-West segmentation, reduces the cyber threat attack surface by disallowing certain communication between workstations in campus/branch networks. After initial malware enters the network, subsequent compromise of other users' systems is avoided as segmentation prevents the malware from propagating from workstation-to-workstation, within the same VLAN or between VLANs. Stacked Cisco Catalyst 3850 and 3750-X Series switches and Cisco Catalyst 4500 Supervisor Engine 8-E were used as access switches with Catalyst 4500-X Series switches and Catalyst 6500 Series Supervisor Engine 2T switches as the distribution switches supporting inline tagging with SXP also being tested using the ASR1000 as an SXP reflector.
- Wide Area Application Services with TrustSec. Many customers use Wide Area Application Services (WAAS) for WAN optimization between the branch and main campus network. Seamless interoperability of these WAN services is validated with TrustSec inline tagging from the branch site over the WAN to the campus head end using GRE, IPsec, DMVPN and GETVPN. SGT Caching is a feature which caches the Security Group Tags as traffic is redirected to WAAS appliances which are not SGT-aware.. Traffic is re-tagged with the appropriate SGT after optimization. SGT Caching is supported on the Cisco ISR 4000 Series, Cisco ISR-G2 series, Cisco ASR 1000 series, and Cisco CSR 1000V routers, as well as the Cisco Nexus 7000 Series and Cisco Catalyst 6500 Series switches.
- TrustSec policy enforcement on a single switch. The TrustSec solution is flexible and allows policy enforcement be enabled anywhere on the network, even on a single network device. We can classify protected subnets with an SGT or assign SGTs to specific IP addresses related to protected applications. These static SGT assignments can be defined in ISE and provisioned to the Cisco Catalyst 3850 Series, Cisco Catalyst 4500X Series, and Cisco Catalyst 6500/6800 Series with Supervisor Engine 2T
- User to Data Center Access Control, where the access-layer does not support TrustSec. Using ISE 2.0 we can generate IP-SGT classifications for endpoints even if they are connected to access-layer network devices they are connected to do not have any TrustSec capabilities. The SGT classification can be generated by ISE 2.0 and propagated to policy enforcement points using the new SGT Exchange Protocol (SXP) version 4 capabilities added in ISE 2.0.
- Wireless segmentation for intra-VLAN/SSID and inter-VLAN/SSID has been validated for the Cisco Wireless LAN Controller 5520 forwarding traffic to the default gateway on a layer 2 connected switch. The Cisco Catalyst 3850 switch and Catalyst 4500-X switches have been validated enforcing SGACL policy for inter-VLAN/SSID traffic. The Cisco Catalyst 4500-X enforces SGACL policy for inter-VLAN, and default SGACL policy for intra-VLAN traffic.
- Segmentation in converged access on the Cisco Catalyst 4500 switch with Supervisor Engine 8 and the Cisco Catalyst 3850 switch with the Cisco Wireless WLC 5520 Mobility Controller is validated within the same SSID and same or different VLANs, between different SSIDs (different VLANs), between a single

SSID (VLAN) and wired port on the same switch (in a different VLAN), and between a single SSID (VLAN) and wired port on different switches. CSCuw48956 currently prevents roaming between AP's on the Cisco Catalyst 3850 and Cisco Catalyst 4500 Supervisor Engine 8e from maintaining the SGT. CSCuw49141 prevents VLAN-to-SGT and Subnet-to-SGT classification from working on the Cisco Catalyst 3850 in release IOS XE 3.6.3.

- Segmentation in an Instant Access configuration with the Catalyst 3560C-X Compact Switch. Hosts on a Cisco Catalyst 3560C-X switch connected to a Cisco Catalyst 6500 with Supervisor Engine 2T using Instant Access participate in segmentation. Segmentation validated within the same VLAN, between VLANs, or on traffic going either way between the switches is enforced through SGACLs on the Cisco Catalyst 6500.
- SGT Visibility with NetFlow. Cisco NetFlow provides visibility into network and security operations. In releases IOS-XE 3.6.3 and IOS-XE 3.7.1, Cisco Catalyst 3850 and Cisco Catalyst 4500 with Supervisor Engine 8 provide Source and Destination SGT in Flexible NetFlow records. This enables monitoring services to trace tags from the user to the data center, and from endpoint to endpoint in the same VLAN, or between end points in different VLANs on the same switch.
- TrustSec IPv6 Capabilities. TrustSec now can be enabled for iPv6 traffic on certain platforms. TrustSec policy is based on the classified group information, not based on the IP address and its version. TrustSec policies can be applied to both IPv4 and IPv6 traffic because of the TrustSec IP version agnostic policy. The Cisco Catalyst 3000X Series, 3650 and 3850 Series, 4500 Series with Supervisor Engine 7E/LE or Supervisor 8E, and 6500 Series with Supervisor Engine 2T are able to classify IPv6 address enabled endpoints and send IP-SGT binding to other SXP peers for enforcement. The Cisco Catalyst 6500 with Supervisor Engine 2T and the Adaptive Security Appliance (ASA) enforce policies for IPv6 traffic with TrustSec. The Cisco ASA is able to translate IPv6 to IPv4 bindings for further propagation as well.
- Cisco Security Manager provides a central management console for multiple firewalls. Cisco Security Manager 4.8 is able to provision TrustSec capabilities in equivalent fashion to CLI or ASDM. TrustSec capabilities are enhanced by the high availability of ASA clustering of ASA 5585-X configured through CSM 4.8.

Summary of current Cisco TrustSec Features Validated in 5.3

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

These platforms were tested in this release.

- Cisco Identity Services Engine (ISE)
- Cisco Catalyst 6500 with Supervisor Engine 2T
- Cisco Catalyst 4500 with Supervisor Engine 8
- Cisco Catalyst 3750X, 3560CX, and 3850
- Cisco Catalyst 2960S and 2960S Series
- ISR-G2 2910
- WLC5760 and WLC5520
- Cisco IE2000U, IE3000, and IE4000 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 5.3 validation program, and some follow-on defect verification (Catalyst 3850 3.6.4).

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.

Table 1. Cisco TrustSec Platform Support Matrix

System Component	Platform	License	Solution-Level Validated Version	Security Group Tag (SGT) Classification	SGT Exchange Protocol (SXP) Support and Version	Inline SGT Tagging	SGT Enforcement
Cisco Identity Services Engine	Cisco ISE 3415, and 3495; Appliance and VMware	Base	Cisco ISE 2.0, ISE 1.4	IP to SGT, Dynamic	Speaker, Listener V4	–	–
Cisco Catalyst® 2000 Series	Cisco Catalyst 2960-Plus Series Switches	LAN Base K9	- (Minimum version is 15.2(2)E)	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT	Speaker V4	No	No
	Cisco Catalyst 2960-C Series	LAN Base K9	- (Minimum version is 15.2(2)E)	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT	Speaker V4	No	No
	Cisco Catalyst 2960-CX Series	LAN Base K9	- (Minimum version is 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	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	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	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	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	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****	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	Cisco IOS XE 3.6.4	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

System Component	Platform	License	Solution-Level Validated Version	Security Group Tag (SGT) Classification	SGT Exchange Protocol (SXP) Support and Version	Inline SGT Tagging	SGT Enforcement
Cisco Catalyst 4500 Series	Cisco Catalyst 4500 Supervisor Engine 6-E and 6L-E	IP Base K9	Cisco IOS 15.1(1)SG	Dynamic, IP to SGT	Speaker, Listener V4	No	No
	Cisco Catalyst 4500 Supervisor Engine 7-E and 7L-E	IP Base K9	Cisco IOS XE 3.5.1E	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT, Layer 3 Interface (L3IF) to SGT, Port to SGT	Speaker, Listener V4	SGT over Ethernet; SGT over MACsec (See footnote for list of supported line cards)	SGACL
	Cisco Catalyst 4500 Supervisor Engine 8-E and 8L-E	IP Base K9	Cisco IOS XE 3.6.3	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 list of supported line cards)	SGACL
	Cisco Catalyst 4500-X Series	IP Base K9	Cisco IOS XE 3.6.3	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	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	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)
	Cisco Catalyst 6800-X and 6800ia	IP Base K9	Cisco IOS 15.2(1)SY0a, 15.2(3a)E	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 (requires WS-X6900 line cards for Catalyst 6807)	SGACL (IPv4, IPv6)
Cisco Connected Grid Routers and Switches	Cisco 2010 Connected Grid Routers	-	Cisco IOS 15.5(2)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	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 Series	IP Services	Cisco IOS 15.2(3)EA	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT	Speaker, Listener V4	No	No
	Cisco IE 3000 Series	IP Services	Cisco IOS 15.2(3)EA	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT	Speaker, Listener V4	No	No
	Cisco IE 4000 Series	IP Services	Cisco IOS 15.2(2)EA	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT	Speaker, Listener V4	No	No

System Component	Platform	License	Solution-Level Validated Version	Security Group Tag (SGT) Classification	SGT Exchange Protocol (SXP) Support and Version	Inline SGT Tagging	SGT Enforcement
Cisco Wireless Controllers	Cisco 5500 Series (5508,5520) and Cisco 2500 Series (2504); Cisco Wireless Services Module 2 (WiSM2)	-	Cisco Wireless Release 8.1	Dynamic	Speaker V2	No	No
	Cisco 5760 Wireless Controller Series	IP Base K9	Cisco IOS XE 3.7.0E	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 Wireless Release 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 6.1 and later	Cisco NX-OS 7.2(0)D1(1)	IP to SGT[1], Port Profile to SGT, VLAN to SGT[2], Port to SGT[2] [1]:Fabricpath support requires 6.2(10) or later [2] VPC/VPC+ support requires 7.2(0)D1(1) or later	Speaker, Listener V1	SGT over Ethernet[3]; SGT over MACsec[4] [3]: F3 interfaces (L2 or L3) require dot1q tags [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)	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)	Port to SGT	Speaker V1	SGT over Ethernet	SGACL
Cisco Nexus 1000 Series	Cisco Nexus 1000V for VMware vSphere	Advanced license for SGT/ SGACL support	Cisco NX-OS 5.2(1)SV3(1.3)	IP to SGT, Port Profile to SGT	Speaker, Listener v1	SGT over Ethernet	SGACL

System Component	Platform	License	Solution-Level Validated Version	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 enforcement	890: Cisco IOS 15.4(1)T1 1900/2900/3900: Cisco IOS 15.5(1)20T	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
	Cisco 4000 Series (ISR 4451-X validated)	IP Services/K9 for classify/ propagate; SEC/K9 for enforcement	Cisco IOS XE 3.15.01S	IP to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4	SGT over Ethernet, SGT over GETVPN, DMVPN, or IPsec VPN, SGT Caching	SG Firewall PBR
	Cisco SM-X Layer 2/3 EtherSwitch Module	IP Services/K9 for classify/ propagate; SEC/K9 for enforcement	Cisco IOS 15.5.2T	Dynamic, IP to SGT, VLAN to SGT	Speaker, Listener V4	SGT over Ethernet; SGT over MACsec	SGACL
	Cisco Cloud Services Router 1000V Series (CSR)	IP Services/K9 for classify/ propagate; SEC/K9 for enforcement	Cisco IOS-XE 3.15.01S	IP to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4	SGT over Ethernet, SGT over IPsec VPN, DMVPN	SG Firewall PBR
Cisco Aggregation Services Router (ASR)	Cisco 1000 Series Router Processor 1 or 2 (RP1, RP2); ASR 1001, 1002, 1004,1006 and 1013 with Embedded Services Pro-cessor (10,20, or 40 Gbps) and SPA Interface Processor (10/40)	IP Services/K9 for classify/ propagate; SEC/K9 for enforcement	Cisco IOS XE 3.15.0S	IP to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4	SGT over Ethernet, SGT over GETVPN IPsec VPN, or DMVPN SGT Caching	SG Firewall PBR
	Cisco ASR 1001-X and 1002-X	IP Services/K9 for classify/ propagate; SEC/K9 for enforcement	Cisco IOS-XE 3.13.0S	IP to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4	SGT over Ethernet, SGT over GETVPN, IPsec VPN, DMVPN	SG Firewall
Cisco Adaptive Security Appliance (ASA)	Cisco ASA 5510, 5520, 5540, 5550, 5580	-	Cisco ASA 9.0.1, ASDM 7.1.6		Speaker, Listener v2		SG Firewall
	Cisco ASA 5505, 5512, 5515, 5525, 5545, 5555, 5585	-	Cisco ASA 9.4.1, ASDM 7.4.2, CSM 4.8	Remote Access VPN (IPSec, SSL-VPN)	Speaker, Listener V2 (IPv4, IPv6)	SGT over Ethernet	SG Firewall (IPv4, IPv6)
	Cisco ASA 5512-X, 5515-X, 5525-X, 5545-X, 5555-X, 5585-X with FirePower	-	Cisco ASA 9.4.1, ASDM 7.4.2, CSM 4.8	Remote Access VPN (IPSec, SSL-VPN)	Speaker, Listener V2 (IPv4, IPv6)	SGT over Ethernet	SG Firewall (IPv4, IPv6)
	Cisco ASAv	-	Cisco ASA 9.3.1 ADSM 7.1.6	Remote Access VPN (IPSec, SSL-VPN)	Speaker, Listener V2	SGT over Ethernet	SG Firewall

Notes

* Product part numbers of supported line cards for SGT over Ethernet on the Cisco Catalyst 4500 Supervisor Engine 7-E and Supervise Engine 7L-E include the following: WS-X4712-SFP+E, WS-X4748-UPOE+E, WS-X4748-RJ45V+E, WS-X4748-RJ45-E, WS-X4640-CSP-E, WS-X4724-SFP-E, WS-X4748-SFP-E.

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

- With IPv6 support, DGT can be IPv4.

-Cisco WLC 7500 and vWLC do not support Cisco TrustSec.

- Cisco ASR 9k Series with enhanced ethernet line cards support of SGT over Ethernet recently removed command support.

**** 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 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	
Cisco ASA 5510	25	1,000	
Cisco ASA 5520	50	2,500	
Cisco ASA 5540	100	5,000	
Cisco ASA 5550	150	75,000	
Cisco ASA 5580-20	250	10,000	
Cisco ASA 5580-40	500	20,000	

Cisco ASA 5585-SSP10	150	18,750	
Cisco ASA 5585-SSP20	250	20,000	
Cisco ASA 5585-SSP40	500	50,000	
Cisco ASA 5585-SSP60	1,000	100,000	
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) 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 v5.3f C96-731479-00 05/16