



INDEX

Numerics

802.1AE

See Cisco TrustSec, IEEE 802.1AE support

802.1X [6-2](#)

802.1X Host Modes [6-5](#)

C

Cisco TrustSec

architecture [1-1](#)

authorization [1-9](#)

configuring [?? to 4-10](#)

configuring NDAC [1-3](#)

connection caching [4-9](#)

default values [2-3](#)

enabling [3-1, 3-3](#)

environment data download [1-10](#)

guidelines and limitations [2-3](#)

IEEE 802.1AE support [1-11](#)

link security [1-11](#)

manual mode [3-5](#)

permissions matrix [1-7](#)

policy acquisition [1-9](#)

RADIUS relay [1-11](#)

SAP negotiation [1-11](#)

seed device [1-1, 1-10, 3-1](#)

SGACLs [?? to 1-9](#)

SGTs [1-6 to 1-9, 3-9](#)

SXP [4-1 to ??](#)

Cisco TrustSec. See CTS

Cisco TrustSec authentication

description [?? to 1-6](#)

Cisco TrustSec caching

clearing [4-10](#)

enabling [4-9](#)

Cisco TrustSec device credentials

description [1-6](#)

Cisco TrustSec device identities

description [1-6](#)

Cisco TrustSec environment data

download [1-10](#)

Cisco TrustSec manual mode

configuring [3-5](#)

Cisco TrustSec Solution

configuring [2-1 to ??](#)

Cisco TrustSec user credentials

description [1-6](#)

conditional debugging [7-58](#)

CTS

configuring [?? to 4-10](#)

description [1-1 to ??](#)

SGACLs [5-1 to ??](#)

CTS authentication

description [1-3 to ??](#)

cts role-based policy trace [7-25](#)

D

debug condition cts [7-58](#)

DGT

See SGT, destination

DHCP Snooping [6-6](#)

Diagnostic trace [7-25](#)

E

EAP-FAST

in Cisco TrustSec authentication [1-3](#)Error Messages [C-4](#)

FFAS [6-5](#)

Fibre Channel interfaces

default settings [3-11, 3-15](#)

FIPS

Catalyst 6500 Series support [C-4](#)Flexible NetFlow [C-2](#)

G

Galois/Counter Mode. See GCM

GCM

Cisco TrustSec SAP encryption [1-11](#)

GCM authentication. See GMAC

GMAC

Cisco TrustSec SAP authentication [1-11](#)

I

Identity Port Mapping

See IPM

interfaces

default settings [3-11, 3-15](#)

IPM

configuring [3-6](#)description [1-9](#)

LL2 VRF assignment [7-32](#)L3IF-SGT mapping [3-19](#)

MMAB [6-3](#)

MACSec

See Cisco TrustSec, link security

management interfaces

default settings [3-11, 3-15](#)

Media Access Control Security

See Cisco TrustSec, link security

mgmt0 interfaces

default settings [3-11, 3-15](#)

N

NDAC

for Cisco TrustSec [1-3](#)NetFlow [C-2](#)

Network Device Admission Control

See NDAC

P

PAC

in Cisco TrustSec authentication [1-3](#)Pre-Authentication Open Access [6-6](#)

protected access credential

See PAC

S

Security Association Protocol. See SAP

security group access list

See SGACL

security group tag

See SGT

seed device

in a Cisco TrustSec network [1-1, 1-10, 3-1](#)

SGACL policies

- configuration process [5-1](#)
- displaying [5-5](#)
- displaying downloads [5-6](#)
- enabling enforcement for VLANs [5-2](#)
- enabling enforcement globally [5-2](#)
- manually configuring [5-3 to ??](#)

SGACLs

- configuring [5-1 to ??](#)
- description [1-7 to 1-9](#)

SGACLs policies

- acquisition [1-9](#)

SGT

- destination [1-7](#)
- source [1-7](#)

SGT Exchange Protocol

- See SXP

SGTs

- description [1-6 to 1-9](#)
- manually configuring [3-9](#)
- manually mapping IP addresses [3-10](#)

Subnet to SGT mapping [3-10](#)

SXP

- configuration process [4-1](#)
- configuring [4-1 to ??](#)
- configuring peer connections [4-2](#)
- default passwords [4-4](#)
- description [1-12](#)
- enabling [4-2](#)
- reconcile period [4-4](#)
- retry period [4-5](#)
- source IP address [4-4](#)

Syslog Messages [C-4](#)

System Error Messages [C-4](#)

- SGACLs [1-7 to ??](#)

TrustSec. See CTS

V

VLANs

- enabling SGACL policy enforcement [5-2](#)

VLAN to SGT mapping [3-18](#)

VRF

- cts role-based command [7-95](#)
- cts sxp command [7-39](#)
- overview [1-15](#)
- Specifying for an SXP connection [4-3](#)

W

WebAuth [6-4](#)

- web-based authentication [6-4](#)

T

Troubleshooting

- SGACL and SGT behaviour [7-25](#)

TrustSec

