Cisco TrustSec の設定

Cisco TrustSec の概要

Cisco TrustSec は、ネットワーク内のユーザ、ホスト、およびネットワーク デバイスを強力に識別する機能に基づいた、シスコ ネットワーク デバイスのセキュリティを改善します。TrustSec は、特定の役割についてデータ トラフィックを一意に分類することで、トポロジに依存しない、スケーラブルなアクセス コントロールを実現します。TrustSec は、認証されたピアおよびこれらのピアとの暗号化リンク間で信頼を確立することで、データの機密保持および整合性を保証します。

Cisco TrustSec の主要コンポーネントは、Cisco Identity Services Engine（ISE）です。スイッチ上で手動で設定することもできますが、Cisco ISE は TrustSec ID およびセキュリティ グループ ACL（SGACL）でスイッチをプロビジョニングできます。

Cisco TrustSec の機能

次の表に、TrustSec 対応のシスコ スイッチで実装される Cisco TrustSec 機能を示します。継続的な Cisco TrustSec の一般提供リリースによって、サポートされるスイッチの数および各スイッチでサポートされる Cisco TrustSec 機能の数は増加しています。

Cisco TrustSec の機能	説明
802.1AE タギング（MACSec）	IEEE 802.1AE に基づくワイヤレート ホップ単位レイヤ 2 暗号化のプロトコル。 MACSec 対応デバイス間において、パケットは送信デバイスからの出力で暗号化され、受信デバイスへの入力で復号化されます。デバイス内では平文です。 この機能は、TrustSec ハードウェア対応デバイス間だけで利用できます。
エンドポイント アドミッション コントロール（EAC）	EAC は、TrustSec ドメインに接続しているエンドポイントユーザまたはデバイスの認証プロセスです。通常、EAC はアクセス レベル スイッチで実行されます。EACプロセスの認証および許可に成功すると、ユーザまたはデバイスに対してセキュリティ グループ タグが割り当てられます。現在、EAC は 802.1X、MAC 認証バイパス（MAB）、および Web 認証プロキシ（WebAuth）とすることができます。
ネットワーク デバイス アドミッション コントロール（NDAC）	NDAC は、TrustSec ドメイン内の各ネットワーク デバイスがピア デバイスのクレデンシャルおよび信頼性を確認できる認証プロセスです。NDAC は、IEEE 802.1X ポート ベースの認証に基づく認証フレームワークを利用し、EAP方式として EAP-FAST を使用します。NDACプロセスの認証および許可に成功すると、IEEE 802.1AE暗号化のセキュリティ アソシエーション プロトコル ネゴシエーションとなります。
セキュリティ グループ アクセス コントロール リスト（SGACL）	セキュリティ グループ アクセス コントロール リスト（SGACL）は、セキュリティ グループ タグをポリシーと関連付けます。ポリシーは、Cisco TrustSec ドメインから出力される SGT タグ付きトラフィックに対して適用されます。

Cisco TrustSec の機能	説明
Cisco TrustSec SGACL のハイ アベイラビリティ	Cisco TrustSec セキュリティ グループ アクセス コントロール リスト（SGACL）は、Cisco StackWise 技術をサポートしているスイッチでのハイ アベイラビリティ機能をサポートしています。Cisco StackWise 技術によってステートフルな冗長性が提供され、スイッチ スタックはアクセス制御エントリを強制し、処理できます。 この機能を有効にする Cisco TrustSec 固有の設定はありません。
セキュリティ アソシエーション プロトコル（SAP）	NDAC認証後、セキュリティアソシエーションプロトコル（SAP）は、その後の Cisco TrustSec ピア間の MACSec リンク暗号化のキーおよび暗号スイートについて、自動的にネゴシエーションを行います。SAP は IEEE 802.11i で定義されます。
セキュリティ グループ タグ（SGT）（Security Group Tag (SGT)）	SGT は、Cisco TrustSec ドメイン内の送信元のセキュリティ分類を示す 16 ビットの単一ラベルです。イーサネットフレームまたはIPパケットに追加されます。
SGT 交換プロトコル（SXP）	Security Group Tag Exchange Protocol（SXP）。SXP を使用すると、Cisco TrustSec にハードウェアで対応していないデバイスが Cisco Identity Services Engine（ISE）または Cisco Secure アクセス コントロール システム（ACS）から認証されたユーザとデバイスの SGT 属性を受信できます。次にデバイスは、SGACL を適用するために送信元トラフィックにタグ付けする Cisco TrustSec ハードウェア対応のデバイスに送信元 IP と SGT のバインディングを転送できます。

リンクの両端で 802.1AE MACsec をサポートしている場合、SAP ネゴシエーションが実行されます。サプリカントとオーセンティケータの間で EAPOL-Key が交換され、暗号スイートのネゴシエーション、セキュリティ パラメータの交換、およびキーの管理が実行されます。これらの作業が正常に完了すると、セキュリティ アソシエーション（SA）が確立します。

ソフトウェア バージョンとライセンスおよびリンク ハードウェア サポートに応じて、SAP ネゴシエーションは次の動作モードの 1 つを使用できます。

- Galois Counter Mode（GCM）：認証と暗号化
- GCM authentication（GMAC）：GCM 認証、暗号化なし

- No Encapsulation：カプセル化なし（クリア テキスト）
- null：カプセル化、認証または暗号化なし

Cisco TrustSec の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよび Cisco ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1*：*Cisco TrustSec* の機能情報

機能名	リリース	機能情報	
Cisco TrustSec	Cisco IOS XE Everest 16.6.1	Cisco TrustSec は、ネットワーク内のユーザ、ホスト、およびネットワーク デバイスを強力に識別する機能に基づいた、シスコ ネットワーク デバイスのセキュリティを改善します。Cisco TrustSec は、特定の役割についてデータ トラフィックを一意に分類することで、トポロジに依存しない、スケーラブルなアクセスコントロールを実現します。Cisco TrustSec は、認証されたピアおよびこれらのピアとの暗号化リンク間で信頼を確立することで、データの機密保持および整合性を保証します。 この機能は、次のプラットフォームに実装されていました。 • Cisco Catalyst 9300 シリーズ スイッチ	