CHAPTER 14

Cisco TrustSec

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、特定のロールについてデータ 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。

スイッチ上で Cisco TrustSec を設定するには、次の URL にある『*Cisco TrustSec Switch Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/trustsec.html

Cisco TrustSec General Availability リリースのリリース ノートについては、次の URL を参照してください。

http://www.cisco.com/en/US/docs/switches/lan/trustsec/release/notes/rn_cts_crossplat.html

Cisco TrustSec ソリューションの詳細（概要、データシート、およびケース スタディなど）については、次の URL を参照してください。

http://www.cisco.com/en/US/netsol/ns1051/index.html

表 1 に、TrustSec がイネーブルになった Cisco スイッチで実装される TrustSec 機能を示します。継続的な TrustSec の General Availability 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 TrustSec 機能の数は増加しています。

Catalyst 3750-X スイッチおよび Catalyst 3560-X スイッチに関する TrustSec 機能の制限事項の詳細については、「設定時の注意事項および制限事項」（P.14-3）を参照してください。

表 1　Cisco TrustSec の主要機能

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、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。
セキュリティ アソシエーション プロトコル（SAP）	NDAC 認証のあと、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 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）	SGT は、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、TrustSec にハードウェアで対応していないデバイスが、Cisco Secure アクセス コントロール システム（ACS）からの認証済みユーザまたはデバイスの SGT 属性を受信できます。デバイスは、タグ付けおよび SGACL の適用のために、TrustSec にハードウェアで対応しているデバイスに、sourceIP-to-SGT バインディングを転送できます。

設定時の注意事項および制限事項

次の注意事項と制約事項は、Catalyst 3750-X および Catalyst 3560-X スイッチの Cisco TrustSec SGT と SGACL の設定に適用されます。

- IP サブネットを SGT に静的にマッピングすることはできません。SGT には、IP アドレスだけをマッピングできます。IP アドレスから SGT へのマッピングを設定する場合、IP アドレス プレフィックスは 32 である必要があります。
- ポートがマルチ認証モードに設定されている場合は、そのポートに接続されているすべてのホストを同じ SGT に割り当てる必要があります。ホストが認証を試みると、割り当てられた SGT は以前に認証されたホストに割り当てられた SGT と同じでなければなりません。SGT がすでに認証されているホストの SGT ではない場合にホストが認証を試みると、これらのホストが属する VLAN ポート（VP）は errdisable になります。
- Cisco TrustSec 強制は、VLAN トランク リンクの最大 8 つの VLAN でだけサポートされます。VLAN トランク リンクに 8 つを超える VLAN が設定されている場合、Cisco TrustSec 強制がこれらの VLAN でイネーブルにされると、これらの VLAN トランク リンクのスイッチ ポートが errdisable になります。
- スイッチは、エンドホストがスイッチに隣接するレイヤ 2 である場合にだけ SGT を割り当て、SXP リスニングに基づいて、対応する SGACL をエンドホストに適用できます。
- ポートから SGT へのマッピングは、Cisco TrustSec リンク（つまり、スイッチ間リンクのスイッチ）でだけ設定できます。ポートから SGT へのマッピングは、ホストからスイッチへのリンクには設定できません。

  ポートにポートから SGT へのマッピングが設定されている場合、そのポートのすべての入力トラフィックに SGT が割り当てられます。ポートの出力トラフィックに対する SGACL 強制はありません。
- SGT/SGACL は、すべてのネットワーク アップリンク モジュール搭載 Cisco Catalyst 3750-X および 3650-X シリーズ スイッチでサポートされます: C3KX-NM-1G、C3KX-NM-10G、C3KX-NM-10GT および C3KX-SM-10G。C3KX-SM-10G はアップリンク MACsec でのみ必要です。