Cisco Secure Access and TrustSec Release 4.0

PB712066

Introduction

The Cisco Secure Access and TrustSec capabilities provide an intelligent access control solution that enables secure network access, shows who and what is connecting to the network and mitigates risk by providing centralized controls over the resources that users and devices can access.

Cisco Secure Access features provide flexible authentication and device classification functions that enable identity and context-aware network services to be deployed in the access-layer of enterprise networks. These features work with the Cisco Identity Services Engine (ISE) to allow user and device identities to be validated, devices to be profiled and on-boarded, device posture to be assessed and remediated, if necessary.

Cisco Secure Access capabilities also allow access controls to be applied at the point of network access. These controls include VLAN and downloadable IP Access Control List (ACL) assignments.

Cisco TrustSec provides a new approach to defining access controls, allowing them to be invoked anywhere on the network or applied across a network. This is possible because the access controls are managed through a layer of abstraction, decoupling the security rules and policies from the network devices that apply them.

- Cisco TrustSec functions can be applied to user access networks, data center infrastructure, routers and security appliances.
- Cisco TrustSec simplifies the provision of access controls and segmentation functions through the use of logical identifiers called Security Group Tags (SGTs). These can be used anywhere on the network, because they work independently of the underlying IP address or VLAN mechanisms traditionally used for access control.

The Cisco Secure Access capabilities provide baseline network access authentication and the enforcement of granular user identity-based policies for network access. Cisco TrustSec functions simplify the provisioning and management of access control policies after the user or device is granted access to the network.

To ensure smooth customer deployments of the complete solution, Cisco has developed a rigorous validation process including component level interoperability, scalability and performance tests.

Summary of New Cisco TrustSec Capabilities Tested

One of the major advantages of the Cisco TrustSec solution is that it allows customers to apply policy-defined segmentation functions, with the policy elements decoupled from underlying network topology. With version 4.0 of the solution:

- The solution's policy enforcement capabilities have been extended to support branch networks, so that WAN customers can enable consistent policy enforcement across data centers, campus and branch offices. Previous TrustSec validation work has been focused on campus networks and data centers.
- Solution capabilities have been added to Cisco Connected Grid Routers, delivering new policy enforcement capabilities to field locations for our energy provider and utility customers.

- For Data Center environments, Cisco has validated new capabilities in two areas:
  - New options for classifying servers into TrustSec roles, simplifying how firewall rules and data center access controls are applied and also reducing SecOps effort.
  - Cisco TrustSec functions can now be applied to Cisco FabricPath data center networks. Cisco FabricPath facilitates highly virtualized data centers, private clouds and high-performance computing, which can now take advantage of the highly-scalable policy enforcement capabilities of the Cisco TrustSec solution, embedded in Nexus 7000 and 5000 Series Switches. Cisco FabricPath allows highly scalable Layer 2 multipath networks to be built without the use of the Spanning Tree Protocol. SGT functions are now fully supported in Cisco FabricPath environments in data centers.

Cisco TrustSec 4.0 also validates new use-cases requested by customers, including:

- Assigning SGT-VLAN mappings for SSL-VPN Remote Access users connecting to the Cisco Adaptive Security Appliance (ASA).
- Wireless policy enforcement provided by the Cisco Catalyst 6500 System using the Supervisor Engine 2T and the Cisco Wireless Services Module 2 (WiSM2), which apply SGT classification and enforcement functions within the same chassis.

New Cisco TrustSec Platform Support Validated

- The Cisco 2951 and 3945 Integrated Service Routers Generation 2 (ISR-G2) support for inline Security Group Tagging on built-in Gigabit Ethernet ports. This capability allows SGT information to be exchanged with peers without using the SGT Exchange Protocol (SXP). A SEC-K9 license is required to enable this feature.
- The Cisco CGR 2010 Connected Grid Router, Cisco ISRG2 series routers and Cisco Aggregation Services Routers (ASR) 1000 products can now transport SGT tags over GET-VPN networks. A SEC-K9 license is required to enable this feature.
- Both Cisco ISRG2 series routers and Cisco ASR 1000 Series routers now support SXP Version 4, which handles any duplication of IP-SGT information sent when SXP connections are configured in a loop. The SEC-K9 license is also required to enable this feature.
- Nexus 7000 Series Switches with NX-OS 6.2 support for Cisco FabricPath with Cisco TrustSec.

Summary of Cisco Secure Access New Platform Support Tested

- Cisco 2520 Connected Grid Switch (CGS 2520).
- Cisco Industrial Ethernet 2000 and 3000 Series Switches.
- Cisco Catalyst 3850 Series.

New Cisco Secure Access Features Validated

The converged access platforms of the Cisco Catalyst 3850 Series and Cisco 5760 LAN Controller (WLC) now support bring-your-own-device (BYOD) initiatives, concurrent authentication sessions, default ACL management for critical authentication, and the download of RADIUS-based service templates.

Table 1 shows Cisco Secure Access functions that have been previously validated on Cisco IOS® Software switches in the Cisco TrustSec program.

Table 1. Baseline Validated Functions in Cisco Secure Access

Cisco TrustSec Program	Features
Release 1.99	IEEE 802.1X authentication
	MAC Authentication Bypass (MAB)
	Open Access
	Flexible Authentication
	Single Host Mode
	Multi Host Mode
	Multidomain authentication mode (MDA)
	Multiple authentication mode
	VLAN assignment
	Downloadable ACL
	Inactivity timer (MAB and IEEE 802.1X)
	Local Web Authentication (LWA)
	Wake on LAN (WoL)
	Cisco Discovery Protocol 2nd second port disconnect
	Integration with Dynamic Address Resolution Protocol (ARP) Inspection, IP services gateway, and port security
	MDA with Dynamic Voice VLAN Assignment
	Filter ID
	RADIUS-supplied timeout
	Guest VLAN
	Authorization-failed VLAN
	RADIUS accounting
	Critical port and inaccessible authentication bypass (IAB) for data domain
	Conditional logging and debugging on a per-port basis
Release 2.0 Addition	Change of authorization (Cisco Catalyst 2000, Catalyst 3000 and 6000 Series Switches, and Cisco WLC)
	Central web authentication (CWA) (URL-Redirect) with Cisco ISE
Release 2.1 Addition	Device sensor (Cisco Catalyst 3000 and 4000 Series Switches and Cisco WLC)
	IEEE 802.1AE MACsec and MACsec Key Agreement (Cisco Catalyst 3560-X, 3750-X Series and Catalyst 4500 Supervisor Engine 7-E)
	MAC Move
	MAC Replace
	Downloadable ACL enhancements
	Critical port and IAB for voice domain (Cisco Catalyst 2000, 3000, 4500, and 6500 Series)
	Change of Authorization (Cisco Catalyst 4500 Series)
	Change of Authorization with CWA (Cisco WLC)

Validated Platforms and Features

Table 2 summarizes the latest platforms and features that are validated in Cisco Secure Access and TrustSec 4.0. A complete and frequently updated list is available at cisco.com/go/TrustSec.

Table 2. Validated Platforms and Features in Cisco Secure Access and TrustSec Solution

Component	Platform	Cisco TrustSec 4.0 Validated Versions	Cisco Secure Access Features	Device Sensor	Cisco TrustSec (Security Group)				MACsec	
					Classification	Transport		Enforcement	Client to Switch	Switch to Switch
						Out-of-Band	Inline			
Cisco Identity Services Engine (ISE)	Cisco ISE 3315 and 3355 or 3395 appliances and VMware	Cisco ISE 1.2		Cisco ISE 1.2 Patch 1 (requires advanced license)					Cisco ISE 1.2 Patch1	
Cisco Catalyst 2000 platform switches	Cisco Catalyst 2960-C Series	Cisco IOS Software Release 15.0(2)SE2	Y	-	Dynamic	SXP (S)	-	-	-	-
	Cisco Catalyst 2960-S Series and 2960-SF Series	Cisco IOS Software Release 15.0(2)SE2	Y	-	Dynamic	SXP (S)	-	-	-	-
Cisco Catalyst 3000 Series Switches	Cisco Catalyst 3560 Series and 3750 Series	Cisco IOS Software Release 12.2(55)SE3	Y	-	Dynamic	SXP (S)	-	-	-	-
	Cisco Catalyst 3560-E Series and 3750-E Series	Cisco IOS Software Release 15.0(2)SE2	Y	Y	Dynamic	SXP (S, L)	-	-	-	-
	Cisco Catalyst 3560-C Series	Cisco IOS Software Release 15.0(2)SE2	Y	Y	Dynamic	SXP (S, L)	-	-	Y	Y
	Cisco Catalyst 3560-X Series and 3750-X Series	Cisco IOS Software Release 15.0(2)SE4	Y	Y	Dynamic and static VLAN-SGT mapping	SXP (S, L)	SGT over Ethernet (with MACsec option)	SG-ACL	Y	Y (requires Cisco Catalyst 3000-X and Services Module with 10 Gbps for uplinks)
	Cisco Catalyst 3850 Series	Cisco IOS XE 3.2.2SE	Y	N	-	-	-	-	-	-
Cisco Catalyst 4000 Series Switches	Cisco Catalyst 4500 Supervisor Engine 6-E and Supervisor Engine 6L-E	Cisco IOS Software Release 15.1(1)SG	Y	Y	Dynamic	SXP (S, L)	-	-	-	-
	Cisco Catalyst 4500 Supervisor Engine 7-E and Supervisor Engine 7L-E	Cisco IOS XE 3.3.0SG	Y	Y	Dynamic	SXP (S, L)	-	-	Y	Y (requires WS-X47xx linecards)

Component	Platform	Cisco TrustSec 4.0 Validated Versions	Cisco Secure Access Features	Device Sensor	Cisco TrustSec (Security Group)				MACsec	
					Classification	Transport		Enforcement	Client to Switch	Switch to Switch
						Out-of-Band	Inline			
Cisco Catalyst 6500 Series Switches	Cisco Catalyst 6500 Supervisor Engine 32 and Catalyst 6500 Series Supervisor Engine 720	Cisco IOS Software Release 12.2(33)SXJ2	Y	-	Dynamic	SXP (S, L)	-	-	-	-
	Cisco Catalyst 6500 Series Supervisor Engine 2T	Cisco IOS Software Release 15.1(1)SY1	Y	-	Dynamic, static VLAN-SGT, IP-SGT, subnet-SGT, and Layer 3 interface-SGT	SXP (S, L)	SGT over Ethernet (with MACsec option)	SG-ACL		Y (requires WS-X6900 Series line cards)
Cisco Integrated Services Routers Generation 2 (ISR G2)	Cisco 890 ISR platform, 1900 Series, 2900 Series, and 3900 Series	Cisco IOS Software Release 15.3(2)T	Y**	-	Dynamic, IP-SGT	SXP (S, L)	SGT over Ethernet (only on Cisco 2951 and 3945), SGT over GET-VPN	Zone-based security group firewall	-	-
Cisco ASR 1000 Series Aggregation Services Routers	Cisco ASR 1000 Series Router Processor 1 or 2 (RP1 or RP2) ASR 1001, 1002, 1004, 1006, and 1013 Routers with Embedded Services Processor (10, 20, or 40 Gbps) and SPA Interface Processor (10 and 40 Gbps)	Cisco IOS XE 3.9	-	-	Static IP-SGT mapping	SXP (S, L)	SGT over Ethernet SGT over GET-VPN	Zone-based security group firewall	-	-
Cisco Nexus 1000V Series Switches	Cisco Nexus 1000V	Cisco NX-OS 4.2(1)SV2(1.1) with Advanced feature license	-	-	Port profile-SGT	SXP (S)	-	-	-	-
Cisco Nexus 5000 Series Switches and 2200 platform fabric extenders	Cisco Nexus 5500 platform and Cisco Nexus 5548P, 5548P and 5596UP Switches	Cisco NX-OS 5.1(3)N2(1C)	-	-	Static IP-SGT, port profile-SGT	SXP (S)	SGT over Ethernet (no MACsec option)	SG-ACL	-	-
Cisco Nexus 7000 Series Switches and 2200 platform fabric extenders	All Cisco Nexus 7000 Series line cards and chassis (F-Series line cards do not support MACsec)	Cisco NX-OS 6.2(2) (no license needed for 6.1 and later)	-	-	Static IP-SGT, L2 interface-SGT, ort profile-SGT	SXP (S, L)	SGT over Ethernet (with MACsec option)	SG-ACL	-	Y (all line cards except F-Series modules)

Component	Platform	Cisco TrustSec 4.0 Validated Versions	Cisco Secure Access Features	Device Sensor	Cisco TrustSec (Security Group)				MACsec	
					Classification	Transport		Enforcement	Client to Switch	Switch to Switch
						Out-of-Band	Inline			
Cisco Wireless Controllers	Cisco Flex 7500 Series, Cisco 5500 Series and 2500 Series, Cisco Wireless Services Module 2 (WiSM2), Cisco Wireless LAN Controller Module for Integrated Services Routers G2 (WLCM2)	Cisco AireOS 7.2 MR1	Y**	-	-	-	-	-	-	-
	Cisco 5500 Series and 2500 Series, Cisco Wireless Services Module 2 (WiSM2), Cisco Wireless LAN Controller Module for Integrated Services Routers G2 (WLCM2)	Cisco AireOS 7.4.110	Y**	-	Dynamic	SXP (S)	-	-	-	-
	Cisco 5760 WLC	Cisco IOS XE 3.2.1SE	Y	-	-	-	-	-	-	-
Cisco Connected Grid Routers	Cisco 2010 CGR	Cisco IOS 15.3(2)T	Y	-	Dynamic, IP-SGT, VLAN-SGT	SXP (S/L)	SGT over GET-VPN	Zone-based security group firewall	-	-
Cisco Industrial Ethernet Switches	IE2000	Cisco IOS 15.0(2)EB	Y	-	-	-	-	-	-	-
Cisco ASA 5500 Series Adaptive Security Appliances	Cisco ASA 5505, 5510, 5520, 5540, 5550, 5580, 5585-X, 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X service modules and firewalls	Cisco ASA 9.1 ASDM 7.0(1)	-	-	-	SXP (S, L)	-	Security group firewall	-	-
Cisco Prime™ LAN Management Solution (LMS)	Software only	Cisco Prime LMS 4.1 or 4.2								
Cisco Prime Network Control System (NCS)	Software only	Cisco Prime Network Control System 1.1								
Cisco AnyConnect® Secure Mobility Client	Software only	Cisco AnyConnect 3.0								

Component	Platform	Cisco TrustSec 4.0 Validated Versions	Cisco Secure Access Features	Device Sensor	Cisco TrustSec (Security Group)				MACsec	
					Classification	Transport		Enforcement	Client to Switch	Switch to Switch
						Out-of-Band	Inline			
Cisco IP Phones	Cisco Unified IP Phones, including the following models: 6901, 6911, 6921, 6941, 6945, 6961, 7910G+SW, 7911G, 7912G, 7940G, 7941G, 794G-GE, 7942G, 7945G, 7960G, 7961G, 7961G-GE, 7962G, and 7965G	Skinny Client Control Protocol (SCCP) and Cisco Firmware Release 9.2(1)SR1								
Supported client supplicants		Native supplicants for Microsoft Windows 7, XP, and Vista, and Mac OS 10.6.5 and 10.7.1								

Notes

- For SXP roles, S represents Speaker and L represents Listener roles.
- Y means Yes (feature is supported). N means No (feature is not supported).
- Y** means that supported feature sets are different from Cisco Catalyst series switches as shown in Table 2.
- The Cisco LAN Base K9 license is required for Cisco Catalyst 2960 Series Switches for all Cisco Secure Access features. Cisco TrustSec classification and SXP requires the Cisco IP Base K9 license.
- The Cisco IP Base K9 license is required for Cisco Catalyst 3560, 3560-C, 3560-E, 3560-X, 3750, 3750-E, and 3750-X Series Switches; Cisco Catalyst 4500 Supervisor Engine 6-E and Supervisor Engine 6L-E, Cisco Catalyst 4500 Supervisor Engine 7-E and Supervisor Engine 7L-E, Cisco Catalyst 6500 Series Supervisor Engine 720, and Cisco Catalyst 6500 Series Supervisor Engine 2T.
- The Cisco ISR Base K9 license is required for Cisco Secure Access features. For Cisco TrustSec classification, propagation, and enforcement functions, the Cisco ISR SEC-K9 License is required.
- The Cisco ASR 1000 Cisco TrustSec license is required for Cisco ASR 1000 Series Aggregation Services Routers for all Cisco TrustSec functions.

For More Information

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

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C25-712066-02 10/13