TrustSec
2.1
Certified

Cisco TrustSec How-To Guide: Introduction

For Comments, please email: howtoguides@external.cisco.com

Current Document Version: 3.0

August 3, 2012

Table of Contents

Introduction

What Is the Cisco TrustSec System?

Cisco TrustSec®, a core component of the Cisco SecureX Architecture™, is an intelligent access control solution. Cisco TrustSec mitigates security risks by providing comprehensive visibility into who and what is connecting across the entire network infrastructure, and exceptional control over what and where they can go.

TrustSec builds on your existing identity-aware access layer infrastructure (switches, wireless controllers, and so on). The solution and all the components within the solution are thoroughly vetted and rigorously tested as an integrated system.

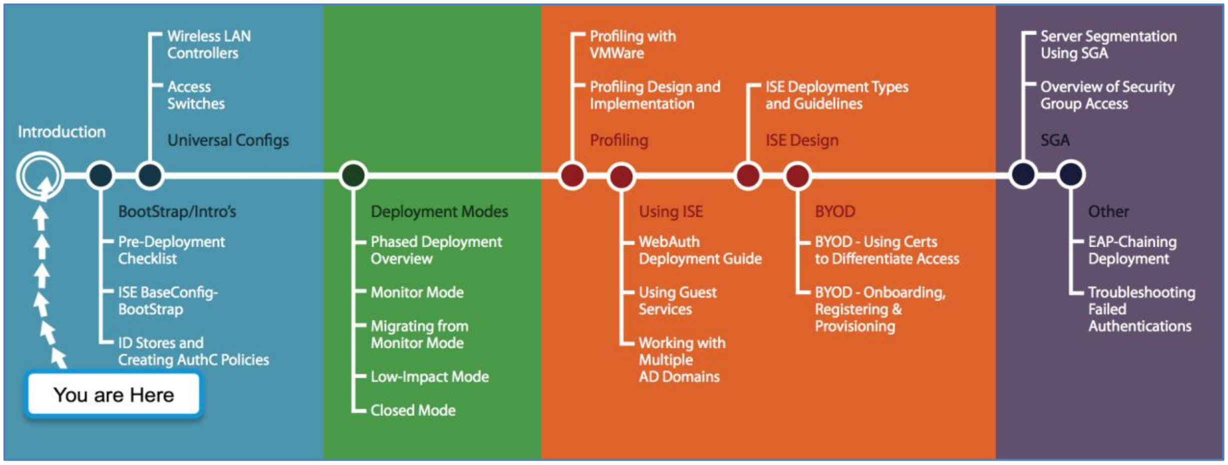
In addition to combining standards-based identity and enforcement models, such as IEEE 802.1X and VLAN control, the Cisco TrustSec system it also includes advanced identity and enforcement capabilities such as flexible authentication, Downloadable Access Control Lists (dACLs), Security Group Tagging (SGT), device profiling, posture assessments, and more.

About the TrustSec How-To Guides

The TrustSec team is producing this series of How-To documents to describe best practices for Cisco TrustSec deployments. The documents in the series build on one another and guide the reader through a successful implementation of the Cisco TrustSec system. You can use these documents to follow the prescribed path to deploy the entire system, or simply pick the single use-case that meets your specific need.

Each guide is this series comes with a subway-style "You Are Here" map to help you identify the stage the document addresses and pinpoint where you are in the Cisco TrustSec deployment process (Figure 1).

Figure 1: How-To Guide Navigation Map


Wireless LAN Controllers
Access Switches
Universal Configs
Introduction
BootStrap/Intro's
Pre-Deployment Checklist
ISE BaseConfig-BootStrap
ID Stores and Creating AuthC Policies
You are Here
Deployment Modes
Phased Deployment Overview
Monitor Mode
Migrating from Monitor Mode
Low-Impact Mode
Closed Mode
Profiling with VMWare
Profiling Design and Implementation
Profiling
ISE Deployment Types and Guidelines
ISE Design
Using ISE
WebAuth Deployment Guide
Using Guest Services
Working with Multiple AD Domains
BYOD
BYOD - Using Certs to Differentiate Access
BYOD - Onboarding, Registering & Provisioning
Server Segmentation Using SGA
Overview of Security Group Access
SGA
Other
EAP-Chaining Deployment
Troubleshooting Failed Authentications

What does it mean to be 'TrustSec Certified'?

Each TrustSec version number (for example, Cisco TrustSec Version 2.0, Version 2.1, and so on) is a certified design or architecture. All the technology making up the architecture has undergone thorough architectural design development and lab testing. For a How-To Guide to be marked "TrustSec certified," all the elements discussed in the document must meet the following criteria:

- Products incorporated in the design must be generally available.
- Deployment, operation, and management of components within the system must exhibit repeatable processes.
- All configurations and products used in the design must have been fully tested as an integrated solution.

Many features may exist that could benefit your deployment, but if they were not part of the tested solution, they will not be marked as "Cisco TrustSec "certified". The Cisco TrustSec team strives to provide regular updates to these documents that will include new features as they become available, and are integrated into the Cisco TrustSec test plans, pilot deployments, and system revisions. (i.e., Cisco TrustSec 2.2 certification).

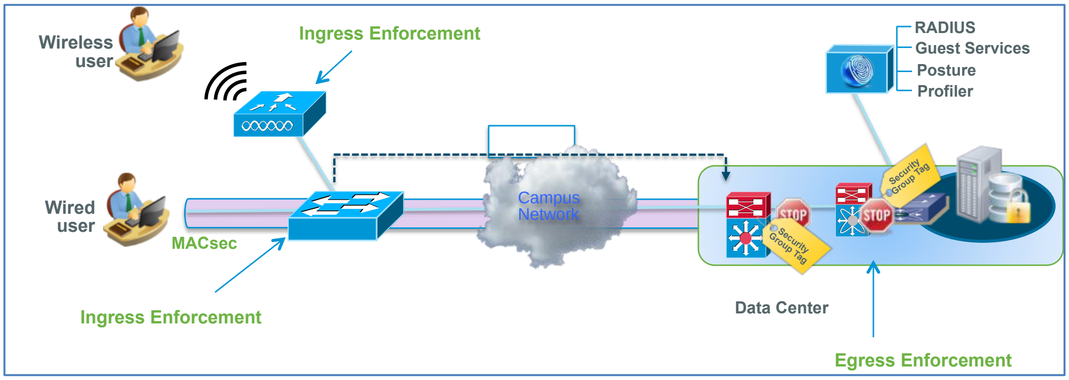
Additionally, many features and scenarios have been tested, but are not considered a best practice, and therefore are not included in these documents. As an example, certain IEEE 802.1X timers and local web authentication features are not included.

Note: Within this document, we describe the recommended method of deployment, and a few different options depending on the level of security needed in your environment. These methods are examples and step-by-step instructions for Cisco TrustSec deployment as prescribed by Cisco best practices to help ensure a successful project deployment.

Architecture Overview

Figure 2 depicts an end-to-end Cisco TrustSec system architecture. While all the scenarios shown in Figure 2 were part of the systems test, each How-To Guide will focus on a specific use-case and the components specific to the use-case. The TrustSec Certification system has integrated all the use cases into a solution. Please refer to each How-To Guide to find the details of the deployment. The 'Sample Scenarios' section focused few of the use cases explained in the How-To Guides.

Figure 2: Cisco TrustSec Architecture Overview



Sample Scenarios

BYOD: Onboarding, Registering and Provisioning

Cisco TrustSec Certification System helps companies move beyond basic Bring Your Own Device (BYOD) connectivity to create a better workplace experience. The BYOD scenario is created to safeguard network services, protect data, and provide a balance between enterprise needs and user demands. The BYOD How-To guide(s) cover some of the security features built into Cisco Identity Services Engine (ISE), such as:

- Native supplicant provisioning (NSP) for Apple iOS devices, Android, Windows, and Mac OS-X
- Endpoint certificate enrollment and provisioning
- Providing differentiated access with certificates

Guest Services

The Cisco Identity Services Engine offers centralized guest access management and enforcement for wired and wireless users, and can integrate easily with wireless solutions, third-party guest access portals, and billing providers. The Guest Services How-To Guide reviews the overall workflow for configuring full Guest Lifecycle Management Services, including:

- Configuring sponsor groups
- Guest account provisioning
- Configuration of authorization policies for guest access

Phased Deployments

The Phased Deployment How-To Guide discusses the three different modes of deployment: Monitor Mode, Low-Impact Mode, and Closed-Mode. It compares the modes, and discusses how to successfully migrate your network from Monitor Mode to Low-Impact or Closed Mode in a prescribed, safe, and repeatable manner.

Components Certified in Cisco TrustSec 2.1

Table 1 lists the Cisco TrustSec certified components in Cisco TrustSec Version 2.1.

Component	Hardware	Features Tested	Software Release
Policy Server			
Cisco Identity Services Engine (ISE)	Cisco ISE 3315, 3355, and 3395 Appliances and VMWare	All ISE functions and features	Cisco ISE Software Version 1.1.1.268
Network Access Devices (NADs)			
Cisco Catalyst® 2900 Series Switches	Cisco Catalyst 2960 and 2960S Series Switches	Basic identity features 802.1X authentication Profiling Change of authorization (CoA)	Cisco IOS® Software Release 15.0(1)SE2
Cisco Catalyst 3000 Series Switches	Cisco Catalyst 3560, 3560-E 3750, 3750-G, and 3750-E Series Switches	Basic identity features 802.1X authentication Profiling Change of authorization (CoA) IOS Device Sensor Security-group eXchange Protocol (SXP)	Cisco IOS Software Release 15.0(1)SE2
	Cisco Catalyst 3560-X and 3750-X Series Switches	Basic identity features 802.1X authentication Profiling Change of authorization (CoA) IOS Device Sensor MACSec 802.1AE Security-group eXchange Protocol (SXP)	Cisco IOS Software Release 15.0(1)SE2
Cisco Catalyst 4500 Series Switches	Cisco Catalyst 4500 Supervisor Engine 7-E and Supervisor Engine 7L-E	Basic identity features 802.1X Authentication Profiling Change of authorization (CoA) IOS Device Sensor MACsec 802.1AE Security-group eXchange Protocol (SXP)	Cisco IOS XE Software Release 3.3.0SG
	Cisco Catalyst 4500 Supervisor Engine 6-E and Supervisor Engine 6L-E	Basic identity features 802.1X authentication Profiling Change of authorization (CoA) IOS Device Sensor Security-group eXchange Protocol (SXP)	Cisco IOS Software Release 15.0(1)SG2
Cisco Wireless LAN Controller (WLC)	Cisco 5500 Series Wireless Controller Cisco 2500 Series Wireless Controller Cisco Wireless Services Module 2 (WiSM2) Cisco Wireless LAN Controller Module 2 (WLCM2)	Basic identity features 802.1X authentication Profiling Change of authorization (CoA) Device Sensor Lite Security-group eXchange Protocol (SXP)	Cisco Unified Wireless Network Software Release 7.2.110.0
Cisco Catalyst 6500 Switches	Cisco Catalyst 6500 Supervisor Engine 32 and Supervisor Engine 720	Basic identity features 802.1X authentication Profiling Change of authorization (CoA) Security-group eXchange Protocol (SXP)	Cisco IOS Software Release 12.2(33)SXJ2
Security Group Access (SGA) Enforcement			
Cisco Catalyst 6500 Series Switches	Cisco Catalyst 6500 Supervisor Engine 2T	SXP, SGT, and Security Group Access Control List (SGACL) enforcement MACsec 802.1AE Security Group name download Subnet to SGT mapping	Cisco IOS Software Release 15.0(1)SY1

Component	Hardware	Features Tested	Software Release
Cisco Nexus® 7000 Series Switches	All Cisco Nexus 7000 Series line cards and chassis**	SXP, SGT, SGACL enforcement, and MACsec	Cisco NX-OS Release 5.2.4
Cisco Nexus 5000 Series Switches	Cisco Nexus 5000 Series, including 5548P, 5548P, and 5596UP Switches	SXP, SGT, SGACL enforcement, and MACsec	Cisco NX-OS Release 5.1(3)N1(1)
Cisco ASR 1000 Series Aggregation Services Router	Cisco ASR 1000 Series Route Processor 1 and 2 (RP1/RP2), Cisco ASR 1000 Series Router Processor 1 or 2 (RP1/RP2), Cisco ASR 1001 Router, Cisco ASR 1002 Fixed Router, Cisco 1004, 1006, and 1013 Routers with • Embedded Services Processor (ESP) with 10, 20, or 40 Gbps • SPA Interface Processor (SIP) 10/40	SXP, Security Group Firewall (SG-FW)	Cisco IOS XE Software Release 3.5 or Cisco IOS Software Release 15.2(1)S
Cisco Integrated Services Router (ISR)	Cisco ISR 890, 1900, 2900, and 3900 Series	SXP, SG-FW	Cisco IOS Software Release 15.2(2)T
Supplicants			
Cisco AnyConnect® technology	Cisco AnyConnect Network Access Manager		Cisco AnyConnect Software Version 3.0.5075
Cisco Unified IP Phone	Cisco Unified IP Phones including 7910, 7940, 7960, 6900, 6910, 6920, 6940, and 6960 Series		Skinny Client Control Protocol (SCCP) Software, Version 9.2(1)SR1
Network Management Applications			
Cisco LAN Management System (LMS)			Cisco Prime LAN Management Solution 4.1 or 4.2
Cisco Prime Network Control System (NCS)			Cisco Prime Network Control System 1.1

Note: In order to support Security Group Access (SGA) features, the image needs to be crypto image (K9). In order to support SGA (including SGT and SGACL) with Cisco Catalyst 6500 Series Switch Supervisor Engine 2T, the Supervisor Cisco IOS Software image needs to be Advanced IP Services or Enterprise Advanced. SGACL is not available with IP Base at the time of this publication.

**Cisco Nexus 7000 F-Series line cards do not support MACsec 802.1AE.

Appendix A: References

Cisco TrustSec System:

- http://www.cisco.com/go/trustsec
- http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

Device Configuration Guides:

Cisco Identity Services Engine User Guides:
http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

For more information about Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software releases, please refer to following URLs:

- For Cisco Catalyst 2900 series switches:
  http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 3000 series switches:
  http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 3000-X series switches:
  http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 4500 series switches:
  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 6500 series switches:
  http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html
- For Cisco ASR 1000 series routers:
  http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html
- For Cisco Wireless LAN Controllers:
  http://www.cisco.com/en/US/docs/wireless/controller/7.0MR1/configuration/guide/wlc_cg70MR1.html