**This document has been superseded. The one current document encompassing capability and scale can be found at: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/policy-platform-capability-matrix.pdf

# Cisco Group Based Policy Release 6.5 System Bulletin

## (inclusive of TrustSec Software-Defined Segmentation)

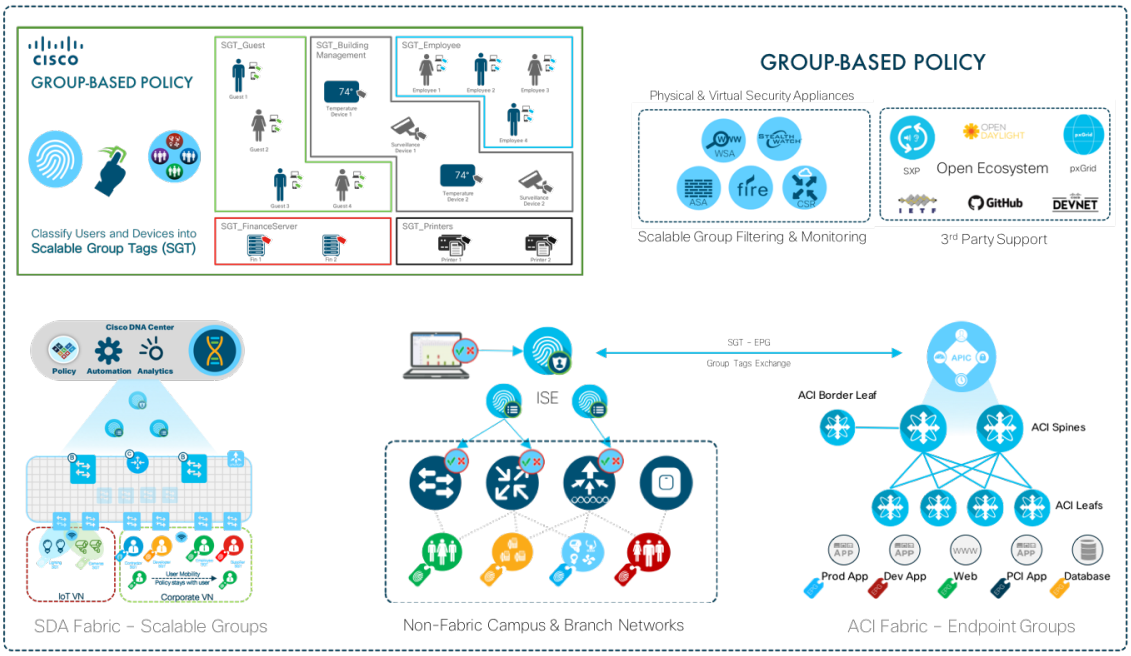
### Introduction

Network segmentation is essential for protecting critical business assets. Cisco Group Based Policy balances the demands for agility and security without the operational complexity and difficulty of deploying into existing environments seen with traditional segmentation. Endpoints are classified into groups that can be used anywhere on the network in both fabric and non-fabric Cisco environments. This allows us to decouple the segmentation policies from the underlying network infrastructure.

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. Scalable Groups (IETF), aka Security Groups, can indicate the role of the system or person, the type of application and server hosts, the purpose of an IoT device, or the threat-state of a system, which IP addresses alone cannot. These scalable 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.

Group Based Policy is much easier to enable and manage than VLAN-based segmentation and avoids the associated processing impact on network devices. Figure 1 shows the breadth in use of Group Based Policy in Enterprise networks. From the Software Defined Access Fabric with micro-segmentation to the traditional network with TrustSec® technology to the ecosystem with pxGrid carrying GBP information and interoperability with shared groups in the ACI data center and into the cloud (future), Group Based Policy protects network assets and limits the spread of malware end to end.

Figure 1. Group Based Policy in the Enterprise Network




Cisco DNA Center or 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.

Group Based Policy technology is embedded in Cisco switches, routers, wireless LAN and security products and is the foundation for using a Network as an Enforcer. Segmentation enforcement capabilities mitigate risk by reducing attack surface through better segmentation, whilst also increasing operational efficiency and making compliance goals easier to achieve.

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 Group Based Policy (aka TrustSec) can be quickly enabled.

## Summary of New Capabilities

The Cisco Group Based Policy 6.5 release continues to validate three major deployment scenarios. All three of these 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 platforms were tested in this release:

- Cisco Catalyst 9200 Series Switches
- Cisco Catalyst 9500H Series Switches
- Cisco Catalyst 9600 Series Switches
- Cisco Industrial Ethernet 3400 Switches

## New Cisco Group-Based Policy Features Validated in Release 6.5

- IPv6 SGACL Enforcement on 3850 IOS-XE 16.12.1, 4500 IOS-XE 03.10.01.E.165 EARLY DEPLOYMENT [PROD IMAGE] ENGINEERING NOVA_WEEKLY BUILD, 4507 15.2. Customers can now enforce the same group-based policy (i.e., SGACLs) on IPv6 traffic in their networks. Whether you have embraced and deployed IPv6 as an organization, IPv6 traffic is traversing your networks. You can now implement security measures to restrict unauthorized resource access and segmentation for IPv6.
- CMD Tagging Exemption for L2 Control Plane Protocols in IOS-XE 16.10.2 (ASR1K, ISR, and CSR1KV) to enable interoperability with the Nexus 7000 leveraging F3 Linecards. This addresses the limitation on the Nexus 7000 F3 linecards that prevents CMD tagged L2 control plane protocols on CTS enabled interfaces. With this new functionality, the IOS-XE devices will exempt key Layer-2 control plane protocols that are responsible for creating and maintaining certain operational states between devices connected through CTS links. These L2 protocols are exempted from SGT CMD tagging when using this functionality.
- SDA-ACI Phase 1 - ISE-ACI Bulk API Update. The interoperability for SDA and non-fabric TrustSec now supports up to 64,000 mapping being shared and transferred to ACI border leafs at the following transactions per second; Nexus 9000 EX leafs at (100/sec) & Nexus 9000 FX leafs at (250/sec). Additionally, interoperability with Cisco DNAC Software Defined Access (SDA) to ACI via ISE was part of the validation. See components used in this validation in Figure 1 below.

Figure 1. SDA-ACI Integration Phase 1 Test Summary

| Model No. | Hardware/Software Platform | SW Ver | Role |
|---|---|---|---|
| DN1-HW-APL | DNAC Appliance | 1.2.10 | DNAC Controller |
| ISE-VM-K9 | Cisco Identity Services Engine Virtual Appliance | 2.4 P6 | Identity Management RADIUS server |
| APIC-Server-M2 | Cisco Application Policy Infrastructure Controller (APIC) | 3.2 (4e) | ACI Controller |
| N9K-C9504 | Cisco Nexus 9500 Series Switch | 13.2 (4e) | ACI Spine node |
| N9K-C9372PX | Cisco Nexus 9000 Series Switch | 13.2 (4e) | ACI Leaf node |
| C9500-24Q | Cisco Catalyst 9500 Series Switch | 16.9.2s | SDA Border/CP |
| C9300-48U | Cisco Catalyst 9300 Series Switch | 16.9.2s | SDA Edge |

New Cisco Software Releases Validated in release 6.5:

- Cisco Wireless LAN AireOS 8.8 & 8.9

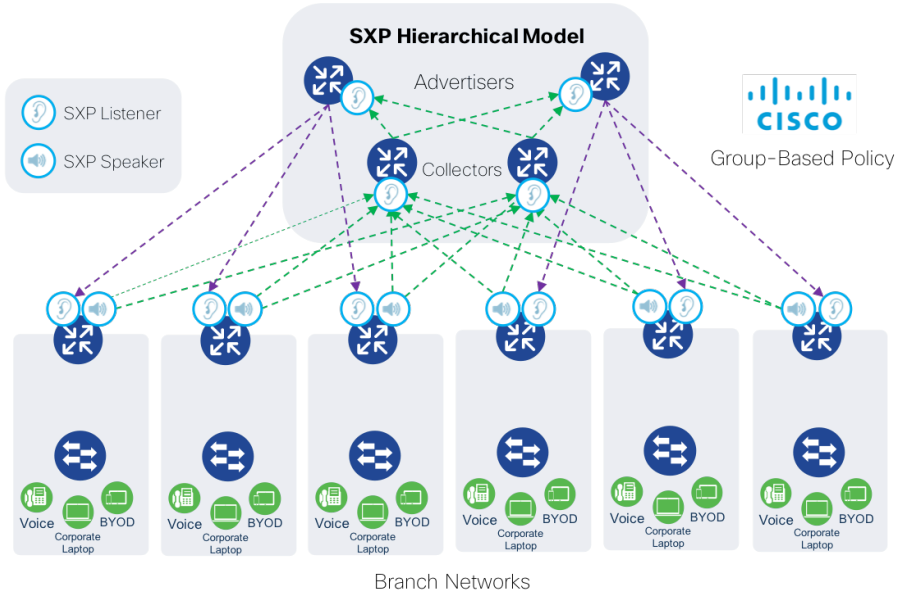
## New Cisco Group-Based Policy Deployment Scenarios Validated in Release 6.5

- ASR1K SXP Hierarchical Model. In this new SXP architecture the deployment leveraging Cisco ASR 1000 Series routers as the SXP reflectors act as both SXP advertisers and SXP collectors. The configuration leverages two

advertisers and collectors to create a scalable and highly available deployment. This utilizes uni-directional SXP connections as oppose to bi-directional. With this new configuration the deployment can achieve 1800 peer connections and 750,000 mappings on the ASR 1000s. This model is shown in figure 2.

- Flexible NetFlow Export of SGTs and Cisco StealthWatch Validation. This included validation of the successful export of SGT fields in the flow data in NetFlow configurations via StealthWatch. Verification of Cisco Rapid Threat Containment (RTC), whereby StealthWatch upon anomaly detection or admin intervention triggers an Adaptive Network Control (ANC) action in ISE to dynamically change to a Quarantine/unquarantined state with SGTs.
- Policy Distribution Scale Testing to 1000 NAD Enforcement Devices
  - Solution Components IOS-XE / Polaris 16.8.1 and ISE 2.6 with the following testing performed:
    - Trigger CoA after the following changes and check behavior between device and ISE:
    - RBACL-ACE change
    - RBACL change
    - Multiple SGT creation and deletion
    - Add SGT and an associated RBACL
    - RBACL ACE update and temporarily disrupt the download by flapping the link between ISE and the device
    - Modify RBACL referenced in multiple cells
    - Block UDP ports from/to device during CoA
    - Verify multiple 'cts refresh policy' operations
    - Multiple refresh PAC, Env data and RBACL
    - Clear CTS PAC and Env-data
    - Disable/re-enable enforcement to check CoA still operates

Figure 2. SXP Hierarchical Model Diagram




### Summary of current Cisco Group Based Policy Features Validated in 6.5

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

## Product Components and Features

Tables 1 through 3 summarize the platforms and features that are validated in Cisco Group Based Policy / TrustSec testing. The list is also available at: cisco.com/go/TrustSec.  It is current with the TrustSec 6.5 validation program.

Table 1 provides cross-platform group-based policy exchange interoperability testing results.  Application Centric Infrastructure (ACI) and Group Based Policy 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, Beryllium, or Carbon release) working together in the Data Center.

**Table 1.** 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 13.2 (4e) | EndPoint Group – Security Group Mappings via TrustSec-ACI policy and data plane exchange | Cisco ISE 2.4 Patch 6 ACI API |
| Cisco Application Policy Infrastructure Controller – Data Center | Cisco APIC-DC | APIC-DC 3.2 (4e) Policy plane; | | |
| Open Daylight SDN controller | ODL SDN | Lithium, Beryllium, Carbon | SGT via SXP v4 | Cisco ISE 2.1- SXP v4<br>Nexus 7000 7.3- SXP v3<br>ASA 9.6.1- SXP v3 |
| Open Daylight SDN controller | ODL SDN | Nitrogen | IPv4, IPv6 SXP Peering | Cisco ISE 2.4<br>ASR 1001-X IOS XE 16.5.1b<br>CSR 1000v IOS XE 16.6.3<br>Cat 6500 IOS 15.4(1)SY2<br>Cat 3850 IOS 3.6.8E |

In Tables 2 and 3, Cisco Group Based Policy 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.

Cisco DNA Premier is a simple and economical solution for deploying branch and campus switches and wireless access points. It offers an uncompromised user experience in a highly secure and feature-rich access infrastructure and simplify the licensing requirements for Group Based Policy deployment. Cisco DNA Advantage requires Network Advantage hardware.

Solution-level validated versions listed in the tables below may not always represent the latest available platform version and feature set. Releases may encounter issues in other subsystems and be deferred. For latest platform firmware version and feature set, refer to product release notes.

As an aid to deployment, products are grouped into Tier I, II, and III with regard to feedback on design and deployment. Tier I ① products have full Group Based Policy functionality with few caveats, and they are common components in successful deployments. Tier II ② products have full Group Based Policy functionality but there are some caveats involved in their deployment. Tier III ③ do not have full Group Based Policy functionality and support Classification and SXP based Propagation only. These products tend to be older with a less rich feature set and more caveats to consider when deploying. Security products are not listed in a tier. End of Sale Products are listed in Table 3.

VXLAN is supported on several platforms but not all are listed in the matrix pending review of solution test verification.

**Table 2.** Cisco Group Based Policy 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<br>*Services* |
|---|---|---|---|---|---|---|---|---|
| Cisco Catalyst® 2000 Series | Catalyst 2960-Plus Series ③ | 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 ③ | 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 ③ | 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-X Series ③ | 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 ③ | 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 3650 and 3850 Series ① | IP Base K9 & above or Cisco One Foundation & above | Cisco IOS XE 3.7.4E<br>3.6.8E<br>3.6.6E | Cisco IOS XE 3.6.4E | 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, Logging (3.6.6E)<br>*SGT Netflow v9* |
| | Catalyst 3650 and 3850 Series ① | IP Base K9 & above or Cisco ONE Foundation & above | Cisco IOS XE Denali 16.6.4 | 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, Monitor mode, Logging |
| | Catalyst 3850-XS Series ① | IP Base K9 & above or 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 [Note5]; SGT over MACsec | SGACL |
| | Catalyst 3560-CX Series ② | IP Base K9 | Cisco IOS 15.2(3)E | Cisco IOS 15.2(4)E | (L2 adjacent hosts only) Dynamic, IP to SGT (v4, v6), VLAN to SGT, Subnet to SGT | Speaker, Listener V4 | No | SGACL [Note16] |
| | Catalyst 3560-C/CG Series ③ | IP Base K9 | Cisco IOS 15.0(1)SE2 | Cisco IOS 15.2(2)E | (L2 adjacent hosts only) Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT | Speaker, Listener V4 | No | No |
| Cisco Catalyst 4500 Series | Catalyst 4500 E-Series Supervisor Engine 8-E and 8L-E ① | IP Base K9 & above or Cisco ONE Foundation & above | Cisco IOS XE 3.7.1E | Cisco IOS XE 3.6.0E<br>3.8.0E-Logging | Dynamic, IP to SGT (v4, v6), VLAN to SGT, Port to SGT, Subnet to SGT (Src & Dst), L3IF to SGT [Note12] | Speaker, Listener V4 | SGT over Ethernet; SGT over MACsec (See note 2 for supported line cards) | SGACL, Logging<br>*SGT Netflow v9* |
| | Catalyst 4500-X Series ① | IP Base K9 & above or Cisco ONE Foundation & above | Cisco IOS XE 3.6.3E<br>3.6.6 | Cisco IOS XE 3.5.1E<br>3.8.0E-logging | Dynamic, IP to SGT (v4,v6), VLAN to SGT, Port to SGT, Subnet to SGT (Src & Dst), L3IF to SGT [Note12] | Speaker, Listener V4 | SGT over Ethernet; SGT over MACsec | SGACL, Logging |

| 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<br>*Services* |
|---|---|---|---|---|---|---|---|---|
| Cisco Catalyst 4500 Series | Catalyst 4500 E-Series Supervisor Engine 7-E and 7L-E ② | IP Base K9 & above or Cisco ONE Foundation & above | Cisco IOS XE 3.7.1E | Cisco IOS XE 3.5.1E | Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT, L3IF to SGT, Port to SGT Note12 | Speaker, Listener V4 | SGT over Ethernet; SGT over MACsec (See note 2 for supported line cards) | SGACL, Logging [3.8.0E]<br>*SGT Netflow v9* |
| | Catalyst 4500 E-Series Supervisor Engine 6-E and 6L-E; ③ | IP Base K9 | Cisco IOS 15.1(1)SG | Cisco IOS 15.1(1)SG | Dynamic, IP to SGT Note12 | Speaker, Listener V4 | No | No |
| Cisco Catalyst 6500 Series | Catalyst 6500 Series Supervisor Engine 2T & Supervisor 6T ①<br>Catalyst 6807-XL ① | 2T: IP Base K9<br>6T: IP Services K9 | Cisco IOS 15.4(1)SY2<br>15.2(1)SY05 15.2(1)SY0a Sup 6T Cisco IOS 15.4(1)SY1 | Cisco IOS 15.2(1)SY0a Sup 6T Cisco IOS 15.4(1)SY1 | 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; SGT over VXLAN | SGACL (IPv4, IPv6), Monitor mode, Logging<br>*SGT Caching*<br>*SGT Netflow v9* |
| | Catalyst 6880-X, 6840-X (incl 6816-X-LE), and 6800ia ① | IP Base K9 & above or Cisco ONE Foundation & above | Cisco IOS 15.2(2)SY2, 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), Monitor mode, Logging<br>*SGT Caching*<br>*SGT Netflow v9* |
| | Catalyst 6500 Series Supervisor Engine 32 and 720 ③ | IP Base K9 | Cisco IOS 12.2(33)SXJ2 | Cisco IOS 15.1(2)SY1 | Dynamic, IP to SGT | Speaker, Listener V4 | No | No |
| Cisco Catalyst 9200 Series | Cisco Catalyst 9200 Series | Network Advantage | Cisco IOS XE 16.12.2 | Cisco IOS XE 16.12.2 | Dynamic, IP to SGT, VLAN to SGT, Port to SGT, Subnet to SGT, L3IF to SGT | Speaker, Listener V4 | SGT over Ethernet SGT over VXLAN | SGACL V4, V6 (Note 17), Monitor mode, Logging<br>*SGT Netflow v9* |
| Cisco Catalyst 9300 Series | Catalyst 9300 Series ① | Network Advantage | Cisco IOS XE Everest 16.6.2 | Cisco IOS XE Everest 16.6.2 SMU (Note 10) 16.8.1 | Dynamic, IP to SGT, VLAN to SGT, Port to SGT, Subnet to SGT, L3IF to SGT | Speaker, Listener V4 | SGT over Ethernet SGT over VXLAN | SGACL V4, V6 (Note 17), Monitor mode, Logging<br>*SGT Netflow v9* |
| Cisco Catalyst 9400 Series | Catalyst 9400 Series Supervisor Engine-1 & -1XL ① | Network Advantage | Cisco IOS XE 16.6.2, 16.8.1 | Cisco IOS XE Everest 16.6.2 SMU (Note 10) 16.8.1 | Dynamic, IP to SGT, VLAN to SGT, Port to SGT, Subnet to SGT, L3IF to SGT | Speaker, Listener V4 | SGT over Ethernet SGT over VXLAN | SGACL V4, V6 (Note 17),, Monitor mode, Logging<br>*SGT Caching*<br>*SGT Netflow v9* |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Cisco Catalyst 9500 Series | Catalyst 9500 Series ① | Network Advantage | Cisco IOS XE Everest 16.6.2 SMU | Cisco IOS XE Everest 16.6.2 SMU (Note 10) | Dynamic, IP to SGT, VLAN to SGT, Port to SGT, Subnet to SGT, L3IF to SGT | Speaker, Listener V4 | SGT over Ethernet SGT over VXLAN Note13 | SGACL V4, V6 (Note 17), Monitor mode *SGT Caching* *SGT Netflow v9* |
| | Catalyst 9500H Series | Network Advantage | Cisco IOS XE 16.12.2 | Cisco IOS XE 16.12.2 | Dynamic, IP to SGT, VLAN to SGT, Port to SGT, Subnet to SGT, L3IF to SGT | Speaker, Listener V4 | SGT over Ethernet SGT over VXLAN | SGACL V4, V6 (Note 17), Monitor mode, Logging *SGT Netflow v9* |
| Cisco Catalyst 9600 Series | Cisco Catalyst 9600 Series | Network Advantage | Cisco IOS XE 16.12.2 | Cisco IOS XE 16.12.2 | Dynamic, IP to SGT, VLAN to SGT, Port to SGT, Subnet to SGT, L3IF to SGT | Speaker, Listener V4 | SGT over Ethernet SGT over VXLAN | SGACL V4, V6 (Note 17), Monitor mode, Logging *SGT Netflow v9* |
| Cisco Connected Grid Router Series | CGR 2010 Series ② | - | 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 |
| **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 Connected Grid Switch Series | CGS 2500 Series ③ | - | 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 ③ | 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 | (L2 adjacent hosts only) Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT | Speaker, Listener V4 | No | No |
| | IE 3400 Series | Network Advantage | Cisco IOS-XE 16.11.1 | Cisco IOS-XE 16.11.1 | Dynamic, IP to SGT, VLAN to SGT, Port to SGT, Subnet to SGT, L3IF to SGT | Speaker, Listener V4 | SGT over Ethernet SGT over VXLAN | SGACL V4, V6 (Note 17), Monitor mode, Logging *SGT Netflow v9* |
| | IE 4000 Series ② | LAN Base; IP Services for SGToE & SGACL | Cisco IOS 15.2(4)EA, 15.2(5)E | Cisco IOS 15.2(5)E | (L2 adjacent hosts only) Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT | Speaker Note11 V4 | SGT over Ethernet | SGACL Note16 |
| | IE 5000 Series ② | LAN Base; IP Services for SGToE & SGACL | Cisco IOS 15.2(2)EB1, 15.2(5)E | Cisco IOS 15.2(5)E1 | (L2 adjacent hosts only) Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT | Speaker Note11 V4 | SGT over Ethernet on1G & 10G interfaces only | SGACL Note16 |
| Cisco Access Points | 1700, 2700, 3700, AP Series (Wave 1) ① | - | Cisco AireOS 8.9 | Cisco AireOS 8.9 | Dynamic | Speaker, Listener V4Note6 | SGT over Ethernet Note6 | SGACL |
| | 1815, 1830, 1850, 2800, 3800 AP Series (Wave 2) ① | - | Cisco AireOS 8.9 | Cisco AireOS 8.9 | Dynamic | Speaker, Listener V4Note6 | SGT over Ethernet Note6 | SGACL |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Cisco Wireless Controller Series | 8540 Series Wireless Controller ① | - | Cisco AireOS 8.9 | Cisco AireOS 8.9 | Dynamic | Speaker v2 | SGT over Ethernet | Supports AP SGACL in Centralized and Flex Connect mode) |
| | 5520 Series Wireless Controller ① | - | Cisco AireOS 8.9 | Cisco AireOS 8.9 | Dynamic | Speaker v2 | SGT over Ethernet | Supports AP SGACL in Centralized and Flex Connect mode) |
| | 3504 Wireless Controller ① | - | Cisco AireOS 8.9 | Cisco AireOS 8.9 | Dynamic | Speaker v2 | SGT over Ethernet (Centralized mode) | Supports AP SGACL in Centralized and Flex Connect mode) |
| | vWLC ① | - | Cisco AireOS 8.5 | Cisco AireOS 8.5 | Dynamic | Speaker v2 | | Supports APs in Flex mode only |
| | 5500 Series (5508,5520)<br>2500 Series (2504) ③ | - | Cisco AireOS 8.3.102.0, 7.6.130.0 | Cisco AireOS 7.6.130.0 | Dynamic | Speaker V2 | No | No |
| | 8500 Series (8540,8510) ③ | - | Cisco AireOS 8.3.102.0 (pre 8.4) | Cisco AireOS 8.1 | Dynamic | Speaker V2 | No | No |
| **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 Nexus® 7000 Series | Nexus 7000 with M3-Series modules ① | Base License NX-OS 6.1 and later | Cisco NX-OS 8.1(2), 8.1(1), 8.0(1)<br>7.3.2<br>7.3(0)D1(1) [logging, monitor mode],<br>7.2(0)D1(1) | Cisco NX-OS 8.0(1) | IP to SGT[1], Port Profile to SGT, VLAN to SGT[2], Port to SGT[2] Subnet to SGT[5] Note14 | Speaker, Listener<br>V4 | SGT over Ethernet[5];<br>SGT over MACsec;<br>SGT over VXLAN<br>[5]: F3 interoperability requires M3 'no propagate-sgt l2 control' command | SGACL,<br>Monitor mode & logging |
| | Nexus 7000 with M2-Series modules ② | Base License NX-OS 6.1 and later | Cisco NX-OS 8.1(1), 8.0(1)<br>7.3(0)D1(1) [Monitor mode & limited logging],<br>7.2(0)D1(1) | Cisco NX-OS 8.0(1) | IP to SGT[1], Port Profile to SGT, VLAN to SGT[2], Port to SGT[2] Subnet to SGT[5] Note14<br>[1]:FabricPath support requires 6.2(10) or later<br>[2] VPC/VPC+ support requires 7.2(0)D1(1) or later<br>[5] Subnet to SGT requires 7.3(0)D1(1) or later | Speaker, Listener<br>V4 | SGT over Ethernet[5];<br>SGT over MACsec<br>[5]: M2 cannot link to F3 module. | SGACL<br>Monitor mode & limited logging |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Nexus 7700 F-Series[Note4] modules ②<br>F3 modules do not support SGT tagging with other Cisco products unless these products support the SGT tagging exemption feature for Layer 2 protocols. M3 series support this by enabling 'no propagate-sgt l2-control' command. | Base License NX-OS 6.1 and later | Cisco NX-OS 8.1(1), 8.0(1) 7.3(0)D1(1), 7.2(0)D1(1) | Cisco NX-OS 8.0(1) | IP to SGT[1], Port Profile to SGT, VLAN to SGT[2], Port to SGT[2] Subnet to SGT[5] [Note14]<br>[1]:FabricPath support requires 6.2(10) or later<br>[2] VPC/VPC+ support requires 7.2(0)D1(1) or later<br>[5] Subnet to SGT requires 7.3(0)D1(1) or later | Speaker, Listener V4 | SGT over Ethernet[35];<br>SGT over MACsec[4]<br>[3]: F3 interfaces (L2 or L3) require 802.1Q or FabricPath<br>[4]: F2e (Copper) all ports; F2e (SFP) & F3 (10G)- last 8 ports; All others- no support<br>[5]: Not supported between F3 and either M2 or F2e | SGACL |
| Cisco Nexus 5000, 6000 Series | Nexus 6000/5600 Series ② | - | Cisco NX-OS 7.1(0)N1(1a) | Cisco NX-OS 7.0(1)N1(1) | (L2 adjacent hosts only) Port to SGT | Speaker V1 | SGT over Ethernet | SGACL [Note16] |
| | Nexus 5548P, 5548UP, and 5596UP ② | - | Cisco NX-OS 7.0(5)N1(1) | Cisco NX-OS 6.0(2)N2(6) | (L2 adjacent hosts only) Port to SGT | Speaker V1 [1]<br>[1]: FabricPath | SGT over Ethernet | SGACL [Note16] |
| **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**<br>———<br>***Services*** |
| Cisco Nexus 1000 Series | Nexus 1000V for VMware vSphere ② | Advanced license for SGToE/ SGACL support | Cisco NX-OS 5.2(1)SV3(3.1) [Logging] 5.2(1)SV3(1.3) | Cisco NX-OS 5.2(1)SV3 (1.1) | Dynamic (802.1x) [Note15], IP to SGT, Port Profile to SGT | Speaker, Listener v4 v1 (prior to 5.2(1)SV3(3.1) | SGT over Ethernet[Note9] | SGACL, Logging |
| | Nexus 1000VE Virtual Edge ② | Advanced license for SGACL support | Cisco NX-OS 5.2(1)SV5(1.1) | Cisco NX-OS 5.2(1)SV5(1.1) | Port Profile to SGT, IP to SGT | Speaker, Listener v4 | No | SGACL |
| Cisco Integrated Services Router (ISR) | 4000 Series ISR 4431, 4451-X, 4321, 4331, 4351 ① | IP Base/K9 for classify/ propagate, SGACL; Security/K9 for SG FW 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, Monitor mode & Logging<br>SG Firewall<br>———<br>*SGT based PBR*<br>*SGT Caching*<br>*SGT based QoS* |
| | ISRv ① | IP Base/K9 for classify/ propagate, SGACL | 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, Monitor mode & Logging |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 890, 1900, 2900, 3900 Series ② | IP Base/K9 for classify/ propagate; Security/K9 for SG FW enforcement | 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) ② | IP Base/K9 for classify/ propagate; Security/K9 for SG FW enforcement | 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* *SGT Netflow v9* |
| | SM-X Layer 2/3 EtherSwitch Module ② | IP Services/K9 | 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 | CSR 1000V ① | IP Base/K9 for classify/ propagate, SGACL; | Cisco IOS XE 16.6.3 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, Monitor mode & Logging |
| | Cloud Services Router 1000V Series (CSR) ② | IP Base/K9 for classify/ propagate; Security/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* *SGT Netflow v9* |
| **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 Aggreg-ation Services Router (ASR) | ASR 1004, 1006, 1013, 1001-X, 1002-X,1002-HX, 1006-X, and 1009-X ① | IP Base/K9 for classify/ propagate, SGACL; Security/K9 for SGFW enforce-ment | Cisco IOS XE 16.5.1b 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, Monitor mode & Logging SG Firewall *SGT based PBR* *SGT Caching* *SGT based QoS* |
| | 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) ② | IP Base/K9 for classify/ propagate; Security/K9 for enforce-ment | 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* *SGT Netflow v9* |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | ASR 1001-X and 1002-X ② | IP Base/K9 for classify/ propagate; Security/K9 for enforce-ment | 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<br>*SGT based PBR*<br>*SGT based QoS*<br>*SGT Caching*<br>*SGT Netflow v9* |
| Cisco Identity Services Engine | ISE 3515, 3595, 3415, and 3495 Appliance & VMware | Base<br>Plus for pxGrid | Cisco ISE 2.4, 2.3P1, 2.2, 2.1, 2.0, 1.4 | Cisco ISE 2.2 | Dynamic, IP to SGT, Subnet to SGT | Speaker, Listener V4 pxGrid | – | – |
| Cisco Adaptive Security Appliance | ASA 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 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)<br>*SGT based PBR* |
| | ASA 5525-X, 5545-X, 5555-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)<br>*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<br>*SGT based PBR* |

| | 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<br>*Services* |
|---|---|---|---|---|---|---|---|---|
| Cisco Firepower NGFW | Cisco Firepower 2100 | Firepower Threat Defense Base | Cisco Firepower System 6.2.1 | Cisco Firepower System 6.2.1 | - | pxGrid | SGT over Ethernet | SG Firewall (src SGTs only)<br>*SGT based PBR* |
| | FP 4100<br>FP 9300 | - | Cisco FXOS 2.0.1.37<br>Cisco ASA 9.6.1 | Cisco FXOS 2.0.1.37<br>Cisco ASA 9.6.1 | Remote Access VPN (IPsec, SSL-VPN) | Speaker, Listener V3 | SGT over Ethernet | SG Firewall<br>*SGT based PBR* |
| | Cisco Firepower Threat Defense Firepower 4100 & 9300 | Firepower Threat Defense Base | Cisco Firepower System 6.1.0 | Cisco Firepower System 6.1.0 | - | pxGrid | SGT over Ethernet | SG Firewall (src SGTs only)<br>*SGT based PBR* |
| | FTDv | Threat & Apps (TA) | Cisco Firepower System 6.2.0.2 | Cisco Firepower System 6.2.0.2 | - | pxGrid | SGT over Ethernet | SG Firewall (src SGTs only)<br>*SGT based PBR* |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Cisco Industrial Security Appliance | ISA 3000 Series | - | Cisco ASA 9.6.1 | Cisco ASA 9.6.1 | Remote Access VPN (IPsec, SSL-VPN) | Speaker, Listener<br>V3 | SGT over Ethernet | SG Firewall (IPv4, IPv6)<br>*SGT based PBR* |

**Table 3.** End of Sale Group Based Policy Platform Support Matrix
(https://www.cisco.com/c/en/us/products/eos-eol-listing.html )

| **Eos 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**<br>*Services* |
|---|---|---|---|---|---|---|---|---|
| Cisco Catalyst® 2000 Series | Catalyst 2960-S and 2960-SF Series | LAN Base K9 | Cisco IOS 15.0(2)SE Note1<br>15.2(2)E | Cisco IOS 15.2(2)E3 | Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT | Speaker<br>V4 Note1 | 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 | (L2 adjacent hosts only) Dynamic, IP to SGT, VLAN to SGT | Speaker, Listener<br>V2 | No | No |
| | Catalyst 3560-X and 3750-X Series | IP Base K9 | Cisco IOS 15.2(2)E3 | Cisco IOS 15.2(2)E1 | (L2 adjacent hosts only) Dynamic, IP to SGT (prefix must be 32), VLAN to SGT, Port to SGT (only on switch to switch links) | Speaker<br>V4 | SGT over Ethernet; SGT over MACsec (with C3KX-SM-10G uplink); SGT over VXLAN | SGACL Note16<br>(maximum of 8 VLANs on a VLAN-trunk link) |
| Cisco Catalyst 4500 Series | Cisco Catalyst 4948 Series | IP Base K9 | Cisco IOS<br>15.1(1)SG | Cisco IOS 15.1(1)SG | Dynamic, IP to SGT | Speaker, Listener<br>V4 | No | No |
| **EoS 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**<br>*Services* |
| Cisco Nexus® 7000 Series | Cisco Nexus 7000 F2-Series*** modules | Base License NX-OS 6.1 and later | Cisco NX-OS 7.3(0)D1(1),<br>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]<br>[1]:FabricPath support requires 6.2(10) or later<br>[2] VPC/VPC+ support requires 7.2(0)D1(1) or later<br>[5] Subnet to SGT requires 7.3(0)D1(1) or later | Speaker, Listener<br>V3 | SGT over Ethernet;<br>SGT over MACsec[4]<br>[4]: M & F2e (Copper-) all ports; F2e (SFP) - last 8 ports; All others- no support | SGACL |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Cisco Wireless Controller | 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 |
| | Wireless Services Module 2 (WiSM2) | - | Cisco AireOS 8.3.102.0, 7.6.130.0 | Cisco AireOS 7.6.130.0 | Dynamic | Speaker V2 | No | No |
| | Flex 7500 Series Wireless Controller | - | Cisco AireOS 8.3.102.0, 7.6.130.0 | Cisco AireOS 8.3 | Dynamic | Speaker V2 | No | No |
| Cisco Aggreg-ation Services Router (ASR) | ASR 1001, 1002 | IP Base/K9 for classify/ propagate; Security/K9 for enforce-ment | 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<br>*SGT based PBR (1000 RP2)*<br>*SGT based QoS*<br>*SGT Caching*<br>*SGT Netflow v9* |
| Cisco Identity Services Engine | ISE 3315, 3355, 3395, Appliance | | Cisco ISE 1.0, 1.1, 1.2 | | | | – | – |
| Cisco Adaptive Security Appliance | ASA 5510, 5520, 5540, 5550 | - | 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[Note3], 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)<br>*SGT based PBR* |
| | ASA 5512-X, 5515-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)<br>*SGT based PBR* |
| **EoS 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**<br>***Services*** |
| Cisco Fire POWER | FirePOWER 7000 and 8000 Series | Threat & Apps (TA) | Cisco FireSIGHT 5.4.0.6, 5.4.1.5, 6.0.1.1, 6.2 | Cisco FireSIGHT 5.4.0.6, 5.4.1.5, 6.0.1.1 | - | - | SGT over Ethernet | - |

**Notes**

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

2: 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.

3: Cisco ASA 5505 does not support releases after 9.2.

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

5: Use of inline tagging with LACP requires future IOS XE Denali or IOS 3.7 release (CSCva22545)

6: For SXP support, AP must run in FlexConnect Mode

7: With IPv6 support, DGT can be IPv4.

8: 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.

9: When inline tagging (SGToE) is enabled with the VIC 12xx and VIC 13xx, packet processing is handled at the processor level which will attribute to lower network I/O performance. An alternative solution is to use Intel adaptors.

10: IOS XE Everest 16.6.2 SMU is required for ISE BYOD, Guest, and Posture features. See ISE Compatibility Matrix: https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-device-support-tables-list.html

11: The IE 4000 and IE 5000 platforms perform similarly to the Catalyst 3560-X and 3750-X platforms in the reliance on IP Address, MAC Address, and physical port/VLAN of the device, learned via dot1x or MAB or IP Device Tracking (IPDT). These devices cannot use information learned via SXP for either enforcement or tag propagation as the device is not directly attached. SXP v4 is supported in Speaker mode only.

12: Catalyst 4500 Series Release 3.9 and later, with the introduction of VRF, an SVI is needed for L3 lookup to derive SGT for switched traffic, and a SVI is also needed on the VLAN for the derivation of source group for L2 traffic.

13: C9500 as a border node does not currently support transferring the tag from the VXLAN header to the CMD field for inline tagging. C9500 outside the fabric supports inline tagging

14: The N7K must have an SVI on the VLAN if the mappings reside in the VRF. If N7K is L2 only, create an SVI without IP to be able to utilize the mappings from the VRF. SVI is not required if entered into the VLAN.

15: Dynamic classification with IEEE 802.1x on Nexus 1000V requires 5.2(1)SV3(4.1). This is validated with VMware Horizon 7 VDI.

16: Port based platforms cannot do enforcement of policy for remote IP addresses, ie. they can only classify or enforce for IP addresses present in the IPDT table (hosts that are L2 adjacent).

17: IPv6 SGACL Support added in IOS-XE 16.10.1 and validation in solution validation 6.5 release was carried out with IOS-XE 16.12.1

## Product Scalability

Cisco Group Based Policy 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 4 show switch, wireless, and security products and Table 5 shows router product scalability. Table 4 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 6 lists select platform maximum number of supported SGACLs.

**Table 4.** Cisco Group Based Policy 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 3750-X & 3560-X Series (non-stack) | 1,000 (500 Bidirectional) | 200,000 | |
| Catalyst 3650 & 3850 Series | 256 (128 Bidirectional) | 12,000 | |
| Catalyst 4500 Supervisor Engine 6-E | 1,000 (900 Bidirectional) | 100,000 routed/L3<br>2,000 Switched/L2 | |
| Catalyst 4500 Supervisor Engine 7-E, 8-E | 1,800 (900 Bidirectional) | 128,000 routed/L3<br>2,000 Switched/L2 | |
| Catalyst 4500 Supervisor Engine 7L-E, 8L-E | 1,800 (900 Bidirectional) | 32,000 routed/L3<br>2,000 Switched/L2 | |
| Catalyst 4500-X Series | 1000 | 32,000 routed/L3<br>2,000 Switched/L2 | |
| Catalyst 6500 Series Supervisor Engine 720 | 2000 (1,000 Bidirectional) | 200,000 | |
| Catalyst 6500 Series Supervisor Engine 2T and 6T | 2000 (1,000 Bidirectional) | 256,000 | |
| Catalyst 6800 Series | 2,000 (1,000 Bidirectional) | 256,000 | |

| | | | |
|---|---|---|---|
| Catalyst 9200 | 256 (125 Bidirectional) | 10,000, | 9200 L (8081 mappings), For IPv6 it is 5000 mappings) |
| Catalyst 9300 Series | 256 (130 Bidirectional) | 10,000 | |
| Catalyst 9400 Supervisor Engine-1 & Sup-1XL | 256 (130 Bidirectional) | 40,000 | |
| | | | |
| Catalyst 9500 Series | 256 (130 Bidirectional) | 40,000 | |
| 9500H | 240 | 200,000 | |
| 9600 | 240 | 200,000 | |
| 1540, 1560, 1570 Series<br>1552 AP<br>1700, 2700, 2800, 3700, AP Series (Wave 1) | 5 | 3000 | |
| WLC 8540, 8510 Series | 5 | 64,000 | |
| WLC 2504 | 5 | 1,000 | |
| WLC 3504 | 5 | 3,000 | |
| WLC 5520 | 5 | 20,000 | |
| WLC 5508 | 5 | 7,000 | |
| WLC 5760 Series | 128 | 12,000 | |
| vWLC | 5 | 15,000 | |
| WISM2 | 5 | 15,000 | |
| Nexus 7000 M1 XL, M2, M3 | 980 (450 Bidirectional) | 200,000 (7.2, +)<br>50,000 (pre 7.2) | |
| Nexus 7000 M1 (non-XL) | 980 (450 Bidirectional) | 128,000 | |
| Nexus 1000V | ?? (64 Bidirectional) | 6,000 | NX-OS 5.2(1)SV3(3.1) |
| Nexus 7000 F2, F2e | 980 (450 Bidirectional) | 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 (32* Bidirectional connections) | 6,000 per VSM | *: Bidirectional max not tested; SGACL & IP-SGT mappings pushed from ISE via SSH |
| 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 |
| **Platform** | **Maximum SXP connections** | **Maximum IP-SGT bindings** | **Comments** |
| 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 5585-SSP60 | 2,000 | 500,000 | CPS method |
| ASA 5506-X | 2,000 | 195,000 | CPS method |
| ASA 5555-X | 2,000 | 500,000 | CPS method |
| FP-2100 | TBD | TBD | Expected to be similar to FP-4100 |
| 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 | |
| ISE 2.4, 2.6 | 200 | 350,000 (1 pair)<br>700,000 (2 pair)<br>1,050,000 (3 pair)<br>1,400,000 (4 pair) | Minimum 6 nodes redundant<br>Max 4 SXPSN pairs supported |
| Open Daylight SDN Controller Nitrogen Release | 100 | 25,000 | |

**Table 5. Cisco Identity Services Engine (ISE) SXP Scaling**

| Deployment Type | Platform | Max PSNs | Max ISE SXP Bindings (Shared SXP & RADIUS PSNs) | Max ISE SXP Bindings (Dedicated RADIUS & SXPSNs) | Max ISE SXP Peers |
|---|---|---|---|---|---|
| Standalone All personas on same node,<br><br>2 nodes redundant | 3515 | 0 | 3,500 | N/A | 20 |
| | 3595 | 0 | 10,000 | N/A | 30 |
| Uniified PAN+MnT on same node and dedicated PSNs<br><br>Minimum 4 nodes redundant | 3515 as PAN+MNT | 5 | 3,750 | 7,500 | 200 |
| | 3595 as PAN+MNT | 5 | 10,000 | 20,000 | 200 |
| Dedicated All personas on dedicated nodes<br><br>Minimum 6 nodes redundant | 3595 as PAN and MNT | 50 | N/A | 350,000 (1 pair)<br>500,000 (2 pair) | 200 (1 pair)<br>400 (2 pair) |
| | 3595 as PAN and Large MNT | 50 | N/A | 350,000 (1 pair)<br>700,000 (2 pair)<br>1,050,000 (3 pair)<br>1,400,000 (4 pair) | 200 (1 pair)<br>400 (2 pair)<br>600 (3 pair)<br>800 (4 pair) |

**Table 6.** Cisco Group Based Policy Platform Scalability of Router Products

| Platform | Maximum Unidirectional SXP Connections (Speaker only/ Listener | Maximum Bidirectional SXP Connections | Maximum IP SGT Bindings |
|---|---|---|---|
| 890 Series Routers | 100 | | 1,000 |
| 1900 Series Routers | 500 | 250 | 100,000 with unidirectional SXP connections<br>25,000 with bidirectional SXP connections |
| 2900, 3900 Series ISRG2 | 250 | 125 | 180,000 with unidirectional SXP connections<br>125,000 with bidirectional SXP connections |
| 4400 Series ISR | 1800 | 900 | 750,000 (IOS XE 3.15 and 3.16)<br>135,000 (IOS XE earlier than 3.15) |
| ASR 1000 Series | 1800 | 900 | 750,000 uni-directional (IOS XE 3.15 and 3.16)<br>180,000 (IOS XE earlier than 3.15) |
| ASR 1006 RP2 as SXP Reflector | | 250 with 100 bindings,<br>126 with 500 bindings | |
| Cloud Services Router 1000V Series (CSR) | 900 | 450 | 750,000 (IOS XE 3.15 and 3.16)<br>135,000 (IOS XE earlier than 3.15) |

**Table 7.** Cisco Group Based Policy Platform Scalability of SGACLs

| Platform | Maximum number of SG ACEs | Notes |
|---|---|---|
| Catalyst 3750-X & 3560-X | | 1015 maximum unique cells |
| Catalyst 3650<br>Catalyst 3850-SE, 3850-XS<br>Catalyst 3850 | 680 L4 per system | Max # of ACEs in SGACL should be 300 or less due to buffer size limits<br>256 Source/Destination Groups |

| | | |
|---|---|---|
| Catalyst 4500-X,<br>Catalyst 4500 Sup 7-E/7L-E/8-E/8L-E | 64,000 | Ranges between 64k ACEs in 1 SGACL to 1 ACE in 64k SGACLs |
| Catalyst 6500 Series Supervisor Engine 2T and 6T | 16,000 | |
| Catalyst 6840-X | 16K | |
| Catalyst 6880-X | 64K (XL), 16K (LE) | |
| Catalyst 9200 | 1408 | 256 Source/Destination Groups |
| Catalyst 9300 | 5,000 | 256 Source/Destination Groups |
| Catalyst 9400<br>Supervisor Engine-1 & -1XL | 18,000 | 256 Source/Destination Groups |
| Catalyst 9500 | 17,500 | 256 Source/Destination Groups |
| Catalyst 9500H | Pending data from test team | 256 Source/Destination Groups |
| Catalyst 9600 | Pending data from test team | 256 Source/Destination Groups |
| 1540, 1560, 1570 Series<br>1552 AP<br>1700, 2700, 2800, 3700, AP Series (Wave 1)<br>1815, 1830, 1850, 2800, 3800 AP Series (Wave 2) | 256 ACEs per SGACL | 400 unique SGACLs, 50 SGTs |
| WLC 8540, 5520, 3504 | 256 ACEs per SGACL | 800 unique SGACLs, 512 SGTs |
| Nexus 7K M3, M2, M1 Modules | 128,000 | |
| Nexus 7K F3, F2, F2e Modules, | 16,000 | |
| Nexus 7K F1 Modules | 1024 | |
| Nexus 1000V | 6,000 | |
| Nexus 5500 | 124 | 124 SGACL TCAM entries available per bank of 8 ports for feature use (4 of 128 are default entries)<br>Sum of SGACL entries per 8 port bank cannot contain more than 124 permissions in total<br>SGACL can be reused extensively; Over 2000 SGT, DGT combinations possible from reusing 124 lines of permissions |
| Nexus 5600, 6000 | 1148 | |
| ASR 1000 | 4,096 per cell | 62,500 maximum number of unique cells |

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

C96-731479-00 v6.4c 1/19