GLOSSARY

数値

802.1AE IEEE 802.1AE は Cisco TrustSec ハードウェア対応デバイス間で使用されるレイヤ 2 のホップバイホップ暗号化プロセスを定義します。TrustSec では、キー管理および暗号ネゴシエーション メカニズムに、SAP を使用します。

C

CTS Cisco Trusted Security、または Cisco TrustSec、または TrustSec。

E

EAC エンドポイント アドミッション コントロール。エンドポイントの特定の IP アドレスへの SGT 値の割り当てプロセス。ハードウェアおよびソフトウェアのサポートに応じて、802.1X 認証、MAC 認証バイパス、Web 認証バイパス、手動割り当て、または IPM で、SGT を送信元 IP アドレスに割り当てることができます。

EAP Extensible Authentication Protocol。EAP-FAST は、NDAC 認証用に TrustSec ネットワークで使用する EAP バリアントです。

I

IPM アイデンティティとポートのマッピング。エンドポイントが接続されているポートのアイデンティティを定義し、このアイデンティティを使用して Cisco Secure ACS サーバで特定の SGT 値を検索する、スイッチの方式。

M

MACSec ホップ単位のリンク暗号化を提供するための、IEEE 802.1AE に基づく Media Access Control Security。TrustSec ハードウェア対応デバイスは、TrustSec ハードウェア対応ピアとの MACSec リンクを確立できます。

N

NDAC ネットワーク デバイス アドミッション コントロール。802.1X プロセスを使用してピアを認証および認可する CTS デバイス間の相互認証のメカニズム。EAP-FAST は、EAP タイプとして使用されます。

R

RBAC ロールベース アクセス コントロール。エンドポイントのロールに基づくアクセス コントロール メカニズム。RBAC は複数のロール ファクタで特定のエンティティの最終ポリシーを取得することができるという点で、RBAC はグループ ベースのアクセス コントロールとは異なります。

RBACL ロールベース アクセス コントロール リスト。TrustSec は Cisco Secure ACS の RBAC 機能を使用するため、SGACL を特徴付けるためによく使用されます。

S

SAP セキュリティ アソシエーション プロトコル。NDAC の認証および認可の成功後に、リンク暗号化のキーおよび暗号スイートをネゴシエートします。SAP は 802.11i 標準をベースとしています。SAP ネゴシエーションは NDAC プロセス後自動的に開始できます。それ以外の場合は PMK をインターフェイスでスタティックに設定できます。

Seed Device シード デバイスは、TrustSec ポリシー認可のために Cisco Secure ACS で認証する最初の TrustSec ハードウェア対応デバイスです。シード デバイスは次の TrustSec サプリカント デバイスのオーセンティケータになり、そのサプリカント デバイスはさらにそのサプリカント デバイスのオーセンティケータになります。

SGACL セキュリティ グループ アクセス コントロール リスト。SGT の値に従ってフィルタリングを行う、レイヤ 3 からレイヤ 4 へのアクセス コントロール リスト。通常、フィルタリングは CTS ドメインの出力ポートで発生します。

SGT セキュリティ グループ タグ。ロールに基づいてトラフィックを分類するために、イーサネット フレームに追加されたレイヤ 2 タグ。タグの処理は、CTS のドメインの入力で実行されます。SGT は Cisco Secure ACS 設定で定義されています。

SXP SGT 交換プロトコル。SXP をサポートするデバイスが送信元 IP と SGT のバインディング テーブルを作成し、MD5 ベースの認証を使用して範囲外の TCP 接続を通じて TrustSec ハードウェア対応デバイスにそのテーブルを転送できるようにします。

T

TrustSec Trusted Security。Cisco Trusted Security（CTS）と同じです。

TrustSec ソフトウェア対応 TrustSec ピアとの NDAC および SXP 接続を確立できるネットワーク デバイス。

TrustSec ハードウェア対応 トラフィックに SGT をタグ付けし、SGACL を適用し、TrustSec ピアとの MACSec の接続を確立できるネットワーク デバイス。

お

オーセンティケータ TrustSec ネットワークのメンバであるネットワーク デバイスは、サプリカント デバイスに対するオーセンティケータのロールで、TrustSec ネットワークに参加しようとするネットワーク デバイスを認証できます。NDAC はサプリカント デバイスが TrustSec ネットワークに入ることを許可されるプロセスです。

さ

サプリカント TrustSec において、認証された TrustSec ネットワーク デバイス（オーセンティケータ）からの TrustSec 認証を要求している、Cisco Secure ACS に直接接続していないネットワーク デバイス。NDAC は、サプリカント デバイスが TrustSec ネットワークに入ることを許可されるプロセスです。

ひ

非シード デバイス 非シード デバイスには Cisco Secure ACS への直接 IP 接続がないため、シード デバイスまたはすでに TrustSec ネットワークに登録されたデバイスなどのその他のデバイスが、非シード デバイスの TrustSec ネットワークへの参加を認証および許可する必要があります、