Cisco Group Based Policy Platform and Capability Matrix
(Inclusive of TrustSec Software-Defined Segmentation)

Cisco Group Based Policy (also known as TrustSec Software-Defined Segmentation) uniquely builds upon your existing identity-aware infrastructure by enforcing segmentation and access control policies in a scalable manner. This document summarizes the platforms and features that are validated in Cisco Group Based Policy testing. For more information about Cisco Group Based Policy please visit the following links:
https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html
https://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html

As an aid to deployment, products are grouped into Tier I, II, and III with regard to feedback on design and deployment. Tier I products are in Table 1 and have full Group Based Policy functionality with few caveats, and they are common components in successful deployments. Tier II products are in Table 2 and have full Group Based Policy functionality, but there are some caveats involved in their deployment. Tier III products are in Table 3 and do not have full Group Based Policy functionality and only support Classification and SXP based Propagation. These products tend to be older with a less rich feature set and more caveats to consider when deploying. In some cases, depending on the Solution-Level Validated Version, a product may be cross listed in multiple Tiers. This will be noted in the entry with a link to the cross posting and the Solution-Level Version in parenthesis. Non-Tiered Security Products are listed in Table 4. End of Sale Products are listed in Table 5. It's important to note that in some cases products in Tables 1, 2, and 3 may be at or near their End of Life or End of Sale. In this case, the product entry will have a note indicating End of Sale/Life. For a full list of Cisco products that have reached their End of Sale or Life and to review Cisco's policy on End of Sale or Life products, please visit the links at the top of Table 5. Tables 6 through 9 are Group Based Policy Scalability Tables. Finally, Table 10 defines TrustSec Group Based Policy Interoperability with Application Centric Infrastructure.

In Tables 1, 2, 3, and 4, Cisco 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 Confidential

Table 1. Tier I Cisco Group Based Policy Platform Support Matrix

Tier I products have full Group Based Policy functionality with few caveats, and they are common components in successful deployments.

System Component	Platform	License	Security Group Tag (SGT) Classification	SGT Exchange Protocol (SXP) Support and Version	Inline SGT Tagging	SGT Enforcement _____ *Services*
Tier I Cisco Catalyst 3000 Series	Catalyst 3650 and 3850 Series [Software Catalyst 3650 Series] [Software Catalyst 3850 Series]	IP Base K9 & above or Cisco ONE Foundation & above	Dynamic, IP to SGT (v4, v6), VLAN to SGT, Port to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4	SGT over Ethernet	SGACL, Logging (3.6.6E) _____ *SGT NetFlow v9*
	Catalyst 3650 and 3850 Series [Software Catalyst 3650 Series] [Software Catalyst 3850 Series]	IP Base K9 & above or Cisco ONE Foundation & above	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 VXLAN	SGACL, Monitor mode, Logging
	Catalyst 3850-XS Series [Software Catalyst 3850 Series]	IP Base K9 & above or Cisco ONE Foundation & above	Dynamic, IP to SGT, VLAN to SGT, Port to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4	SGT over Ethernet [Note5];	SGACL
Tier I Cisco Catalyst 4500 Series	Catalyst 4500 E-Series Supervisor Engine 8-E and 8L-E [Software 8L-E] [Software 8-E] **Note:** [Tier II] and [Tier III] contain entries for 4500	IP Base K9 & above or Cisco ONE Foundation & above	Support for v4/v6: Dynamic, IP to SGT VLAN to SGT, Port to SGT, Subnet to SGT, L3IF-to- SGT [Note12]	Speaker, Listener V4	SGT over Ethernet. (See note 2 for supported line cards)	SGACL, Logging _____ *SGT NetFlow v9*
	Catalyst 4500-X Series (Cisco IOS XE 3.6.3E, 3.6.6) [Software Catalyst 4500-X Series] **Note:** [Tier II] and [Tier III] contain entries for 4500	IP Base K9 & above or Cisco ONE Foundation & above	Support for v4/v6: Dynamic, IP to SGT VLAN to SGT, Port to SGT, Subnet to SGT, L3IF-to- SGT [Note12]	Speaker, Listener V4	SGT over Ethernet.	SGACL, Logging
Tier I Cisco Catalyst 6500 Series	Catalyst 6500 Series Supervisor Engine 2T & Supervisor 6T [Software Catalyst 6500 Supervisor Engine 2T] Catalyst 6807-XL [Software Catalyst 6807-XL] Cisco IOS 15.4(1)SY2 15.2(1)SY05 15.2(1)SY0a Sup 6T Cisco IOS 15.4(1)SY1 **Note:** [Tier III] contains entries for 6500	2T: IP Base K9 6T: IP Services K9	Support for v4/v6: Dynamic, IP to SGT VLAN to SGT, Port to SGT, Subnet to SGT, L3IF-to- SGT	Speaker, Listener V4 (IPv4, IPv6)	SGT over Ethernet 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. _____ *SGT Caching* *SGT NetFlow v9*
	Catalyst 6880-X, 6840-X (incl 6816-X-LE), and 6800ia [Software Catalyst 6880-X] [Software Catalyst 6840-X]	IP Base K9 & above or Cisco ONE Foundation & above	Support for v4/v6: Dynamic, IP to SGT VLAN to SGT, Port to SGT, Subnet to SGT, L3IF-to- SGT	Speaker, Listener V4 (IPv4, IPv6)	SGT over Ethernet.	SGACL (IPv4, IPv6), Monitor mode, Logging. _____ *SGT Caching* *SGT NetFlow v9*

Cisco Confidential

Tier I Cisco Catalyst 9200 Series	Cisco Catalyst 9200 Series Software Catalyst 9200 Series	Network Advantage	Support for v4/v6: Dynamic, IP to SGT, VLAN to SGT, Port to SGT, Subnet to SGT, L3IF to SGT,	Speaker, Listener V4 V5 from 17.9.1	SGT over Ethernet SGT over VXLAN	SGACL V4, V6 (Note 17), Monitor mode, Logging. ___ *SGT NetFlow v9* *SGACL drops in NetFlow - 17.13.1*
Tier I Cisco Catalyst 9300 Series	Catalyst 9300 Series Software Catalyst 9300 Series	Network Advantage	Support for v4/v6: Dynamic, IP to SGT, VLAN to SGT, Port to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4 V5 from 17.9.1	SGT over Ethernet SGT over VXLAN	SGACL V4, V6 (Note 17), Monitor mode, Logging. ___ *SGT NetFlow v9* *SGACL drops in NetFlow - 17.13.1*
Tier I Cisco Catalyst 9400 Series	Catalyst 9400 Series Supervisor Engine-1 & 1XL Software Catalyst 9400 Supervisor Engine-1	Network Advantage	Support for v4/v6: Dynamic, IP to SGT, VLAN to SGT, Port to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4 V5 from 17.9.1	SGT over Ethernet SGT over VXLAN	SGACL V4, V6 (Note 17), Monitor mode, Logging. ___ *SGT Caching* *SGT NetFlow v9* *SGACL drops in NetFlow - 17.13.1*
Tier I Cisco Catalyst 9500 Series	Catalyst 9500 Series Software Catalyst 9500 Series	Network Advantage	Support for v4/v6: Dynamic, IP to SGT, VLAN to SGT, Port to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4 V5 from 17.9.1	SGT over Ethernet SGT over VXLAN	SGACL V4, V6 (Note 17), Monitor mode. ___ *SGT Caching* *SGT NetFlow v9* *SGACL drops in NetFlow - 17.13.1*
	Catalyst 9500H/X Series	Network Advantage	Support for v4/v6: Dynamic, IP to SGT, VLAN to SGT, Port to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4 V5 from 17.9.1	SGT over Ethernet (Silicon One models supported from 17.13.1) SGT over VXLAN	SGACL V4, V6 (Note 17), Monitor mode, Logging. ___ *SGT NetFlow v9* *SGACL drops in NetFlow - 17.13.1 (Doppler only)*
Tier I Cisco Catalyst 9600 Series	Cisco Catalyst 9600 Series Software Catalyst 9600 Series	Network Advantage	Support for v4/v6: Dynamic, IP to SGT, VLAN to SGT, Port to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4 V5 from 17.9.1	SGT over Ethernet (Silicon One models supported from 17.13.1) SGT over VXLAN.	SGACL V4, V6 (Note 17), Monitor mode, Logging. ___ *SGT NetFlow v9* *SGACL drops in NetFlow - 17.13.1 (Doppler only)*
Tier I Cisco Catalyst 9800 Series	Cisco Catalyst 9800 Series	No license for the 9800 itself. Each AP joined is licensed through global setting of either Essentials or Advantage	Support for v4/v6: Dynamic, IP to SGT, Subnet to SGT, Policy Profile to SGT	Speaker, Listener V4 V5 from 17.9.1	SGT over Ethernet SGT over VXLAN	SGACL V4, V6 (Note 17), Monitor mode, Logging. ___ *SGT NetFlow v9*
Tier I Cisco Industrial Ethernet Switches	IE 3400 Series Software Catalyst IE3400 Heavy Duty Series Software Catalyst IE3400 Rugged Series	Network Advantage	Dynamic, IP to SGT, VLAN to SGT, Port to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4	SGT over Ethernet	SGACL V4, V6 (Note 17 and 19), Monitor mode, Logging. ___ *SGT NetFlow v9*

Category	Device	License	Classification	Propagation	Transport	Enforcement
	IE 9300	Network Advantage	Support for v4/v6: Dynamic, IP to SGT (v4, v6), VLAN to SGT, Port to SGT, Subnet to SGT	Speaker, Listener V4	SGT over Ethernet	SGACL V4, V6 (Note 17), Monitor mode, Logging. ⎯⎯ SGT *NetFlow* v9
Tier I Cisco Industrial Ethernet Routers	IR 8340	Both Network Essentials and Advantage	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 SGT caching
Tier I Cisco Access Points	1540, 1560 AP series [Software AP 1540](#) [Software AP 1560](#)	-	Dynamic	Speaker, Listener V4[Note6]	SGT over Ethernet [Note6]	SGACL
	1700, 2700, 3700, AP Series (Wave 1) [Software AP 1700](#) [Software AP 2700](#) [Software AP 3700](#)	-	Dynamic	Speaker, Listener V4[Note6]	SGT over Ethernet [Note6]	SGACL
	1815, 1830, 1850, 2800, 3800 AP Series (Wave 2) [Software AP 1815](#) [Software AP 1830](#) [Software AP 1850](#) [Software AP 2800](#) [Software AP3800](#) [Software AP4800](#)	-	Dynamic	Speaker, Listener V4[Note6]	SGT over Ethernet [Note6]	SGACL
Tier I Cisco Wireless Controller Series	8540 Series Wireless Controller (Cisco AireOS 8.9) [Software 8540 Wireless Controller](#) **Note:** [Tier III](#) contains entries for 8540	-	Dynamic	Speaker v2	SGT over Ethernet	Supports AP SGACL in Centralized and Flex Connect mode)
	5520 Series Wireless Controller (Cisco AireOS 8.9) [Software 5520 Wireless Controller](#) **Note:** [Tier III](#) contains entries for 5520	-	Dynamic	Speaker v2	SGT over Ethernet	Supports AP SGACL in Centralized and Flex Connect mode)
	3504 Wireless Controller [Software 3540 Wireless Controller](#)	-	Dynamic	Speaker v2	SGT over Ethernet (Centralized mode)	Supports AP SGACL in Centralized and Flex Connect mode)
	vWLC [Software vWLC](#)	-	Dynamic	Speaker v2		Supports APs in Flex mode only
Tier I Cisco Nexus® 7000 Series	Nexus 7000 with M3-Series modules Cisco NX-OS 8.1(2), 8.1(1), 8.0(1) 7.3.2 7.3(0)D1(1) [logging, monitor mode], 7.2(0)D1(1) **Note:** [Tier II](#) contains entries for Nexus 7000s	Base License NX-OS 6.1 and later	IP to SGT[1], Port Profile to SGT, VLAN to SGT[2], Port to SGT[2] Subnet to SGT[5] [Note14]	Speaker, Listener V4	SGT over Ethernet[5]; SGT over VXLAN [5]: F3 interoperability requires M3 'no propagate-sgt l2 control' command	SGACL, Monitor mode & logging
Tier I Cisco Integrated Services Router (ISR)	ISR 1000 Series [Cisco 1000 Series ISRs DSL and LTE SKUs](#)	IP Base/K9 for classify/ propagate, SGACL, Security/K9 for SG FW enforcement	IP to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4 V5 from 17.9.1	SGT over Ethernet, SGT over GETVPN, DMVPN, or IPsec VPN	SGACL, Monitor mode & Logging SG Firewall ⎯⎯ *SGT based PBR. SGT Caching SGT based QoS.*

Cisco Confidential

System Component	Platform / Solution Validated Software Version	License	Security Group Tag (SGT) Classification	SGT Exchange Protocol (SXP) Support and Version	Inline SGT Tagging	SGT Enforcement / Services
	ISR 1100 Series Recommended Software	IP Base/K9 for classify/propagate, SGACL, Security/K9 for SG FW enforcement	IP to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4 V5 from 17.9.1	SGT over Ethernet, SGT over GETVPN, DMVPN, or IPsec VPN	SGACL, Monitor mode & Logging SG Firewall ——— *SGT based PBR.* *SGT Caching* *SGT based QoS.*
	4000 Series ISR 4431, 4451-X, 4321, 4331, 4351 (Cisco IOS XE Denali 16.3.2, Everest 16.4.1) Software ISR 4000 Series **Note:** Tier II contains entries for 4451	IP Base/K9 for classify/propagate, SGACL, Security/K9 for SG FW enforcement	IP to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4 V5 from 17.9.1	SGT over Ethernet, SGT over GETVPN, DMVPN, or IPsec VPN	SGACL, Monitor mode & Logging SG Firewall ——— *SGT based PBR.* *SGT Caching* *SGT based QoS.*
	ISRv	IP Base/K9 for classify/propagate, SGACL	IP to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4 V5 from 17.9.1	SGT over Ethernet, SGT over IPsec VPN, DMVPN	SGACL, Monitor mode & Logging
Tier I Cisco Cloud Services Router	CSR 1000V (Cisco IOS XE 16.6.3 Denali 16.3.2, Everest 16.4.1) Recommended Software **Note:** Tier II contains entries for CSR 1000V	IP Base/K9 for classify/propagate, SGACL;	IP to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4 V5 from 17.9.1	SGT over Ethernet, SGT over IPsec VPN, DMVPN	SGACL, Monitor mode & Logging
Tier I Cisco Aggregation Services Router (ASR)	ASR 1004, 1006, 1013, 1001-X, 1002-X,1002-HX, 1006-X, and 1009-X (Cisco IOS XE 16.5.1b Denali 16.3.2, Everest 16.4.1) Software ASR 1004 Software ASR 1006 Software ASR 1013 Software ASR 1001-X Software ASR1002-X Software ASR 1002-HX Software ASR 1006-X Software ASR 1009-X **Note:** Tier II contains entries for ASR	IP Base/K9 for classify/propagate, SGACL, Security/K9 for SGFW enforce-ment	IP to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4 V5 from 17.9.1	SGT over Ethernet, SGT over GETVPN, DMVPN, or IPsec VPN	SGACL, Monitor mode & Logging, SG Firewall ——— *SGT based PBR.* *SGT Caching* *SGT based QoS.*
Tier 1 Cisco Catalyst 8000 series routers	C8200-1N-4T, C8200L-1N-4T, C8500-12X, C8500L-8S4X, C8300-2N2S-6T, C8000V 16vCPU/16GB, C8000V 8vCPU/8GB, C8000V 2vCPU/4GB Software 8000v Edge Software 8500 Edge	Network Advantage	IP to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4 V5 from 17.9.1	SGT over Ethernet, SGT over GETVPN, DMVPN, or IPsec VPN Note18	SGACL, Monitor mode & Logging SG Firewall ——— *SGT based PBR.* *SGT Caching* *SGT based QoS.*
Tier I Cisco Identity Services Engine	ISE 34xx, 35xx, 36xx, 37xx Appliance & VMware Software ISE	Advantage (for both TrustSec and pxGrid)	Dynamic, IP to SGT, Subnet to SGT	Speaker, Listener V4 pxGrid	–	–

Table 2. Tier II Cisco Group Based Policy Platform Support Matrix

Tier II products have full Group Based Policy functionality but there are some caveats involved in their deployment.

System Component	Platform ——— Solution Validated Software Version	License	Security Group Tag (SGT) Classification	SGT Exchange Protocol (SXP) Support and Version	Inline SGT Tagging	SGT Enforcement ——— Services

Tier II Cisco Catalyst 3000 Series	Catalyst 3560-CX Series (Cisco IOS 15.2(3)E) Software Catalyst 3560-CX **Note:** Tier III contain entries for 3560	IP Base K9	(L2 adjacent hosts only) Dynamic, IP to SGT (v4, v6), VLAN to SGT, Subnet to SGT	Speaker, Listener V4	No	SGACL Note16
Tier II Cisco Catalyst 4500 Series	Catalyst 4500 E-Series Supervisor Engine 7-E and 7L-E (Cisco IOS XE 3.7.1E) **Note:** Tier I and Tier III contain entries for 4500 **Note:** End of Sale/Life	IP Base K9 & above or Cisco ONE Foundation & above	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT, L3IF to SGT, Port to SGT Note12	Speaker, Listener V4	SGT over Ethernet. (See note 2 for supported line cards)	SGACL, Logging [3.8.0E] _SGT NetFlow v9_
Tier II Cisco Connected Grid Router Series	CGR 2010 Series Software CGR 2010 Series	-	Dynamic, IP to SGT, VLAN to SGT	Speaker, Listener V4	SGT over GETVPN, SGT over IPsec VPN	SG Firewall
Tier II Cisco Industrial Ethernet Switches	IE 4000 Series Software IE 4000 Series	LAN Base, IP Services for SGToE & SGACL	(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 Software IE 5000 Series	LAN Base, IP Services for SGToE & SGACL	(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
Tier II Cisco Nexus® 7000 Series	Nexus 7000 with M2-Series modules Cisco NX-OS 8.1(1), 8.0(1) 7.3(0)D1(1) [Monitor mode & limited logging], 7.2(0)D1(1) **Note:** Tier 1 contains entries Nexus 7000s	Base License NX-OS 6.1 and later	IP to SGT[1], Port Profile to SGT, VLAN to SGT[2], Port to SGT[2] Subnet to SGT[5] Note14 [1]:FabricPath support requires 6.2(10) or later. [2] VPC/VPC+ support requires 7.2(0)D1(1) or later. [5] Subnet to SGT requires 7.3(0)D1(1) or later.	Speaker, Listener V4	SGT over Ethernet[5]; [5]: M2 cannot link to F3 module.	SGACL Monitor mode & limited logging
Tier II Cisco Nexus® 7000 Series	Nexus 7700 F-Series[Note4] modules 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. Cisco NX-OS 8.1(1), 8.0(1) 7.3(0)D1(1), 7.2(0)D1(1) **Note:** Tier 1 contains entries for Nexus 7000s	Base License NX-OS 6.1 and later	IP to SGT[1], Port Profile to SGT, VLAN to SGT[2], Port to SGT[2] Subnet to SGT[5] Note14 [1]:FabricPath support requires 6.2(10) or later. [2] VPC/VPC+ support requires 7.2(0)D1(1) or later. [5] Subnet to SGT requires 7.3(0)D1(1) or later.	Speaker, Listener V4	SGT over Ethernet[35]; [3]: F3 interfaces (L2 or L3) require 802.1Q or FabricPath [4]: F2e (Copper) all ports; F2e (SFP) & F3 (10G)- last 8 ports; All others- no support [5]: Not supported	SGACL

Tier II Cisco Nexus 5000, 6000 Series	Nexus 6000/5600 Series [Software Nexus 6000]	-	(L2 adjacent hosts only) Port to SGT	Speaker V1	SGT over Ethernet	SGACL [Note16]
	Nexus 5548P, 5548UP, and 5596UP [Software Nexus 5548P] [Software Nexus 5548UP] [Software Nexus 5596UP]	-	(L2 adjacent hosts only) Port to SGT	Speaker V1 [1] [1]: FabricPath	SGT over Ethernet	SGACL [Note16]
Tier II Cisco Nexus 1000 Series	Nexus 1000V for VMware vSphere [Software Nexus 1000V]	Advanced license for SGToE/ SGACL support	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 [Software Nexus 1000VE]	Advanced license for SGACL support	Port Profile to SGT, IP to SGT	Speaker, Listener v4	No	SGACL
Tier II Cisco Integrated Services Router (ISR)	890, 1900, 2900, 3900 Series [Software ISR 890 and 1900] [Software 2900 Series] [Software 3900 Series]	IP Base/K9 for classify/ propagate, Security/K 9 for SG FW enforcem ent	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*
Tier II Cisco Integrated Services Router (ISR)	4000 Series (ISR 4451-X validated) (Cisco IOS XE 3.15.01S) [Software ISR 4000 Series] **Note:** [Tier I] contains entries for 4451 Products	IP Base/K9 for classify/ propagate, Security/K 9 for SG FW enforcem ent	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 [Software SM-X Layer 2/3]	IP Services/K9	Dynamic, IP to SGT, VLAN to SGT	Speaker, Listener V4	SGT over Ethernet.	SGACL
Tier II Cisco Cloud Services Router	Cloud Services Router 1000V Series (CSR) (Cisco IOS XE 3.15.01S) [Software CSR 1000V] **Note:** [Tier I] contains entries for CSR 1000V	IP Base/K9 for classify/ propagate, Security/K9 for enforce-ment	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*
Tier II Cisco Aggreg-ation Services Router (ASR)	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) (Cisco IOS XE 3.13.0S) [Software ASR 1000 RP1] [Software ASR 1000 RP2] [Software ASR 1001] [Software ASR 1002] [Software ASR 1004] [Software ASR 1006] [Software ASR 1013] **Note:** [Tier I] contains entries for ASR Products	IP Base/K9 for classify/ propagate, Security/K9 for enforce-ment	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*

	Platform	License	Security Group Tag (SGT) Classification	SGT Exchange Protocol (SXP) Support and Version	Inline SGT Tagging	SGT Enforcement / *Services*
	ASR 1001-X and 1002-X (Cisco IOS XE 3.13.0S) Software ASR 1001-X Software ASR 1002-X **Note:** Tier I contains entries for ASR Products	IP Base/K9 for classify/propagate, Security/K9 for enforcement	IP to SGT, Subnet to SGT, L3IF to SGT	Speaker, Listener V4	SGT over Ethernet, SGT over GETVPN, IPsec VPN, DMVPN	SG Firewall *SGT based PBR* *SGT based QoS.* *SGT Caching* *SGT NetFlow v9*

Table 3. Tier III Cisco Group Based Policy Platform Support Matrix

Tier III products do not have full Group Based Policy functionality and support Classification and SXP based propagation only.

System Component	Platform	License	Security Group Tag (SGT) Classification	SGT Exchange Protocol (SXP) Support and Version	Inline SGT Tagging	SGT Enforcement *Services*
Tier III Cisco Catalyst® 2000 Series	Catalyst 2960-Plus Series Software 2960-Plus Series **Note**: End of Sale/Life	LAN Base K9	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT	Speaker V4	No	No
	Catalyst 2960-C Series Software 2960-C Series **Note:** End of Sale/Life	LAN Base K9	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT	Speaker V4	No	No
	Catalyst 2960-CX Series Software 2960-CX Series **Note:** End of Sale/Life	LAN Base K9	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT	Speaker V4	No	No
	Catalyst 2960-X Series Software 2960-X Series **Note:** End of Sale/Life	LAN Base K9	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT	Speaker V4	No	No
	Catalyst 2960-XR Series Software 2960-XR Series **Note:** End of Sale/Life	IP Lite K9	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT	Speaker V4	No	No
Tier III Cisco Catalyst 3000 Series	Catalyst 3560-C/CG Series (Cisco IOS 15.0(1)SE2) Software Catalyst 3560-C **Note:** Tier II contains entries for Nexus 3560 **Note**: End of Sale/Life	IP Base K9	(L2 adjacent hosts only) Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT	Speaker, Listener V4	No	No
Tier III Cisco Catalyst 4500 Series	Catalyst 4500 E-Series Supervisor Engine 6-E and 6L-E; (Cisco IOS 15.1(1)SG) Software 4500 Supervisor Engine 6-E Software Supervisor Engine 6L-E **Note:** Tier I and Tier II contain entries for 4500 **Note:** End of Sale/Life	IP Base K9	Dynamic, IP to SGT [Note12]	Speaker, Listener V4	No	No

Cisco Confidential

Tier III Cisco Catalyst 6500 Series	Catalyst 6500 Series Supervisor Engine 32 and 720 Cisco IOS 15.2(2)SY2, 15.2(1)SY0a, 15.2(3a)E Software 6500 Series Supervisor Engine 720 **Note:** Tier I contain entries for 6500 **Note:** End of Sale/Life	IP Base K9	Dynamic, IP to SGT	Speaker, Listener V4	No	No
Tier III Cisco Connected Grid Switch Series	CGS 2500 Series Software CGS-2520-16S-8PC Software CGS-2520-24TC	-	Dynamic, IP to SGT, VLAN to SGT, Port to SGT, Subnet to SGT	Speaker, Listener V3	No	No
Tier III Cisco Industrial Ethernet Switches	IE 2000 & 2000U Series IE 3000 Series Software IE 2000 Series Software IE 2000U Series Software IE 3000 Series	LAN Base	(L2 adjacent hosts only) Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT	Speaker, Listener V4	No	No
Tier III Cisco Wireless Controller Series	5500 Series (5508, 5520) 2500 Series (2504) (Cisco AireOS 8.3.102.0, 7.6.130.0) Software 5500 Series Software 2500 Series **Note:** Tier I contains entries for 8520 **Note:** End of Life/Sale	-	Dynamic	Speaker V2	No	No
	8500 Series (8540,8510) (Cisco AireOS 8.3.102.0 (pre 8.4)) Software 8500 Series **Note:** Tier I contains entries for 8540	-	Dynamic	Speaker V2	No	No

Table 4. Non-Tiered Security Cisco Group Based Policy Platform Support Matrix

System Component	Platform	License	Security Group Tag (SGT) Classification	SGT Exchange Protocol (SXP) Support and Version	Inline SGT Tagging	SGT Enforcement _____ *Services*
	ASA 5580 Software ASA 5580	-		Speaker, Listener v2		SG Firewall

Cisco Confidential

Cisco Adaptive Security Appliance	ASA 5506-X, 5506H-X, 5506W-X, 5508-X, 5516-X [Software ASA 5506-X](#) [Software ASA 5506H-X](#) [Software ASA 5506W-X](#) [Software ASA 5516-X](#) [Software ASA 5508-X](#)	-	Remote Access VPN (IPsec, SSL-VPN); SGT assigned via ISE Authz.	Speaker, Listener V3	SGT over Ethernet	SG Firewall (IPv4, IPv6) *SGT based PBR*
Cisco Adaptive Security Appliance	ASA 5525-X, 5545-X, 5555-X with FirePower Services [Software ASA 5525-X](#) [Software ASA 5545-X](#)	-	Remote Access VPN (IPsec, SSL-VPN); SGT assigned via ISE Authz.	Speaker, Listener V3	SGT over Ethernet	SG Firewall (IPv4, IPv6) *SGT based PBR.*
	ASAv [Software ASAv](#)	-	Remote Access VPN (IPsec, SSL-VPN); SGT assigned via ISE Authz.	Speaker, Listener V3	SGT over Ethernet	SG Firewall *SGT based PBR.*
Cisco Secure Firewall	Secure FW 1000, 2100, 3100, 4100, 4200, 9300 [(ASA software)](#)	-	Remote Access VPN (IPsec, SSL-VPN)	Speaker, Listener V3	SGT over Ethernet	SG Firewall (IPv4, IPv6) *SGT based PBR.*
Cisco Secure Firewall	Secure FW 1000, 2100, 3100, 4100, 4200, 9300, FTDv [(Firepower Threat Defense software)](#)	Firepower Threat Defense Base	Remote Access VPN; SGT assigned via pxGrid (not via ISE Authz)	pxGrid	SGT over Ethernet	SG Firewall (src SGTs only before ver 6.5, src & dst from 6.5) *SGT based PBR.*
Cisco Industrial Security Appliance	ISA 3000 Series [Software ISA 3000](#)	-	Remote Access VPN (IPsec, SSL-VPN)	Speaker, Listener V3	SGT over Ethernet	SG Firewall (IPv4, IPv6) *SGT b based PBR.*

Table 5. End of Sale Group Based Policy Platform Support Matrix

(https://www.cisco.com/c/en/us/products/eos-eol-listing.html)

(https://www.cisco.com/c/en/us/products/eos-eol-policy.html)

EOS System Component	Platform	License	Security Group Tag (SGT) Classification	SGT Exchange Protocol (SXP) Support and Version	Inline SGT Tagging	SGT Enforcement *Services*
Cisco Catalyst® 2000 Series	Catalyst 2960-S and 2960-SF Series	LAN Base K9	Dynamic, IP to SGT, VLAN to SGT, Subnet to SGT	Speaker V4 [Note1]	No	No
	Catalyst 3560-E and 3750-E Series	IP Base K9	(L2 adjacent hosts only) Dynamic, IP to SGT, VLAN to SGT	Speaker, Listener V2	No	No

Cisco Catalyst 3000 Series	Catalyst 3560-X and 3750-X Series	IP Base K9	(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 V4	SGT over Ethernet, SGT over VXLAN	SGACL [Note16] (Maximum of 8 VLANs on a VLAN-trunk link)
Cisco Catalyst 4500 Series	Cisco Catalyst 4948 Series	IP Base K9	Dynamic, IP to SGT	Speaker, Listener V4	No	No
Cisco Nexus® 7000 Series	Cisco Nexus 7000 F2-Series*** modules	Base License NX-OS 6.1 and later	IP to SGT[1], Port Profile to SGT, VLAN to SGT[2], Port to SGT[2] Subnet to SGT[5] [1]:FabricPath support requires 6.2(10) or later [2] VPC/VPC+ support requires 7.2(0)D1(1) or later. [5] Subnet to SGT requires 7.3(0)D1(1) or later.	Speaker, Listener V3	SGT over Ethernet. [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	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)	-	Dynamic	Speaker V2	No	No
	Flex 7500 Series Wireless Controller	-	Dynamic	Speaker V2	No	No
Cisco Aggreg-ation Services Router (ASR)	ASR 1001, 1002	IP Base/K9 for classify/ propagate. Security/K 9 for enforce-ment	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*
Cisco Identity Services Engine	ISE 3315, 3355, 3395, Appliance				–	–
	ASA 5510, 5520, 5540, 5550	-		Speaker, Listener v2		SG Firewall

Cisco Adaptive Security Appliance	ASA 5505[Note3], 5512, 5515, 5525, 5545, 5555, 5585	-	Remote Access VPN (IPsec, SSL-VPN)	Speaker, Listener V2 (IPv4, IPv6)	SGT over Ethernet	SG Firewall (IPv4, IPv6) *SGT based PBR.*
	ASA 5512-X, 5515-X, 5585-X with FirePower Services	-	Remote Access VPN (IPsec, SSL-VPN)	Speaker, Listener V3	SGT over Ethernet	SG Firewall (IPv4, IPv6) *SGT based PBR.*
Cisco Fire POWER	FirePOWER 7000 and 8000 Series	Threat & Apps (TA)	-	-	SGT over Ethernet	-

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 6 show switch, wireless, and security products, Table 7 shows ISE SXP scaling, and Table 8 shows router product scalability. Table 6 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 9 lists select platform maximum number of supported SGACLs.

Table 6. 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 2,000 Switched/L2	
Catalyst 4500 Supervisor Engine 7-E, 8-E	1,800 (900 Bidirectional)	128,000 routed/L3 2,000 Switched/L2	
Catalyst 4500 Supervisor Engine 7L-E, 8L-E	1,800 (900 Bidirectional)	32,000 routed/L3 2,000 Switched/L2	
Catalyst 4500-X Series	1000	32,000 routed/L3 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 9200L	200 (100 Bidirectional)	8,081	
Catalyst 9200 Catalyst 9200CX	200 (100 Bidirectional)	10,000	
Catalyst 9300/L/LM Series	256 (130 Bidirectional)	10,000	
Catalyst 9300X		32,000	
Catalyst 9400 Supervisor Engine-1 & Sup-1XL	256 (130 Bidirectional)	40,000	
Catalyst 9400X		109,000	

Catalyst 9500/H	256 (130 Bidirectional)	200,000	
Catalyst 9500X		200,000	
Catalyst 9600/X	240	200,000	200k mappings for both Sup1 and Sup2
Industrial Ethernet 3400	500	1024 Host to SGT. (64 subnet to SGT)	
Industrial Ethernet 9300	512 (256 Bidirectional)	10,000 (5,000 IPv6)	
1540, 1560, 1570 Series 1552 AP 1700, 2700, 2800, 3700, AP Series (Wave 1) 1815, 1830, 1850, 2800, 3800 AP Series (Wave 2)	5	3000	
91xx AP	5	5,000	200 SGTs max
WLC Catalyst 9800CL (Large)		750,000	
WLC Catalyst 9800-40		750,000	
WLC Catalyst 9800-80		750,000	
WLC Catalyst 9800-L		150,000	
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, +) 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	
ASA 5510	25	1,000	
ASA 5520	50	2,500	

ASA 5540	100	5000	
ASA 5550	150	7,500	
ASA 5580-20	250	10,000	
ASA 5580-40	500	20,000	
ASA 5585-SSP10	150	18,750	
ASA 5585-SSP20	250	25,000	
ASA 5585-SSP40	500	50,000	
ASA 5585-SSP60	1,000	100,000	
ASA 5506-X	2,000	195,000	
ASA 5555-X	2,000	500,000	
FP-2100 running ASA code	TBD	TBD	Expected to be similar to FP-4100
FP-4110 running ASA code	2,000	1M	
FP-9300 SM-36 running ASA code	2,000	1M	
FTD running on vFTD, KVM, VMWare, AWS, Azure	pxGrid	64,000	
FTD running on ASA 5508, 5516, 5525, 5545, 5555	pxGrid	64,000	
FTD running on Firepower 1010, 1120, 1140, 1150	pxGrid	64,000	
FTD running on Firepower 2110, 2120, 2130, 4110	pxGrid	64,000	
FTD running on Firepower 2140, 4112, 4115, 4120, 4125	pxGrid	150,000	
FTD running on Firepower 9300 and 4100, 3100	pxGrid	300,000	
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 -> 3.1	200	350,000 (1 pair) 700,000 (2 pair) 1,050,000 (3 pair) 1,400,000 (4 pair)	Minimum 6 nodes redundant Max 4 SXPSN pairs supported
Open Daylight SDN Controller Nitrogen Release	100	25,000	

Table 7. 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, 2 nodes redundant	3515	0	3,500	N/A	20
	3595	0	20,000	N/A	30
	3615	0	12,500	N/A	30
	3655/3715	0	25,000	N/A	40
	3695/3755/3795	0	50,000	N/A	50

Uniified PAN+MnT on same node and dedicated PSNs Minimum 4 nodes redundant	3515 as PAN+MNT	6	3,750	7,500	200
	3595 as PAN+MNT	6	10,000	20,000	200
	3655 as PAN+MNT	6	12,500	25,000	200
	3695 as PAN+MNT	6	25,000	50,000	200
	3715 as PAN+MNT	6	37,500	75,000	200
	3755/3795 as PAN+MNT	6	75,000	150,000	200
Dedicated All personas on dedicated nodes. Minimum 6 nodes redundant	3595/3655 as PAN and MnT	50	N/A	350,000 (1 pair) 500,000 (2 pair)	200 (1 pair) 400 (2 pair)
	3595/3695/3755/3795 as PAN and Large MNT	50	N/A	350,000 (1 pair) 700,000 (2 pair) 1,050,000 (3 pair) 1,400,000 (4 pair)	200 (1 pair) 400 (2 pair) 600 (3 pair) 800 (4 pair)

Table 8. Cisco Group Based Policy Platform Scalability of Router Products

Platform	Maximum Unidirectional SXP Connections (Speaker only/ Listener only)	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 25,000 with bidirectional SXP connections
2900, 3900 Series ISRG2	250	125	180,000 with unidirectional SXP connections 125,000 with bidirectional SXP connections
4400 Series ISR	1800	900	750,000 (IOS XE 3.15 and 3.16) 135,000 (IOS XE earlier than 3.15)
ASR 1000 Series	1800	900	750,000 uni-directional (IOS XE 3.15 and 3.16) 180,000 (IOS XE earlier than 3.15)
ASR 1006 RP2 as SXP Reflector		250 with 100 bindings, 126 with 500 bindings	
Cloud Services Router 1000V Series (CSR)	900	450	750,000 (IOS XE 3.15 and 3.16) 135,000 (IOS XE earlier than 3.15)
C8500-12X C8500L-8S4X C8300-2N2S-6T	1800	900	750,000 IPv4 and IPv6 in both SDWAN controller and Autonomous modes.
C8000V 16vCPU/16GB	1800	900	720,000 IPv4 and IPv6 in SDWAN controller mode. 750,000 IPv4 and IPv6 in Autonomous mode.
C8000V 8vCPU/8GB	900	450	720,000 IPv4 and IPv6 in SDWAN controller mode. 750,000 IPv4 and IPv6 in Autonomous mode.
C8200L-1N-4T	500	250	135,000 in both SDWAN controller and Autonomous modes.
C8000V 2vCPU/4GB	250	125	100,000 IPv4 and IPv6 in both SDWAN controller and Autonomous modes.
ISR1121X-8P	500	250	100,000 IPv4 and IPv6 in both SDWAN controller and Autonomous modes.

Table 9. 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 Catalyst 3850-SE, 3850-XS Catalyst 3850	1,350	Max # of ACEs in SGACL should be 300 or less due to buffer size limits 256 Source to unique Destination Groups 4,000 SGT/DGT Policies
Catalyst 4500-X, Catalyst 4500 Sup 7-E/7L-E/8-E/8L-E	64,000	Ranges between 64,000 ACEs in 1 SGACL to 1 ACE in 64,000 SGACLs
Catalyst 6500 Series Supervisor Engine 2T and 6T	16,000	
Catalyst 6840-X	16,000	
Catalyst 6880-X	64,000 (XL), 16,000 (LE)	
Catalyst 9200/L Catalyst 9200CX	1,408	256 Source to unique Destination Groups in releases < 17.2, then 4,096 from 17.2 2,000 SGT/DGT Policies
Catalyst 9300/L/LM	Total ACL entries: 5,000	256 Source to unique Destination Groups in releases < 17.2, then 4,096 from 17.2 8,000 SGT/DGT Policies
Catalyst 9300X	Total ACL entries: 4,800	4,096 Source to unique Destination Groups 7,400 SGT/DGT Policies
Catalyst 9400 Supervisor Engine-1 & -1XL	18,000	256 Source to unique Destination Groups in releases < 17.2, then 4,096 from 17.2 8,000 SGT/DGT Policies
Catalyst 9400X	16,000	32,000 SGT/DGT Policies
Catalyst 9500	18,000	256 Source to unique Destination Groups in releases < 17.2, then 4,096 from 17.2 8,000 SGT/DGT Policies
Catalyst 9500H	13,000	16,000 SGT/DGT Policies
Catalyst 9500X	4,000	32,000 SGT/DGT Policies
Catalyst 9600	Total number of ACL entries: 27,000	256 Source to unique Destination Groups in releases < 17.2, then 4,096 from 17.2 SGT/DGT policies 32,000 for Sup1 default profile, 28,000 for Sup1 tested.
Catalyst 9600X	4,000	32,000 SGT/DGT Policies
Industrial Ethernet 3400	6630	SGT/DGT 21 * 21, Max ACE per SGACL 15
Industrial Ethernet 9300	1,408	2,000 SGT/DGT policies
1540, 1560, 1570 Series 1552 AP 1700, 2700, 2800, 3700, AP Series (Wave 1) 1815, 1830, 1850, 2800, 3800 AP Series (Wave 2)	256 ACEs per SGACL	400 unique SGACLs, 50 SGTs
91xx AP		Validated for 50 SGTs and 200 unique SGACLs per AP
WLC Catalyst 9800-40	32,000 ACE's	512 Max no. SGTs 256 Max no. ACE's per SGACL 128 Max no. unique SGACLs 65,536 SGT/DGT Policy recommended limit (256*256*16*256)

WLC Catalyst 9800-80	96,000 ACE's	512 Max no. SGTs 256 max no. ACE's per SGACL 128 Max no. unique SGACLs 65,536 SGT/DGT Policy recommended limit (256*256*16*256)
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) Sum of SGACL entries per 8 port bank cannot contain more than 124 permissions in total 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
C8500-12X C8500L-8S4X C8300-2N2S-6T C8000V 16vCPU/16GB C8000V 8vCPU/8GB	64,000	24,000 SGT/DGT Policies
C8200L-1N-4T	20,000	20,000 SGT/DGT Policies
C8000V 2vCPU/4GB	10,000	10,000 SGT/DGT Policies
ISR1121X-8P	10,000	10,000 SGT/DGT Policies

Table 10 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 (Nitrogen and earlier releases) working together in the Data Center.

Table 10. TrustSec 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;		

Nexus 9k (in L2 mode) can forward an SGT tagged packet unmodified.	Cloudscale ASICs in Standalone NX-OS mode. FX, FX2, FX3 and GX	NX-OS 9.3.3	Nexus 9k in L2 mode can propagate SGT unmodified between two CTS devices	Providing interoperability in CTS enabled environments. NO PLANS for generating or rewriting SGT in packets. NO PLANS for classification or enforcement in standalone NX-OS mode.
Nexus 9k (in L3 mode) can forward an SGT tagged packet unmodified.	Cloudscale ASICs in Standalone NX-OS mode. FX, FX2, FX3 and GX	NX-OS 10.2.2F	Nexus 9k in L3 mode to propagate SGT unmodified between two CTS devices	Providing interoperability in CTS enabled environments. NO PLANS for generating or rewriting SGT in packets. NO PLANS for classification or enforcement in standalone NX-OS mode.
Meraki Adaptive Policy. Adaptive Policy transport across MX LAN and AutoVPN for full-stack LAN segmentation	Security & SD-WAN (MX)	MX17 Beta. Subsequent major FW version will support Adaptive Policy enforcement.		
Open Daylight SDN controller	ODL SDN	Lithium, Beryllium, Carbon	SGT via SXP v4	Cisco ISE 2.1- SXP v4 Nexus 7000 7.3- SXP v3 ASA 9.6.1- SXP v3
Open Daylight SDN controller	ODL SDN	Nitrogen	IPv4, IPv6 SXP Peering	Cisco ISE 2.4 ASR 1001-X IOS XE 16.5.1b CSR 1000v IOS XE 16.6.3 Cat 6500 IOS 15.4(1)SY2 Cat 3850 IOS 3.6.8E

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 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 an SVI is also needed on the VLAN for the derivation of source group for L2 traffic.

13: 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.

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

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

16: Port based platforms cannot do enforcement of policy for remote IP addresses, ie. they can only classify or enforce 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

18: For the C82xx and C83xx, the following WAN modules do support SGT inline tagging: C-NIM-2T, C-NIM-1M, C-NIM-1X.

19: IE3400 supports SGACL on base switch and only on IEM-3400 expansion modules. IEM-3300-8P and IEM-3300-16P are non-FPGA expansion modules on the 3400 and do not support enforcement. When non-FPGA expansion module used then base 3400 does not support enforcement.

Cisco Confidential