Current Technologies
Computer Learning Centers

+1 (219) 764-3800
6210 Central Ave, Portage IN
sales@ctclc.com
www.ctclc.com

Cisco Partner
Platinum Learning

WHERE GREAT TRAINING HAPPENS EVERYDAY!

Cisco TrustSec with SGT Segmentation Across Wired, Wireless, and SD-WAN Including Policy Enforcement by SGFW and Cisco ISE Policy Management

Cisco TrustSec with SGT Segmentation Across Multi-Domain Networks (Campus, Data Center, SD-WAN, SGFW, Remote VPN Sites) Across Wired, Wireless, and SD-WAN, Including Firewall Enforcement and Cisco ISE Policy Management

In this 5-day Cisco TrustSec and SGT-Based Segmentation is easiest to teach when the class moves from core concepts into repeated design-configure-validate cycles across wired, wireless, and SD-WAN, then finishes with centralized policy governance and third-party firewall enforcement. Below is a detailed multi-day outline with aligned labs, focused on how Security Group Tags (SGTs) are assigned, propagated, and enforced, and how Cisco ISE and Security Group Firewalls (SGFWs) work together for consistent unified policy across the Mutli-domain network.

Why Attend with Current Technologies CLC

- Our Instructors are in the top 10% rated by Cisco
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs run up to Date Code for all our courses

Course Duration
5 days
Course Price
$4,295.00 or TBA CLCs
Methods of Delivery
- Instructor Led
- Virtual ILT
- On-Site

Objectives

By the end of the course, students will be able to design and implement end-to-end SGT assignment and propagation, validate enforcement at multiple points in the network, troubleshoot TrustSec-related issues, and centrally manage policy in Cisco ISE while extending enforcement to Security Group Firewalls.

Who Should Attend

- **Network Security Engineers:** Those responsible for implementing and managing network access controls (NAC), security policies, and segmentation.
- **Network Architects & Designers:** Professionals designing secure campus and data center networks using software-defined segmentation.
- **Cisco ISE Administrators:** Individuals focusing on Cisco Identity Services Engine (ISE) for policy management and Security Group Tag (SGT) assignment.
- **System Administrators & IT Managers:** Professionals aiming to enhance network security and implement compliance-based access control.
- **IT Professionals tasked with Compliance:** Those needing to meet industry standards like PCI (Payment Card Industry) through rigorous network segmentation.
- **CCNP Security / CCIE Security Candidates:** Those preparing for Cisco certifications that require knowledge of TrustSec concepts (SGT, SGACL, SXP).
- **Network Support Engineers:** Those who need to troubleshoot security policies and access issues

Prerequisites

- A good understanding of security basics.
- Familiarity with general networking concepts and infrastructure.
- Experience with Cisco equipment (routers, switches, ASA firewalls, and ISE)

OUTLINE

Module 1: TrustSec Fundamentals and SGT Architecture

- TrustSec purpose in Zero Trust Networks (ZTN) and micro-segmentation for real networks, such as separating finance endpoints from general users without relying on IP subnets.
- SGT Identity Model, Classification, Propagation, Tag lifecycle, and the difference between classification and enforcement
- TrustSec Policy Enforcement
- SGT Control Plane Components: ISE, TrustSec devices and PxGrid Consumers
- TrustSec SGT Propagation Methods: Inline tagging (SGT over Ethernet), SXP, and IP-to-SGT mapping.
- Policy Model overview: Security Group ACLs (SGACLs), egress vs ingress enforcement, and policy matrix logic
- Cisco TrustSec/SGTs in Wireless Meraki Networks
- Cisco TrustSec/SGTs in Multi-Domain Networks with SD-WAN
- Cisco TrustSec Site with Policy via Firewalls
- Cisco TrustSec Design and Planning Process

Lab 1: Environment Validation and Baseline Access

- Verify lab topology, ISE health, device reachability, and time sync.
- Capture baseline traffic flows before segmentation.

Lab 2: SGT Creation and Policy Matrix Foundation in ISE

- Define a business-aligned SGT set (example: Employees, Contractors, Printers, Servers, Guests).
- Build a starter matrix with permit and deny rules.
- Publish and confirm policy distribution readiness.

Module 2: SGTs and Wired TrustSec

- Wired classification approaches: 802.1X, MAB, dACL fallback, and static SGT assignment.
- Wired TrustSec/SGT Configuration Example
- TrustSec device roles: access switch, distribution, and enforcement points.
- Inline tagging on TrustSec capable switches and how tags traverse trunks.
- SXP in TrustSec networks, for legacy or non-tagging devices, including mapping domains and peer roles.
- Wired SGACL enforcement using SGACLs with examples that mirror customer needs, such as allowing Employees to reach Servers on app ports only.
- Troubleshooting methodology: policy download, tag visibility, and flow evaluation.

Lab 3: Wired 802.1X Classification with Dynamic SGT Assignment

- Configure switch access port for 802.1X with ISE.
- Assign SGTs based on User group.
- Validate Authorization results and Tag assignment from switch and ISE perspectives.

Lab 4: Inline Tagging and End-To-End Propagation Validation

- Enable TrustSec on uplinks and trunks.
- Verify SGT propagation across access to distribution.
- Verify Tags in transit or use show and packet capture tools to confirm Tags in transit.

Lab 5: Wired SGACL Enforcement
- Apply SGACL matrix to enforcement switch.
- Test permitted and denied flows with on-box counters.
- Demonstrate least-privilege behavior change by adjusting one rule in ISE and republishing.

Module 3: SGTs and TrustSec Wireless
- Wireless identity and SGT assignment options: WLAN-level SGT, ISE authorization rules, and posture-based tagging.
- Meraki Adaptive Policy
- Configuring TrustSec for Wireless Network Access with Cisco ISE and WLC
- Integrating Meraki with ISE and Adding Wireless Network Devices to ISE
- Identity Contextual Information in ISE
- Authorization Results for Wireless Identities
- Wireless Network Segmentation Models using SGTs
- Authentiation and Authorization Policy for Wireless Identities
- Wireless Roaming Options.
- Validating Wireless TrustSec Flow
- Wireless SGT Configuration and Verification Example with WLC and ISE
- How tags are carried from WLC to the wired network and where enforcement should occur.

Lab 6: WLAN Integration with ISE for SGT Assignment
- Join WLC to ISE, enable RADIUS and TrustSec on the WLAN.
- Create authorization profiles for multiple wireless roles.
- Validate client onboarding and SGT assignment.

Lab 7: Wireless-To-Wired Propagation and Enforcement
- Verify tags passed from wireless controller to upstream switch.
- Enforce SGACLs at the correct point (controller vs distribution switch).
- Test multi-role clients and confirm policy outcomes.

Module 4: Profiling and Policy Management with ISE
- Profiling Basics
- Profiler Architecture
- Profiler Scale
- Additional Services
- ISE Profiling
- Troubleshooting ISE Profiling

Lab 8: Policy Management with ISE
- Author SGACLs and publish to enforcement nodes
    - Create “Employees to Servers”, “Guests to Internet Only”.
    - Push policy and confirm download/sync.
- Policy staging and rollback
    - Use monitor-only, then enforce.
    - Roll back and validate safety controls.

Lab 9: Security Matrix Policy Management with ISE
- Create a scalable SGT catalog and matrix
    - Build a structured tag scheme by persona and asset class.
    - Export/import SGACM for version control.

- Validate operational dashboards
    - Use ISE and switch telemetry to confirm policy health.

Module 5: TrustSec Multi-Domain Networks with SD-WAN, Data Center, Meraki, IaaS, Non-Fabric/Fabric Campus, SGFW and Remote VPN Sites

- Deploying TrustSec Multi-Domain SD-WAN with Meraki Sites and Campus/Catalyst Sites
    - SGT propagation into SD-WAN fabric: where tags are assigned at branch and how they are preserved across overlay.
    - Identity-Based segmentation in SD-WAN vs traditional VRF segmentation, and when to combine them.
    - Policy enforcement points: Branch edge, Policy Service nodes, and Data Center Edges.
    - Visibility and troubleshooting for Tag-based SD-WAN policies.
- TrustSec in Branch Network
- TrustSec in SD-Access Campus Network
- TrustSec Multi-Domain with Campus and Branch
- TrustSec Multidomain Network with Data Center (ACI)
- TrustSec Multidomain with IaaS and Data Center
- TrustSec Multidomain Network with Remote VPN
- TrustSec Network with Security Group Firewall and SGT Anomaly Detection (Threat Detection and Response)

Lab 10: Multidomain TrustSec Topology

- Branch SGT Classification and Mapping into SD-WAN Policies
    - Assign SGTs at branch access (wired or wireless) and confirm mapping into SD-WAN edge.
    - Configure SD-WAN data policies referencing SGTs or IP-to-SGT mappings.
    - Validate tag-aware forwarding decisions.
- SD-WAN Enforcement and Policy Tuning
    - Test traffic between branch roles and data center roles.
    - Modify an ISE matrix rule and observe SD-WAN edge behavior after policy refresh.
- Demonstrate coordinated segmentation across campus and WAN.

Module 6: Troubleshooting TrustSec

- Troubleshooting Methodology
- Troubleshooting Trustsec Authentication, Classification, Propagation, Enforcement and SXP
    - Authentication/authorization errors in ISE.
    - SGT not assigned or wrong SGT assigned.
    - CTS handshake/authentication between devices failing.
    - SXP adjacency down or stale bindings.
    - Policy not downloading or out of sync.
    - Enforcement anomalies (traffic still passes/blocked unexpectedly).
    - Third-party enforcement mismatch (pxGrid feed, group mapping).
    - ISE live logs and session detailsl, for tag assignment and authorization outcomes
    - Monitoring and reporting.
    - Switch/router CTS state, role, env-data, counters.
    - Network device CTS/SGACL counters and telemetry.
    - SXP neighbors, bindings, and timers.
- TrustSec Monitor Mode
- Common Issues
- Getting Other/Cisco/TAC Support

Lab 11: Troubleshooting TrustSec

- Show different troubleshooting methods and scenarios such as:

- Wrong SGT assignment
  - Inject an authorization rule error.
  - Use ISE logs to find root cause and correct it.
- CTS propagation failure
  - Break CTS link authentication between access and distribution.
  - Restore trust, verify SGT propagation and counters.
- SXP adjacency and binding issues
  - Introduce a timer/ACL issue preventing SXP.
  - Resolve and verify correct tag exchange.
- Palo Alto context/policy mismatch
  - Simulate pxGrid feed loss or wrong mapping.
  - Re-establish feed and fix policy object alignment.