GLOSSARY

Revised: May 28, 2010, OL-22192-01

Numeric

802.1AE IEEE 802.1AE defines a Layer 2 hop-by-hop encryption process used between Cisco TrustSec hardware-capable devices. TrustSec uses SAP for the key management and cipher negotiation mechanism.

A

Authenticator A network device that is a member of a TrustSec network can authenticate a network device attempting to join the TrustSec network, in the role of authenticator to supplicant device. NDAC is the process by which the supplicant device is admitted into the TrustSec Network.

C

CTS Cisco Trusted Security, or Cisco TrustSec, or TrustSec.

E

EAC Endpoint Admission Control. A process of assigning SGT values to a specific IP address of the endpoint. Depending on hardware and software support, an SGT can be assigned to a source IP address with 802.1X authentication, MAC Authentication Bypass, Web Authentication Bypass, manual assignment, or IPM.

EAP Extensible Authentication Protocol. EAP-FAST is the EAP variant used in TrustSec networks for NDAC authentication.

I

IPM Identity-to-port mapping. A method for a switch to define the identity on a port to which an endpoint is connected, and to use this identity to look up a particular SGT value in the Cisco Secure ACS server.

M

MACSec Media Access Control Security based on IEEE 802.1AE to provide hop-to-hop link encryption. A TrustSec hardware-capable device can establish a MACSec link with a TrustSec hardware-capable peer.

N

NDAC Network Device Admission Control. A mutual authentication mechanism between CTS devices to authenticate and authorize its peer using an 802.1X process. EAP-FAST is used as the EAP type.

Non-seed Device Non-seed devices do not have direct IP connectivity to the Cisco Secure ACS and require other devices to authenticate and authorize them onto the TrustSec network, such as a seed device or a device already enrolled in the TrustSec network.

R

RBAC Role-based Access Control. An access control mechanism based on the role of the endpoints. RBAC is different from group based access control in a sense that RBAC can take multiple role factors to derive final policy for a particular entity.

RBACL Role-based Access Control List. Often used to characterize SGACL because TrustSec uses the RBAC features of the Cisco Secure ACS.

S

SAP Security Association Protocol, negotiates keys and cipher suite for link encryption after successful authentication and authorization for NDAC. SAP is derived from the 802.11i standard. SAP negotiation can be automatically initiated after NDAC process or the PMK can be statically configured on an interface.

Seed Device The seed device is the first TrustSec hardware-capable device to authenticate against the Cisco Secure ACS for TrustSec policy authorization. The seed device becomes the authenticator for the next TrustSec supplicant device, which in turn becomes an authenticator to its supplicant devices.

SGACL Security Group Access Control List. A Layer 3 to Layer 4 access control list that filters according to the value of SGTs. Usually, filtering occurs at an egress port of the CTS domain.

SGT Security Group Tag. A Layer-2 tag inserted in an Ethernet frame to classify traffic based on role. The tag process occurs at the ingress of the CTS domain. SGTs are defined in the Cisco Secure ACS configuration.

Supplicant In TrustSec, a network device without a direct connection to the Cisco Secure ACS which is requesting TrustSec authentication from an authenticated TrustSec network device (an authenticator) NDAC is the process by which the supplicant device is admitted into the TrustSec network.

SXP SGT Exchange Protocol. Allows devices with SXP support to build a source IP-to-SGT binding table, and then transfers the table to TrustSec hardware-capable devices through an out-of-bound TCP connection using MD5-based authentication.

T

TrustSec Trusted Security. Same as Cisco Trusted Security (CTS).

TrustSec Hardware-capable A network device that can tag traffic with SGTs, enforce SGACLs, and establish a MACSec connection with a TrustSec peer.

TrustSec Software-capable A network device that can establish NDAC and SXP connections with a TrustSec peer.