CHAPTER 9

Cisco TrustSec の設定

この章では、NX-OS デバイスに Cisco TrustSec を設定する手順について説明します。

この章の内容は次のとおりです。

Cisco TrustSec の概要

ここでは、次の内容について説明します。

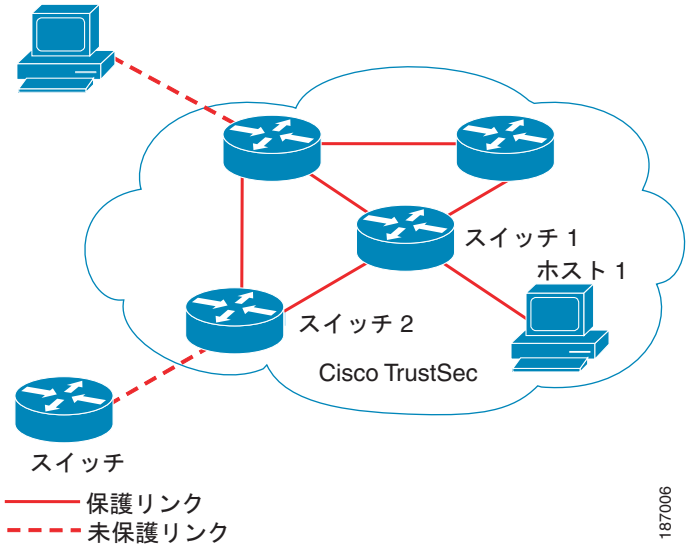
Cisco TrustSec のアーキテクチャ

Cisco TrusSec のセキュリティ アーキテクチャは、信頼できるネットワーク デバイスのクラウドを確立することによってセキュア ネットワークを構築します。クラウド内の各デバイスは、そのネイバーによって認証されます。クラウド内のデバイス間リンクでの通信は、暗号化、メッセージ整合性検査、データパス リプレイ防止メカニズムを組み合わせたセキュリティで保護されます。また Cisco TrustSec は、認証時に取得されたデバイスおよびユーザの識別情報を、ネットワークに入る際のパケットの分類またはカラリングに使用します。このパケット分類は、Cisco TrustSec ネットワークへの入力時にパケットにタグ付けされることにより維持されます。タグによってパケットはデータ パス全体を通じて正しく識別され、セキュリティおよびその他のポリシー基準が適用されます。このタグは、セキュリティ グループ タグ（SGT）と呼ばれることもあります。エンドポイントのデバイスが SGT に応じてトラフィックをフィルタリングできるようにすることにより、アクセス コントロール ポリシーをネットワークに強制できます。

（注）　入力とは、宛先へのパス上のパケットが最初の Cisco TrustSec 対応デバイスに入ることです。出力とは、パス上の最後の Cisco TrustSec 対応デバイスを出ることです。

図 9-1 に、Cisco TrustSec クラウドの例を示します。この例では、Cisco TrustSec クラウド内に、ネットワーク接続されたデバイスが数台とエンドポイント デバイスが 1 台あります。エンドポイント デバイス 1 台とネットワーク接続デバイス 1 台がクラウドの外部にあるのは、これらが Cisco TrustSec 対応デバイスでないか、またはアクセスを拒否されたからです。

図 9-1　Cisco TrustSec ネットワーク クラウドの例



Cisco TrustSec アーキテクチャは、主に次のコンポーネントで構成されています。

- 認証 — Cisco TrustSec ネットワークにデバイスを加入させる前に、各デバイスの識別情報を検証します。
- 許可 — 認証されたデバイスの識別情報に基づいて、Cisco TrustSec ネットワークのリソースに対するデバイスのアクセス権のレベルを決定します。
- アクセス コントロール — 各パケットのソース タグを使用して、パケット単位でアクセス ポリシーを適用します。
- セキュア通信 — Cisco TrustSec ネットワークの各リンク上のパケットに、暗号化、整合性検査、データパス リプレイ防止を提供します。

Cisco TrustSec ネットワークには、次の 3 つのエンティティがあります。

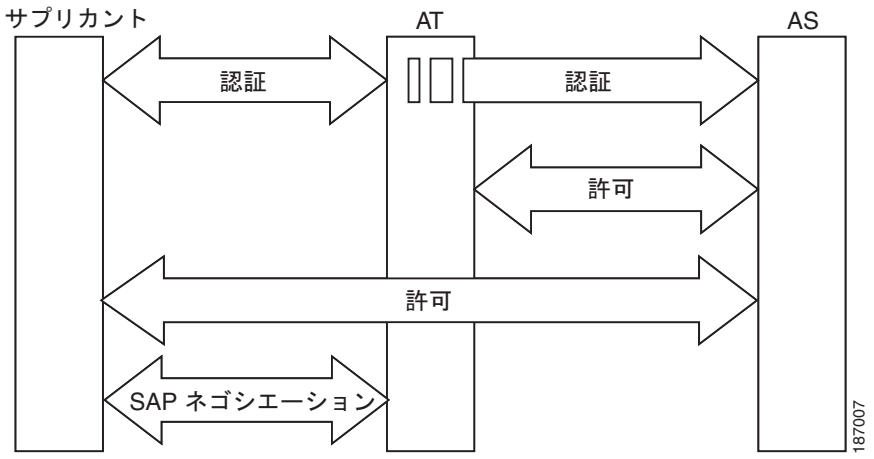
- サプリカント — Cisco TrustSec ネットワークへの加入を試行するデバイス
- オーセンティケータ（AT）— すでに Cisco TrustSec ネットワークに含まれているデバイス
- 許可サーバ — 認証情報、許可情報、またはその両方を提供できるサーバ

サプリカントと AT の間のリンクの初回の確立時には、次の一連のイベントが発生します。

1. 認証（802.1X）— 認証サーバがサプリカントの認証を実行します。あるいは、これらのデバイスが無条件に相互認証するように設定している場合は認証がそのまま完了します。
2. 許可 — リンクの両側が、そのリンクに適用する SGT および ACL などのポリシーを取得します。サプリカントは、認証サーバへの他のレイヤ 3 ルートがない場合には、AT をリレーとして使用する必要があります。
3. Security Association Protocol（SAP）ネゴシエーション — サプリカントと AT 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、Security Parameter Index（SPI; セキュリティ パラメータ インデックス）の交換、キーの管理が実行されます。これら 3 つの作業が正常に完了すると、Security Association（SA; セキュリティ アソシエーション）が確立します。

SAP ネゴシエーションが完了するまで、ポートは未許可状態（ブロッキング状態）です（図 9-2 を参照）。

図 9-2　SAP ネゴシエーション



SAP ネゴシエーションには、次のいずれかの動作モードが使用されます。

- Galois/Counter Mode（GCM）暗号化
- GCM 認証（GMAC）
- カプセル化なし（クリア テキスト）
- 暗号化も認証もなしのカプセル化

Cisco TrustSec は、IEEE 802.1AE 規格に基づいて、ESP-128 GCM および GMAC を使用します。

認証

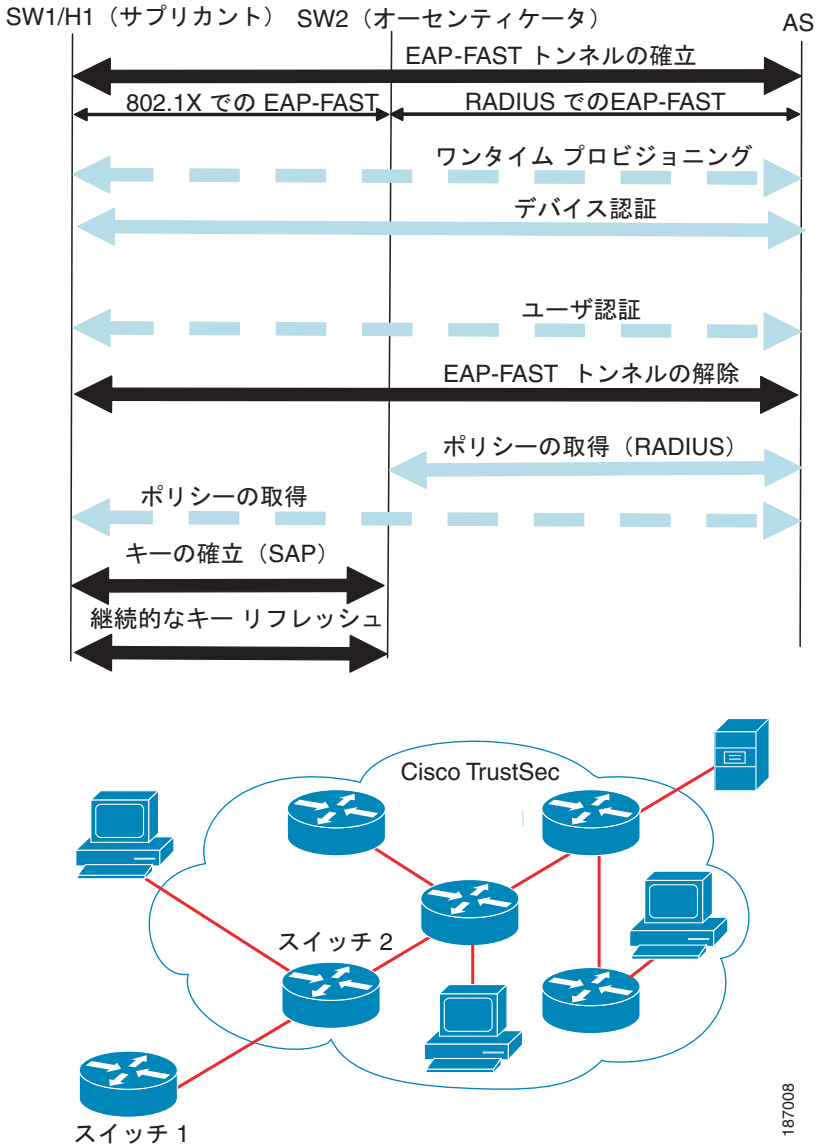
Cisco TrustSec は、デバイスのネットワーク加入を許可する前にデバイスを認証します。Cisco TrustSec は、Extensible Authentication Protocol（EAP）方式としての Extensible Authentication Protocol Flexible Authentication via Secure Tunnel（EAP-FAST）とともに、802.1X 認証を使用して、認証を実行します。

ここでは、次の内容について説明します。

Cisco TrustSec と認証

Cisco TrustSec は認証に EAP-FAST を使用します。EAP-FAST カンバセーションによって、チェーンを使用した EAP-FAST トンネル内で他の EAP 方式の交換が可能になります。この方法では、管理者は Microsoft Challenge Handshake Authentication Protocol Version 2（MSCHAPv2）のような従来型のユーザ認証方式を使用しながら、EAP-FAST トンネルが提供するセキュリティも利用できます。図 9-3 に、EAP-FAST トンネルおよび Cisco TrustSec で使用される内部方式を示します。

図 9-3　Cisco TrustSec の認証



ここでは、次の内容について説明します。

- EAP-FAST への Cisco TrustSec の機能拡張（p.9-5）
- 802.1X ロールの選択（p.9-6）
- Cisco TrustSec 認証の概要（p.9-6）

EAP-FAST への Cisco TrustSec の機能拡張

Cisco TrustSec に EAP-FAST を実装することにより、次の機能拡張が実現されました。

- オーセンティケータの認証 — AT と認証サーバの間の共有秘密を得るために Protected Access Credential（PAC）を使用するように AT に求めることにより、AT のアイデンティティをセキュアに判断します。また、この機能により、AT が使用できるすべての IP アドレスに関して認証サーバに RADIUS 共有秘密を設定する手間が省けます。

- ネイバーのアイデンティティを各ピアに通知 — 認証交換の完了までに、認証サーバはサプリカントと AT の両方を識別します。認証サーバは、保護された EAP-FAST 終端で追加の type-length-value（TLV）パラメータを使用して、AT のアイデンティティと、その AT が Cisco TrustSec に対応しているかどうかをサプリカントに伝えます。認証サーバはさらに、Access-Accept メッセージの RADIUS 属性を使用して、サプリカントのアイデンティティおよびそのサプリカントが Cisco TrustSec に対応しているかどうかを AT に伝えます。各ピアは、ネイバーのアイデンティティを認識しているため、認証サーバに追加の RADIUS Access-Requests を送信し、リンクに適用されるポリシーを取得できます。
- AT ポスチャ評価 — AT は、サプリカントの代わりに認証サーバと認証交換を開始すると、そのポスチャ情報を認証サーバに提供します。

802.1X ロールの選択

802.1X では、AT に認証サーバとの IP 接続が必要です。AT は RADIUS over UDP/IP を使用してサプリカントと AT の認証交換をリレーする必要があるためです。PC などのエンドポイント デバイスはネットワークへの接続時にサプリカントとして動作することになります。ただし、2 つのネットワーク デバイス間の Cisco TrustSec 接続の場合、各ネットワーク デバイスの 802.1X ロールが他方のネットワーク デバイスに即座に認識されない場合もあります。

NX-OS デバイスに AT とサプリカントのロールを手動で設定する代わりに、Cisco TrustSec はロール選択アルゴリズムを実行し、AT として動作する NX-OS デバイスとサプリカントとして動作する NX-OS デバイスを自動的に判断します。ロール選択アルゴリズムは、RADIUS サーバに IP で到達可能なデバイスに AT ロールを割り当てます。どちらのデバイスも AT とサプリカントの両方のステート マシンを起動します。ある NX-OS デバイスが、ピアに RADIUS サーバへのアクセス権があることを検出すると、そのデバイスは自身の AT ステート マシンを終了し、サプリカントのロールを引き受けます。両方の NX 飽 S デバイスに RADIUS サーバへのアクセス権がある場合、アルゴリズムは EAP over LAN（EAPOL）パケット送信の送信元として使用される MAC アドレスを比較します。MAC アドレスの値が大きい方の NX-OS デバイスが AT になり、もう一方の NX-OS デバイスがサプリカントになります。

Cisco TrustSec 認証の概要

Cisco TrustSec 認証プロセスが完了するまでに、認証サーバは次の処理を行います。

- サプリカントと AT のアイデンティティの検証
- サプリカントがエンドポイント デバイスの場合はユーザの認証

Cisco TrustSec 認証プロセスの完了時には、AT およびサプリカントの両方が次の情報を取得しています。

- ピアのデバイス ID
- ピアの Cisco TrustSec 機能についての情報
- SAP に使用されるキー

デバイスのアイデンティティ

Cisco TrustSec はデバイスのアイデンティティとして IP アドレスも MAC アドレスも使用しません。その代わり、各 Cisco TrustSec 対応 NX-OS デバイスに、Cisco TrustSec ネットワークで一意に識別できる名前（デバイス ID）を手動で割り当てる必要があります。このデバイス ID は次の操作に使用されます。

- 認証ポリシーの検索
- 認証時におけるデータベース内のパスワードの検索

デバイスの証明書

Cisco TrustSec はパスワードベースの証明書をサポートしています。認証サーバは、代わりに自己署名式の証明書を使用する場合もあります。Cisco TrustSec はパスワードでサプリカントを認証し、MSCHAPv2 を使用することにより、たとえ認証サーバの証明書を検証できなくても、相互認証が可能です。

認証サーバはこれらの証明書を EAP-FAST フェーズ 0（プロビジョニング）の交換（サプリカントで PAC がプロビジョニングされる）中にサプリカントの相互認証に使用します。Cisco TrustSec は PAC の期限が切れるまで、EAP-FAST フェーズ 0 交換は再実行しません。その後のリンク起動時には、EAP-FAST フェーズ 1 とフェーズ 2 の交換のみを実行します。EAP-FAST フェーズ 1 交換では、認証サーバとサプリカントの相互認証に PAC が使用されます。Cisco TrustSec がデバイスの証明書を使用するのは、PAC プロビジョニング（または再プロビジョニング）段階だけです。

認証サーバは、Cisco TrustSec ネットワークにサプリカントが最初に加入する際に、一時的に設定されたパスワードをそのサプリカントの認証に使用します。サプリカントが最初に Cisco TrustSec ネットワークに加入する際に、認証サーバは証明書を作成してサプリカントを認証し、強力なパスワードを生成して、これを PAC でサプリカントに送信します。認証サーバはさらに、データベースに新しいパスワードを保存します。認証サーバとサプリカントは、その後の EAP-FAST フェーズ 0 交換の相互認証にこのパスワードを使用します。

ユーザの証明書

Cisco TrustSec には、エンドポイント デバイスの特定タイプのユーザ証明書は必要ありません。ユーザに対して任意のタイプの認証方式（MSCHAPv2、LEAP、Generic Token Card [GTC]、または OTP など）を選択し、対応する証明書を使用できます。Cisco TrustSec は、EAP-FAST フェーズ 2 交換の一部として EAP-FAST トンネル内でユーザ認証を実行します。

SGACL と SGT

SGACL（セキュリティ グループ アクセス リスト）を使用すると、割り当てられたセキュリティ グループに基づいてユーザが実行できる操作を制御できます。許可をロールにまとめることにより、セキュリティ ポリシーの管理が容易になります。NX-OS デバイスにユーザを追加する際に、1 つ以上のセキュリティ グループを割り当てれば、ユーザは適切な許可を即座に受信できます。セキュリティ グループを変更することにより、新しい許可を追加したり、現在の許可を制限することもできます。

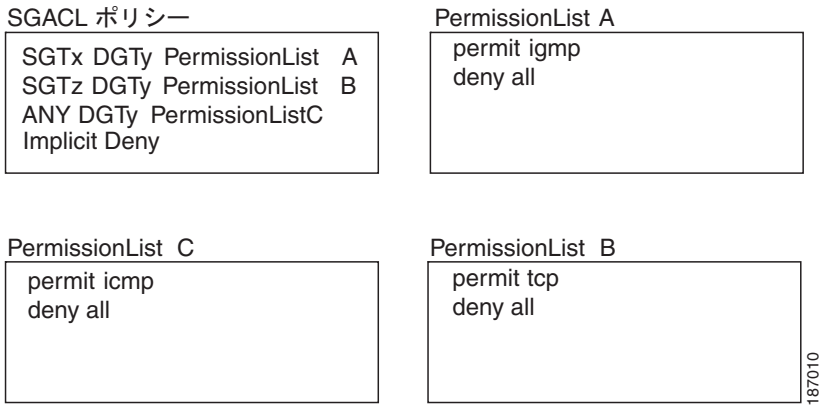
Cisco TrustSec はセキュリティ グループに、SGT（セキュリティ グループ タグ）という 16 ビットの固有のタグを割り当てます。NX-OS デバイス内の SGT の数は認証済みのネットワーク エンティティの数に制限されます。SGT は全社内の送信元の許可を示す単一ラベルです。範囲は Cisco TrustSec ネットワーク内でグローバルです。

管理サーバは、セキュリティ ポリシーの設定に基づいて SGT を引き出します。これらを手動で設定する必要はありません。

いったん認証されると、Cisco TrustSec はデバイスを送信元とするすべてのパケットに、そのデバイスが割り当てられているセキュリティ グループを表す SGT を付けます。タグ付けされたパケットはネットワークを通じて Cisco TrustSec ヘッダーで SGT を運びます。このタグは、送信元のグループを表しているので、送信元の SGT として参照されます。Cisco TrustSec は、ネットワークの出口で、パケットの宛先デバイスに割り当てられているグループを判断し、アクセス コントロール ポリシーを適用します。

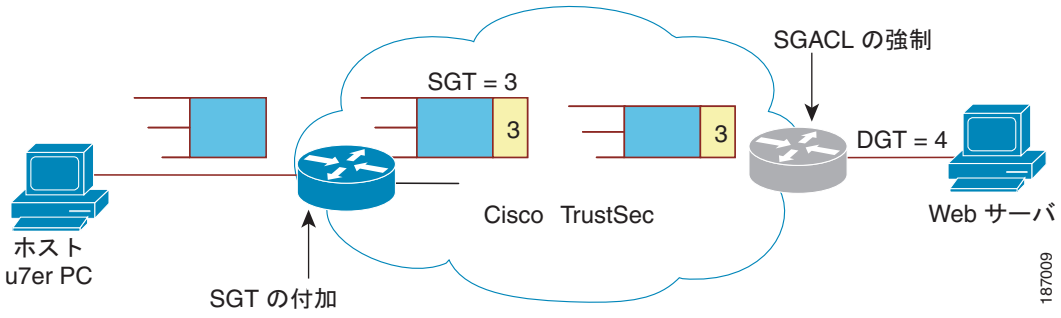
Cisco TrustSec はセキュリティ グループ間のアクセス コントロール ポリシーを定義します。Cisco TrustSec は、ネットワーク内のデバイスをセキュリティ グループに割り当て、セキュリティ グループ間およびセキュリティ グループ内でアクセス コントロールを適用することにより、ネットワーク内での原則的なアクセス コントロールを達成します。図 9-4 に SGACL ポリシーの例を示します。

図 9-4　SGACL ポリシーの例



Cisco TrustSec ネットワークでは、図 9-5 のように SGT の割り当てと SGACL の強制が実行されます。

図 9-5　Cisco TrustSec ネットワークでの SGT と SGACL



NX-OS デバイスは、従来の ACL の IP アドレスではなく、デバイス グループに Cisco TrustSec アクセス コントロール ポリシーを定義します。このような組み合わせの解除によって、ネットワーク全体でネットワーク デバイスを自由に移動し、IP アドレスを変更できます。ネットワーク トポロジ全体を変更することが可能です。ロールと許可が同じであれば、ネットワークが変更されてもセキュリティ ポリシーには影響しません。これによって、ACL のサイズが大幅に節約され、保守作業も簡単になります。

従来の IP ネットワークでは、設定されている ACE（アクセス コントロール エントリ）の数は次のように決定されます。

ACE の数 =（指定されている送信元の数）X（指定されている宛先の数）X（指定されている許可の数）

Cisco TrustSec では、次の式が使用されます。

ACE の数 = 指定されている許可の数

ここでは、次の内容について説明します。

送信元セキュリティ グループの判断

Cisco TrustSec クラウドの入口のネットワーク デバイスは、Cisco TrustSec クラウドにパケットを転送する際に、パケットに SGT をタグ付けできるように、Cisco TrustSec クラウドに入るパケットの SGT を判断する必要があります。出口のネットワーク デバイスは、パケットの SGT を判断し、SGACL を適用する必要があります。

ネットワーク デバイスは、次のいずれかの方法でパケットの SGT を判断します。

- ポリシー取得時に送信元の SGT を取得する — Cisco TrustSec 認証フェーズ後、ネットワーク デバイスは認証サーバからポリシーを取得します。認証サーバは、ピア デバイスが信頼できるかどうかを伝えます。ピア デバイスが信頼できる場合、認証サーバはそのピア デバイスから着信するすべてのパケットに適用する SGT も提供します。
- Cisco TrustSec ヘッダーの送信元 SGT フィールドを取得する — 信頼できるピア デバイスからパケットが着信した場合、Cisco TrustSec ヘッダーの SGT フィールドで正しい値が伝送されます。これは、そのパケットにとって、そのネットワーク デバイスが Cisco TrustSec クラウド内の最初のネットワーク デバイスではない場合に適用されます。
- 送信元 IP アドレスに基づいて送信元 SGT を検索する — 場合によっては、送信元 IP アドレスに基づいてパケットの SGT を判断するように手動でパケットを設定することもできます。SGT Exchange Protocol（SXP）も、IP-address-to-SGT マッピング テーブルに値を格納できます。

宛先セキュリティ グループの判断

Cisco TrustSec クラウドの出口のネットワーク デバイスは、SGACL を適用する宛先グループを判断します。場合によっては、入口のデバイスまたは出口以外のその他のデバイスが使用できる宛先グループの情報を持っていることもあります。このような場合、SGACL は出口のデバイスではなく、これらのデバイスに適用されます。

Cisco TrustSec は、パケットの宛先グループを次の方法で判断します。

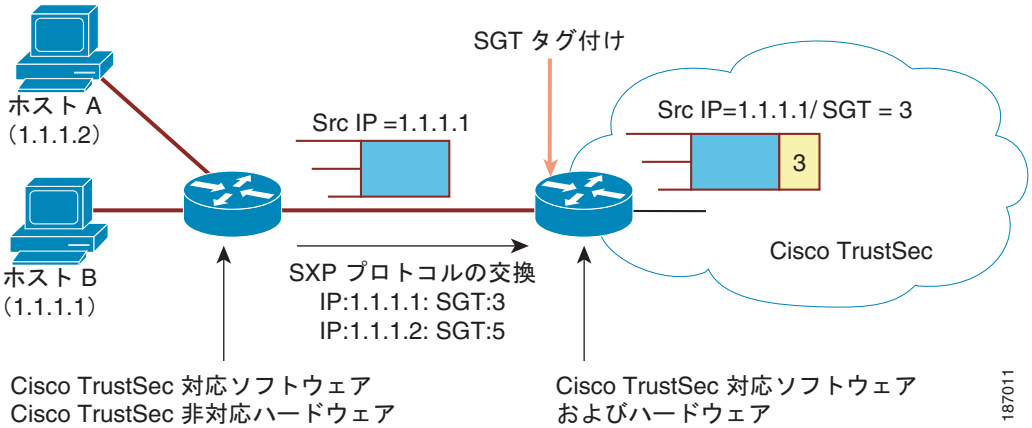
- ポリシー取得時に出力ポートの宛先 SGT を取得する
- 宛先 IP アドレスに基づいて宛先 SGT を検索する。

SXP によるレガシー アクセス ネットワークへの SGT の伝播

アクセス レイヤの NX-OS デバイス ハードウェアは Cisco TrustSec をサポートしています。Cisco TrustSec ハードウェアがないと、Cisco TrustSec ソフトウェアはパケットに SGT をタグ付けできません。SXP を使用すると、Cisco TrustSec のハードウェア サポートがないネットワーク デバイスに SGT を伝播 できます。

SXP はアクセス レイヤ デバイスと宛先レイヤ デバイスの間で動作します。アクセス レイヤ デバイスは SXP を使用して、SGT とともに Cisco TrustSec 認証デバイスの IP アドレスを宛先スイッチに渡します。Cisco TrustSec 対応のソフトウェアとハードウェアを両方備えたディストリビューション デバイスはこの情報を使用して、パケットに適切にタグを付けます（図 9-6 を参照）。

図 9-6　SXP プロトコルによる SGT 情報の伝播



許可とポリシーの取得

認証が終了すると、サプリカントと AT はいずれも認証サーバからセキュリティ ポリシーを取得します。サプリカントと AT はお互いに対してポリシーを強制します。サプリカントと AT はいずれも、認証後に受信したピア デバイス ID を提供します。ピア デバイス ID を使用できない場合、Cisco TrustSec は手動で設定されたピア デバイス ID を使用できます。

認証サーバは次の属性を返します。

- Cisco TrustSec の信頼状態 — パケットに SGT を付けるにあたり、ネイバー デバイスが信用できるかどうかを示します。
- ピア SGT — ピアが属しているセキュリティ グループを示します。ピアが信頼できない場合は、ピアから受信したすべてのパケットにこの SGT がタグ付けされます。SGACL がピアの SGT に関連付けられているかどうかデバイスが認識できないと、そのデバイスは SGACL を取得するために追加要求を送信する場合もあります。
- 許可期限 — ポリシーの期限が切れるまでの秒数を示します。シスコ独自の属性値（AV）ペアは、許可または Cisco TrustSec デバイスへのポリシー応答の期限を表します。Cisco TrustSec デバイスはポリシーと許可を期限が切れる前にリフレッシュする必要があります。

ヒント　Cisco TrustSec デバイスは、認証サーバからピアの適切なポリシーを取得できない場合に備えて、最小限のデフォルト アクセス ポリシーをサポートする必要があります。

環境データのダウンロード

Cisco TrustSec 環境データは、Cisco TrustSec ノードとしてのデバイスの機能を支援するひとまとまりの情報またはポリシーです。デバイスは、Cisco TrustSec クラウドに最初に加入する際に、認証サーバから環境データを取得しますが、一部のデータをデバイスに手動で設定することもできます。たとえば、Cisco TrustSec のシード デバイスには認証サーバの情報を設定する必要がありますが、この情報は、デバイスが認証サーバから取得するサーバ リストを使用して、あとで追加することができます。

デバイスは、期限前に Cisco TrustSec 環境データをリフレッシュする必要があります。データの期限が切れていなければ、デバイスはデータをキャッシュしてリブート後に再使用することもできます。

デバイスは RADIUS を使用して、認証サーバから次の環境データを取得します。

- サーバ リスト ― クライアントがその後の RADIUS 要求に使用できるサーバのリスト（認証および許可の両方）
- デバイス SGT ― そのデバイス自体が属しているセキュリティ グループ
- 有効期間 ― Cisco TrustSec デバイスが環境データをリフレッシュする頻度を左右する期間

RADIUS リレー機能

802.1X 認証プロセスで Cisco TrustSec AT のロールを引き受ける NX-OS デバイスは、認証サーバへの IP 接続を通じて、UDP/IP での RADIUS メッセージの交換により、認証サーバからポリシーと許可を取得します。サプリカント デバイスは認証サーバとの IP 接続がなくてもかまいません。サプリカントに 認証サーバとの IP 接続 がない場合、Cisco TrustSec は AT をサプリカントの RADIUS リレーとして機能させることができます。

サプリカントは、RADIUS サーバの IP アドレスと UDP ポートを持つ Cisco TrustSec AT に特別な EAP over LAN（EAPOL）メッセージを送信し、RADIUS 要求を完了します。Cisco TrustSec AT は受信した EAPOL メッセージから RADIUS 要求を抽出し、これを UDP/IP を通じて認証サーバに送信します。認証サーバから RADIUS 応答が返ると、Cisco TrustSec AT はメッセージを EAPOL フレームにカプセル化して、サプリカントに転送します。

バーチャライゼーション サポート

Cisco TrustSec の設定および動作は、各 Virtual Device Context（VDC）に固有です。VDC の詳細については、『*Cisco NX-OS Virtual Device Context Configuration Guide, Release 4.0*』を参照してください。

Cisco TrustSec のライセンス要件

この機能のライセンス要件は次の表のとおりです。

製品	ライセンス要件
NX-OS	デフォルト以外の VDC を作成するには、Advanced Services ライセンスが必要です。NX-OS のライセンス スキームおよびライセンスの取得方法と適用方法に関する詳細は、『*Cisco NX-OS Licensing Guide, Release 4.0*』を参照してください。 （注） Cisco TrustSec ライセンスには猶予期間はありません。Cisco TrustSec を使用するためには、事前に Advanced Services ライセンスを取得しインストールする必要があります。

Cisco TrustSec の前提条件

Cisco TrustSec の前提条件は次のとおりです。

- Advance Service ライセンスをインストールする必要があります。
- 802.1X 機能をイネーブルにする必要があります。

注意事項および制約事項

Cisco TrustSec に関する注意事項と制約事項は次のとおりです。

- Cisco TrustSec は認証に RADIUS を使用します。
- 1 つのインターフェイスに、Cisco TrustSec と 802.1X を両方設定することはできません。設定できるのはこれらのどちらか一方です。ただし、Cisco TrustSec で EAP-FAST 認証を使用するには、802.1X 機能をイネーブルにする必要があります。
- Cisco TrustSec の AAA 認証および許可は、Cisco Secure Access Control Server（ACS）でのみサポートされます。
- Cisco TrustSec は IPv4 アドレスのみをサポートします。
- SXP は管理（mgmt 0）インターフェイスを使用できません。
- 半二重モードのインターフェイスでは、Cisco TrustSec をイネーブルにできません。

Cisco TrustSec の設定

ここでは、次の内容について説明します。

Cisco TrustSec 機能のイネーブル化

Cisco TrustSec を設定するには、その前に、NX-OS デバイス上で 802.1X と Cisco TrustSec の機能をイネーブルにする必要があります。

（注）　Cisco TrustSec 機能をイネーブルにすると、その後に 802.1X 機能をディセーブルにすることはできません。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switchto vdc** コマンドを使用します）。

手順の概要

1. **config t**
2. **feature dot1x**
3. **feature cts**
4. **exit**
5. **show cts**
6. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	`config t`
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	`feature dot1x`
	
	例：
	`switch(config)# feature dot1x`
		802.1X 機能をイネーブルにします。

ステップ 3	`feature cts`
	
	例：
	`switch(config)# feature cts`
		Cisco TrustSec 機能をイネーブルにします。

	コマンド	目的

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 5	**show cts** **例：** `switch# show cts`	（任意）Cisco TrustSec の設定を表示します。
ステップ 6	**copy running-config startup-config** **例：** `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Cisco TrustSec デバイスの証明書の設定

ネットワーク内の Cisco TrustSec 対応 NX-OS デバイス各々に、固有の Cisco TrustSec 証明書を設定する必要があります。Cisco TrustSec は証明書のパスワードをデバイスの認証に使用します。

（注）　Cisco Secure ACS にも NX-OS デバイスの Cisco TrustSec 証明書を設定する必要があります（「*Configuration Guide for the Cisco Secure ACS*」を参照）。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switchto vdc** コマンドを使用します）。

Cisco TrustSec がイネーブルになっていることを確認します（「Cisco TrustSec 機能のイネーブル化」[p.9-13] を参照）。

手順の概要

1. **config t**
2. **cts device-id** *name* **password** *password*
3. **exit**
4. **show cts**
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**cts device-id** *name* **password** *password* **例：** `switch(config)# cts device-id MyDevice1 password CiscO321`	固有のデバイス ID およびパスワードを設定します。*name* 引数は、最大 32 文字で大文字と小文字を区別します。

	コマンド	目的
ステップ 3	**exit** **例：** switch(config)# exit switch#	コンフィギュレーション モードを終了します。
ステップ 4	**show cts** **例：** switch# show cts	（任意）Cisco TrustSec の設定を表示します。
ステップ 5	**copy running-config startup-config** **例：** switch# copy running-config startup-config	（任意）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Cisco TrustSec の AAA の設定

Cisco TrustSec の認証に Cisco Secure ACS を使用できます。ネットワーク クラウド内の Cisco TrustSec 対応 NX-OS デバイスの 1 つに、RADIUS サーバ グループを設定し、デフォルトの AAA 認証および許可を指定する必要があります。Cisco TrustSec は RADIUS リレーをサポートしているため、AAA を設定するのは、Cisco Secure ACS に直接接続されている NX-OS シード デバイスのみです。Cisco TrustSec がイネーブルのすべての NX-OS デバイスに対して、Cisco TrustSec は自動的にプライベート AAA サーバ グループ aaa-private-sg を提供します。NX-OS シード デバイスは管理 VRF を使用して、Cisco Secure ACS と通信します。

（注）　Cisco TrustSec をサポートしているのは、Cisco Secure ACS のみです。

RADIUS サーバの設定に関する詳細は、第 3 章「RADIUS の設定」を参照してください。RADIUS サーバ グループの設定に関する詳細は、第 2 章「AAA の設定」を参照してください。

ここでは、次の内容について説明します。

- Cisco TrustSec シード NX-OS デバイスでの AAA の設定（p.9-15）
- Cisco TrustSec 非シード NX-OS デバイスでの AAA の設定（p.9-18）

Cisco TrustSec シード NX-OS デバイスでの AAA の設定

ここでは、Cisco TrustSec ネットワーク クラウド内のシード NX-OS デバイスに AAA を設定する手順を説明します。

（注）　シード NX-OS デバイスの AAA RADIUS サーバ グループを設定する際には、VRF を指定する必要があります。管理 VRF を使用する場合、ネットワーク クラウド内の非シード デバイスにそれ以上の設定を行う必要はありません。異なる VRF を使用する場合は、非シード デバイスに VRF を設定する必要があります（「Cisco TrustSec 非シード NX-OS デバイスでの AAA の設定」[p.9-18] を参照）。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switch to vdc** コマンドを使用します）。

Cisco ACS の IPv4 または IPv6 のアドレスまたはホスト名を取得します。

Cisco TrustSec がイネーブルになっていることを確認します（「Cisco TrustSec 機能のイネーブル化」[p.9-13] を参照）。

手順の概要

1. **config t**
2. **radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **password** *password* **pac**
3. **show radius-server**
4. **aaa group server radius** *group-name*
5. **server** {*ipv4-address* | *ipv6-address* | *hostname*}
6. **use-vrf** *vrf-name*
7. **exit**
8. **aaa authentication dot1x default group** *group-name*
9. **aaa authorization cts default group** *group-name*
10. **exit**
11. **show radius-server groups** [*group-name*]
12. **show aaa authentication**
13. **show aaa authorization**
14. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **password** *password* **pac** **例：** `switch(config)# radius-server host 10.10.1.1 password L1a0K2s9 pac`	RADIUS サーバ ホストにパスワードと PAC を設定します。
ステップ 3	**show radius-server** **例：** `switch# show radius-server`	（任意）RADIUS サーバの設定を表示します。

ステップ 4	**aaa group server radius** *group-name*
	
	例：
	`switch(config)# aaa group server radius Rad1`
	`switch(config-radius)#`
		RADIUS サーバ グループを指定し、RADIUS サーバ グループ コンフィギュレーション モードを開始します。

ステップ 5	**server** {*ipv4-address* | *ipv6-address* | *hostname*} **例：** `switch(config-radius)# server 10.10.1.1`	RADIUS サーバ ホストのアドレスを指定します。

	コマンド	目的
ステップ 6	**use-vrf** *vrf-name* **例：** `switch(config-radius)# use-vrf management`	AAA サーバ グループの管理 VRF を指定します。 **（注）** 管理 VRF を使用する場合、ネットワーク クラウド内の非シード デバイスにそれ以上の設定を行う必要はありません。異なる VRF を使用する場合は、非シード デバイスに VRF を設定する必要があります（「Cisco TrustSec 非シード NX-OS デバイスでの AAA の設定」[p.9-18] を参照）。

ステップ 7	**exit**
	
	例：
	`switch(config-radius)# exit`
	`switch(config)#`
		RADIUS サーバ グループ コンフィギュレーション モードを終了します。

ステップ 8	**aaa authentication dot1x default group** *group-name* **例：** `switch(config)# aaa authentication dot1x default group Rad1`	802.1X 認証に使用する RADIUS サーバ グループを指定します。
ステップ 9	**aaa authorization cts default group** *group-name* **例：** `switch(config)# aaa authentication cts default group Rad1`	Cisco TrustSec 認証に使用する RADIUS サーバ グループを指定します。

ステップ 10	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 11	**show radius-server groups** [*group-name*] **例：** `switch# show radius-server group rad2`	（任意）RADIUS サーバ グループの設定を表示します。
ステップ 12	**show aaa authentication** **例：** `switch# show aaa authentication`	（任意）AAA 認証の設定を表示します。
ステップ 13	**show aaa authorization** **例：** `switch# show aaa authorization`	（任意）AAA 許可の設定を表示します。
ステップ 14	**show cts pacs** **例：** `switch# show show cts pacs`	（任意）Cisco TrustSec PAC 情報を表示します。
ステップ 15	**copy running-config startup-config** **例：** `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Cisco TrustSec 非シード NX-OS デバイスでの AAA の設定

Cisco TrustSec はネットワーク クラウド内の非シード NX-OS デバイスに aaa-private-sg という名前の AAA サーバ グループを設定します。デフォルトでは、aaa-private-sg サーバ グループは Cisco Secure ACS との通信に管理 VRF を使用し、非シード NX-OS デバイスに対するそれ以上の設定は必要ありません。ただし、異なる VRF の使用を選択した場合は、正しい VRF を使用するように、非シード NX-OS デバイスの aaa-private-sg を変更する必要があります。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switch to vdc** コマンドを使用します）。

Cisco TrustSec がイネーブルになっていることを確認します（「Cisco TrustSec 機能のイネーブル化」[p.9-13] を参照）。

ネットワーク内のシード NX-OS デバイスが設定されていることを確認します（「Cisco TrustSec シード NX-OS デバイスでの AAA の設定」[p.9-15] を参照）。

手順の概要

1. **config t**
2. **aaa group server radius aaa-private-sg**
3. **use-vrf** *vrf-name*
4. **exit**
5. **show radius-server groups** [*group-name*]
6. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**aaa group server radius aaa-private-sg**
	
	例：
	`switch(config)# aaa group server radius aaa-private-sg`
	`switch(config-radius)#`
		RADIUS サーバ グループ aaa-private-sg を指定し、RADIUS サーバ グループ コンフィギュレーション モードを開始します。

ステップ 3	**use-vrf** *vrf-name* **例：** `switch(config-radius)# use-vrf MyVRF`	AAA サーバ グループの管理 VRF を指定します。

ステップ 4	**exit**
	
	例：
	`switch(config-radius)# exit`
	`switch(config)#`
		コンフィギュレーション モードを終了します。

ステップ 5	**show radius-server groups aaa-private-sg** **例：** `switch(config)# show radius-server groups aaa-private-sg`	（任意）RADIUS サーバ グループの設定を表示します。

	コマンド	目的

ステップ 6	`copy running-config startup-config`
	
	例：
	`switch(config)# copy running-config startup-config`
		(任意) 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Cisco TrustSec の認証、許可、SAP、およびデータ パス セキュリティの設定

ここでは、次の内容について説明します。

- Cisco TrustSec 認証のイネーブル化（p.9-19）
- インターフェイスに対する Cisco TrustSec データパス リプレイ保護の設定（p.9-21）
- インターフェイスに対する Cisco TrustSec SAP 動作モードの設定（p.9-22）
- インターフェイスの SAP キーの再生成（p.9-24）

Cisco TrustSec の認証および許可の設定プロセス

Cisco TrustSec の認証および許可を設定するには、次の手順を行います。

ステップ 1　Cisco TrustSec 機能をイネーブルにします（「Cisco TrustSec 機能のイネーブル化」[p.9-13] を参照）。

ステップ 2　Cisco TrustSec の認証をイネーブルにします（「Cisco TrustSec 認証のイネーブル化」[p.9-19] を参照）。

ステップ 3　インターフェイスに対して Cisco TrustSec の 802.1X 認証をイネーブルにします（「Cisco TrustSec 認証のイネーブル化」[p.9-19] を参照）。

Cisco TrustSec 認証のイネーブル化

インターフェイスに対して Cisco TrustSec 認証をイネーブルにする必要があります。デフォルトでは、データパス リプレイ保護機能がイネーブルになり、SAP 動作モードは GCM-encrypt です。

注意　Cisco TrustSec 認証の設定を有効にするには、インターフェイスのイネーブル化とディセーブル化を行う必要があり、インターフェイス上のトラフィックが中断されます。

（注）　Cisco TrustSec の 802.1X モードをイネーブルにすると、そのインターフェイス上の許可と SAP がイネーブルになります。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switchto vdc** コマンドを使用します）。

手順の概要

1. **config t**
2. **interface ethernet** *slot*/*port* [**-** *port2*]
3. **cts dot1x**
4. **exit**
5. **no data-path replay protection**
6. **sap modelist** {**gmc-encrypt** | **gmac** | **no-encap** | **null**}
7. **shutdown**
8. **no shutdown**
9. **exit**
10. **show cts interface all**
11. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet** *slot*/*port* [**-** *port2*]
	
	例：
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		単一ポートまたはポート範囲を指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**cts dot1x**
	
	例：
	`switch(config-if)# cts dot1x`
	`switch(config-if-cts-dot1x)#`
		Cisco TrustSec の 802.1X 認証をイネーブルにして、Cisco TrustSec 802.1X コンフィギュレーション モードを開始します。

ステップ 4	**no replay-protection** **例：** `switch(config-if-cts-dot1x)# no replay-protection`	（任意）リプレイ保護をディセーブルにします。デフォルトはイネーブルです。
ステップ 5	**sap modelist** {**gcm-encrypt** | **gmac** | **no-encap** | **null**} **例：** `switch(config-if-cts-dot1x)# sap modelist gcm-encrypt`	（任意）インターフェイスに SAP 動作モードを設定します。 • **gcm-encrypt** — GCM 暗号化 • **gmac** — GCM 認証のみ • **no-encap** — SAP の非カプセル化および SGT 非挿入 • **null** — 認証または暗号化なしのカプセル化 デフォルトは **gcm-encrypt** です。

ステップ 6	**exit**
	
	例：
	`switch(config-if-cts-dot1x)# exit`
	`switch(config-if)#`
		Cisco TrustSec 802.1X コンフィギュレーション モードを終了します。

	コマンド	目的
ステップ 7	**shutdown** **例：** `switch(config-if)# shutdown`	インターフェイスをディセーブルにします。
ステップ 8	**no shutdown** **例：** `switch(config-if)# no shutdown`	インターフェイスをイネーブルにして、インターフェイスの Cisco TrustSec 認証をイネーブルにします。

ステップ 9	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 10	**show cts interface all** **例：** `switch(config)# show cts interface all`	(任意)インターフェイスに対する Cisco TrustSec の設定を表示します。
ステップ 11	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	(任意) 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスに対する Cisco TrustSec データパス リプレイ保護の設定

デフォルトでは、NX-OS ソフトウェアによってデータパス リプレイ保護機能をイネーブルにします。接続デバイスが SAP をサポートしていない場合は、レイヤ 2 Cisco TrustSec のインターフェイスでデータパス リプレイ保護をディセーブルにできます。

注意　データパス リプレイ保護の設定を有効にするには、インターフェイスのイネーブル化とディセーブル化を行う必要があり、インターフェイス上のトラフィックが中断されます。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switch to vdc** コマンドを使用します）。

インターフェイスの Cisco TrustSec 認証がイネーブルになっていることを確認します（「Cisco TrustSec 認証のイネーブル化」[p.9-19] を参照）。

手順の概要

1. **config t**
2. **interface ethernet** *slot/port* [**-** *port2*]
3. **cts dot1x**
4. **no replay-protection**
5. **exit**
6. **shutdown**
7. **no shutdown**
8. **exit**
9. **show cts**
10. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet** *slot*/*port* [**-** *port2*]
	
	例：
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		単一ポートまたはポート範囲を指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**cts dot1x**
	
	例：
	`switch(config-if)# cts dot1x`
	`switch(config-if-cts-dot1x)#`
		Cisco TrustSec の 802.1X 認証をイネーブルにして、Cisco TrustSec 802.1X コンフィギュレーション モードを開始します。

ステップ 4	**no replay-protection** **例：** `switch(config-if-cts-dot1x)# no replay-protection`	データパス リプレイ保護をディセーブルにします。デフォルトはイネーブルです。

ステップ 5	**exit**
	
	例：
	`switch(config-if-cts-dot1x)# exit`
	`switch(config-if)#`
		Cisco TrustSec 802.1X コンフィギュレーション モードを終了します。

ステップ 6	**shutdown** **例：** `switch(config-if)# shutdown`	インターフェイスをディセーブルにします。
ステップ 7	**no shutdown** **例：** `switch(config-if)# no shutdown`	インターフェイスをイネーブルにして、インターフェイスのデータパス リプレイ保護機能をディセーブルにします。

ステップ 8	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 9	**show cts interface all** **例：** `switch(config)# show cts interface all`	(任意)インターフェイスに対する Cisco TrustSec の設定を表示します。
ステップ 10	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	(任意) 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスに対する Cisco TrustSec SAP 動作モードの設定

レイヤ 2 Cisco TrustSec のインターフェイスに SAP 動作モードを設定できます。デフォルトの SAP 動作モードは GCM-encrypt です。

注意　SAP 動作モードの設定を有効にするには、インターフェイスのイネーブル化とディセーブル化を行う必要があり、インターフェイス上のトラフィックが中断されます。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switch to vdc** コマンドを使用します）。

インターフェイスの Cisco TrustSec 認証がイネーブルになっていることを確認します（「Cisco TrustSec 認証のイネーブル化」[p.9-19] を参照）。

手順の概要

1. **config t**
2. **interface ethernet** *slot*/*port* [**-** *port2*]
3. **cts dot1x**
4. **sap modelist gcm-encrypt**
   sap modelist gmac
   sap modelist no-encap
   sap modelist null
5. **exit**
6. **shutdown**
7. **no shutdown**
8. **exit**
9. **show cts interface all**
10. **copy running-config startup-config**

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface ethernet** *slot*/*port* [**-** *port2*] **例：** switch(config)# interface ethernet 2/2 switch(config-if)#	単一のインターフェイスまたはインターフェイス範囲を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**cts dot1x** **例：** switch(config-if)# cts dot1x switch(config-if-cts-dot1x)#	Cisco TrustSec の 802.1X 認証をイネーブルにして、Cisco TrustSec 802.1X コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 4	**sap modelist gcm-encrypt** **例：** `switch(config-if-cts-dot1x)# sap modelist gcm-encrypt`	インターフェイスに GCM 暗号化の SAP モードを設定します。 デフォルトは **gcm-encrypt** です。
	sap modelist gmac **例：** `switch(config-if-cts-dot1x)# sap modelist gmac`	インターフェイスに GCM 認証のみの SAP モードを設定します。
	sap modelist no-encap **例：** `switch(config-if-cts-dot1x)# sap modelist no-encap`	インターフェイスに非カプセル化および SGT 非挿入の SAP を設定します。
	sap modelist null **例：** `switch(config-if-cts-dot1x)# sap modelist null`	インターフェイスに、認証も暗号化もないカプセル化 SAP を設定します。カプセル化されるのは SGT だけです。

ステップ 5	**exit**
	
	例：
	`switch(config-if-cts-dot1x)# exit`
	`switch(config-if)#`
		Cisco TrustSec 802.1X コンフィギュレーション モードを終了します。

ステップ 6	**shutdown** **例：** `switch(config-if)# shutdown`	インターフェイスをディセーブルにします。
ステップ 7	**no shutdown** **例：** `switch(config-if)# no shutdown`	インターフェイスをイネーブルにして、そのインターフェイスの SAP 動作モードをイネーブルにします。

ステップ 8	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 9	**show cts interface all** **例：** `switch(config)# show cts interface all`	（任意）インターフェイスに対する Cisco TrustSec の設定を表示します。
ステップ 10	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスの SAP キーの再生成

SAP プロトコル交換をトリガーして、新しいキー セットを生成し、インターフェイス上のデータ トラフィックを保護できます。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switchto vdc** コマンドを使用します）。

Cisco TrustSec がイネーブルになっていることを確認します（「Cisco TrustSec 機能のイネーブル化」[p.9-13] を参照）。

手順の概要

1. **cts rekey ethernet** *slot/port*
2. **show cts interface all**

詳細な手順

	コマンド	目的
ステップ 1	**cts rekey ethernet** *slot/port* **例：** `switch# cts rekey ethernet 2/3`	インターフェイスの SAP キーを生成します。
ステップ 2	**show cts interface all** **例：** `switch# show cts interface all`	（任意）インターフェイスの Cisco TrustSec 設定を表示します。

手動での Cisco TrustSec 認証の設定

NX-OS デバイスに Cisco Secure ACS へのアクセス権がない場合や、MAC アドレス認証バイパス機能がイネーブルになっていて認証が必要でない場合には、インターフェイスに手動で Cisco TrustSec を設定することも可能です。接続の両側のインターフェイスに手動で設定する必要があります。

（注） 半二重モードのインターフェイスでは、Cisco TrustSec をイネーブルにできません。インターフェイスが半二重モードに設定されているかどうかを調べるには、**show interface** コマンドを使用します。

注意 手動モードでの Cisco TrustSec の設定を有効にするには、インターフェイスのイネーブル化とディセーブル化を行う必要があり、インターフェイス上のトラフィックが中断されます。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switch to vdc** コマンドを使用します）。

Cisco TrustSec がイネーブルになっていることを確認します（「Cisco TrustSec 機能のイネーブル化」[p.9-13] を参照）。

手順の概要

1. **config t**
2. **interface ethernet** *slot/port*
3. **cts manual**
4. **sap pmk** *key* **modelist** {**gcm-encrypt** | **gmac** | **no-encap** | **null**}
5. **policy dynamic identity** *peer-name*

   policy static sgt *tag* [**trusted**]
6. **exit**
7. **shutdown**

8. **no shutdown**
9. **exit**
10. **show cts interface all**
11. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet** *slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**cts manual**
	
	例：
	`switch(config-if)# cts manual`
	`switch(config-if-cts-manual)#`
		Cisco TrustSec 手動コンフィギュレーション モードを開始します。
		
		（注） 半二重モードのインターフェイスでは、Cisco TrustSec をイネーブルにできません。

ステップ 4	**sap pmk** *key* [**modelist** {**gcm-encrypt** | **gmac** | **no-encap** | **null**}] **例**： `switch(config-if-cts-manual)# sap pmk fedbaa modelist gmac`	SAP の Pairwise Master Key（PMK）と動作モードを設定します。*key* 引数は、最大 32 文字の偶数文字数の 16 進値です。モードのリストには、次に示すデータ パス暗号化と認証の暗号モードを指定します。 • **gcm-encrypt —** GCM 暗号化モード • **gmac —** GCM 認証モード • **no-encap —** 非カプセル化および SGT 非挿入 • **null —** 認証または暗号化なしの SGT カプセル化 デフォルトのモードは **gcm-encrypt** です。

	コマンド	目的
ステップ 5	**policy dynamic identity** *peer-name* **例：** `switch(config-if-cts-manual)# policy dynamic identity MyDevice2`	ダイナミック許可ポリシーのダウンロードを設定します。*peer-name* 引数は、ピア デバイスの Cisco TrustSec デバイス ID です。ピア名では、大文字と小文字が区別されます。 **（注）** Cisco TrustSec 証明書が設定されていること（「Cisco TrustSec デバイスの証明書の設定」[p.9-14] を参照）および Cisco TrustSec の AAA が設定されていること（「Cisco TrustSec の AAA の設定」[p.9-15] を参照）を確認します。
	policy static sgt *tag* [**trusted**] **例：** `switch(config-if-cts-manual)# policy static sgt 0x03`	スタティック許可ポリシーを設定します。*tag* 引数は、0x0 から 0xffff の 16 進形式で指定します。**trusted** キーワードを指定すると、SGT 付きでインターフェイスにトラフィックが着信した場合、そのタグは上書きされません。

ステップ 6	**exit**
	
	例：
	`switch(config-if-cts-manual)# exit`
	`switch(config-if)#`
		Cisco TrustSec 手動コンフィギュレーション モードを終了します。

ステップ 7	**shutdown** **例：** `switch(config-if)# shutdown`	インターフェイスをディセーブルにします。
ステップ 8	**no shutdown** **例：** `switch(config-if)# no shutdown`	インターフェイスをイネーブルにして、インターフェイスの Cisco TrustSec 認証をイネーブルにします。

ステップ 9	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 10	**show cts interface all** **例：** `switch# show cts interface all`	（任意）インターフェイスの Cisco TrustSec 設定を表示します。
ステップ 11	**copy running-config startup-config** **例：** `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SGACL ポリシーの設定

ここでは、次の内容について説明します。

- SGACL ポリシーの設定プロセス（p.9-28）
- VLAN に対する SGACL ポリシーの強制のイネーブル化（p.9-28）
- VRF に対する SGACL ポリシーの強制のイネーブル化（p.9-29）
- IPv4 アドレスと SGACL SGT のマッピングの手動設定（p.9-31）
- SGACL ポリシーの手動設定（p.9-33）
- ダウンロードされた SGACL ポリシーの表示（p.9-36）

- ダウンロードされた SGACL ポリシーのリフレッシュ（p.9-36）

SGACL ポリシーの設定プロセス

Cisco TrustSec の SGACL ポリシーを設定するには、次の手順を行います。

ステップ 1　レイヤ 2 インターフェイスの場合は、Cisco TrustSec がイネーブルになっているインターフェイスがある VLAN に対して、SGACL ポリシーの強制をイネーブルにします（「VLAN に対する SGACL ポリシーの強制のイネーブル化」[p.9-28] を参照）。

ステップ 2　レイヤ 3 インターフェイスの場合は、Cisco TrustSec がイネーブルになっているインターフェイスがある VRF に対して、SGACL ポリシーの強制をイネーブルにします（「VRF に対する SGACL ポリシーの強制のイネーブル化」[p.9-29] を参照）。

ステップ 3　SGACL ポリシーの設定のダウンロードに Cisco Secure ACS 上の AAA を使用しない場合は、SGACL のマッピングとポリシーを手動で設定します（「IPv4 アドレスと SGACL SGT のマッピングの手動設定」[p.9-31] および「SGACL ポリシーの手動設定」[p.9-33] を参照）。

VLAN に対する SGACL ポリシーの強制のイネーブル化

SGACL を使用する場合、Cisco TrustSec がイネーブルになっているレイヤ 2 インターフェイスがある VLAN 内で、SGACL ポリシーの強制をイネーブルにする必要があります。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switchto vdc** コマンドを使用します）。

Cisco TrustSec がイネーブルになっていることを確認します（「Cisco TrustSec 機能のイネーブル化」[p.9-13] を参照）。

手順の概要

1. **config t**
2. **vlan** *vlan-id*
3. **cts role-based enforcement**
4. **exit**
5. **show cts role-based enable**
6. **copy running-config startup-config**

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**vlan** *vlan-id* **例：** switch(config)# vlan 10 switch(config-vlan)#	VLAN を指定し、VLAN コンフィギュレーション モードを開始します。
ステップ 3	**cts role-based enforcement** **例：** switch(config-vlan)# cts role-based enforcement	VLAN に対する Cisco TrustSec SGACL ポリシーの強制をイネーブルにします。
ステップ 4	**exit** **例：** switch(config-vlan)# exit switch(config)#	VLAN コンフィギュレーション モードを終了します。
ステップ 5	**show cts role-based enable** **例：** switch(config)# show cts role-based enable	（任意）Cisco TrustSec SGACL 強制の設定を表示します。
ステップ 6	**copy running-config startup-config** **例：** switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VRF に対する SGACL ポリシーの強制のイネーブル化

SGACL を使用する場合、Cisco TrustSec がイネーブルになっているレイヤ 3 インターフェイスがある VRF 内で、SGACL ポリシーの強制をイネーブルにする必要があります。

（注）　管理 VRF の場合は、SGACL ポリシーの強制をイネーブルにできません。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switchto vdc** コマンドを使用します）。

Cisco TrustSec がイネーブルになっていることを確認します（「Cisco TrustSec 機能のイネーブル化」[p.9-13] を参照）。

ダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査がイネーブルになっていること（第 15 章「DAI の設定」を参照）または Dynamic Host Configuration Protocol（DHCP）スヌーピングがイネーブルになっていること（第 14 章「DHCP スヌーピングの設定」を参照）を確認します。

手順の概要

1. **config t**
2. **vrf context** *vrf-name*
3. **cts role-based enforcement**
4. **exit**
5. **show cts role-based enable**
6. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**vrf context** *vrf-name*
	
	例：
	`switch(config)# vrf context MyVrf`
	`switch(config-vrf)#`
		VRF を指定し、VRF コンフィギュレーション モードを開始します。

ステップ 3	**cts role-based enforcement** **例：** `switch(config-vrf)# cts role-based enforcement`	VRF に対する Cisco TrustSec SGACL ポリシーの強制をイネーブルにします。

ステップ 4	**exit**
	
	例：
	`switch(config-vrf)# exit`
	`switch(config)#`
		VRF コンフィギュレーション モードを終了します。

ステップ 5	**show cts role-based enable** **例：** `switch(config)# show cts role-based enable`	（任意）Cisco TrustSec SGACL 強制の設定を表示します。
ステップ 6	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Cisco TrustSec SGT の手動設定

SGACL が実行されるパケットに、固有の Cisco TrustSec SGT（セキュリティ グループ タグ）を手動で設定できます。

（注） Cisco Secure ACS にも、NX-OS デバイスの Cisco TrustSec 証明書を設定する必要があります。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switchto vdc** コマンドを使用します）。

手順の概要

1. **config t**
2. **cts sgt** *tag*
3. **exit**
4. **show cts environment-data**
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**cts sgt** *tag* **例：** `switch(config)# cts device-id MyDevice1 password CiscO321`	デバイスから送信されるパケットの SGT を設定します。*tag* 引数は、**0x***hhhh* の形式の 16 進値です。有効値の範囲は 0x1 ～ 0xfffd です。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**show cts environment-data** **例：** `switch# show cts environment-data`	（任意）Cisco TrustSec の環境データ情報を表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

IPv4 アドレスと SGACL SGT のマッピングの手動設定

SGACL ポリシー設定のダウンロードに Cisco Secure ACS を使用しない場合は、IPv4 アドレスと SGACL SGT のマッピングを VLAN または VRF に手動で設定できます。NX-OS デバイスで、Cisco Secure ACS、ダイナミック ARP 検査、DHCP スヌーピングを使用できない場合は、この機能を使用できます。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switchto vdc** コマンドを使用します）。

Cisco TrustSec がイネーブルになっていることを確認します（「Cisco TrustSec 機能のイネーブル化」[p.9-13] を参照）。

VLAN に対する SGACL ポリシーの強制がイネーブルになっていること（「VLAN に対する SGACL ポリシーの強制のイネーブル化」[p.9-28] を参照）または VRF に対する SGACL ポリシーの強制がイネーブルになっていること（「VRF に対する SGACL ポリシーの強制のイネーブル化」[p.9-29] を参照）を確認します。

SUMMARY STEPS

1. **config t**
2. **vlan** *vlan-id*

   vrf context *vrf-name*
3. **cts role-based sgt-map** *ipv4-address tag*
4. **exit**
5. **show cts role-based enable**
6. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**vlan** *vlan-id*
	
	例：
	`switch(config)# vlan 10`
	`switch(config-vlan)#`
		VLAN を指定し、VLAN コンフィギュレーション モードを開始します。

	vrf context *vrf-name*
	
	例：
	`switch(config)# vrf context MyVrf`
	`switch(config-vrf)#`
		VRF を指定し、VRF コンフィギュレーション モードを開始します。

ステップ 3	**cts role-based sgt-map** *ipv4-address tag* **例：** `switch(config-vlan)# cts role-based sgt-map 10.10.1.1 100`	VLAN に対する SGACL ポリシーの SGT マッピングを設定します。
	cts role-based sgt-map *ipv4-address tag* **例：** `switch(config-vrf)# cts role-based sgt-map 10.10.1.1 100`	VRF に対する SGACL ポリシーの SGT マッピングを設定します。

ステップ 4	**exit**
	
	例：
	`switch(config-vlan)# exit`
	`switch(config)#`
		VLAN コンフィギュレーション モードを終了します。

	exit
	
	例：
	`switch(config-vrf)# exit`
	`switch(config)#`
		VRF コンフィギュレーション モードを終了します。

ステップ 5	**show cts role-based sgt-map** **例：** `switch(config)# show cts role-based sgt-map`	（任意）Cisco TrustSec SGACL SGT のマッピング設定を表示します。
ステップ 6	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SGACL ポリシーの手動設定

SGACL ポリシー設定のダウンロードに Cisco Secure ACS を使用しない場合は、NX-OS デバイスに手動で SGACL ポリシーを設定できます。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switchto vdc** コマンドを使用します）。

Cisco TrustSec がイネーブルになっていることを確認します（「Cisco TrustSec 機能のイネーブル化」[p.9-13] を参照）。

VLAN に対する SGACL ポリシーの強制がイネーブルになっていること（「VLAN に対する SGACL ポリシーの強制のイネーブル化」[p.9-28] を参照）、または VRF に対する SGACL ポリシーの強制がイネーブルになっていること（「VRF に対する SGACL ポリシーの強制のイネーブル化」[p.9-29] を参照）を確認します。

手順の概要

1. **config t**
2. **cts role-based access-list** *list-name*
3. **deny all**

   deny icmp

   deny igmp

   deny ip

   deny tcp [{**dest** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number* | **range** *port-number1 port-number2*}]

   deny udp [{**dest** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number* | **range** *port-number1 port-number2*}]
4. **permit all**

   permit icmp

   permit igmp

   permit ip

   permit tcp [{**dest** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number* | **range** *port-number1 port-number2*}]

   permit udp [{**dest** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number* | **range** *port-number1 port-number2*}]
5. **exit**
6. **cts role-based sgt** {*sgt-value* | **any** | **unknown**} **dgt** {*dgt-value* | **any** | **unknown**} **access-list** *list-name*
7. **show cts role-based access-list**
8. **copy running-config startup-config**

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**cts role-based access-list** *list-name* **例：** switch(config)# cts role-based access-list MySGACL switch(config-rbacl)#	SGACL を指定し、ロールベース アクセス リスト コンフィギュレーション モードを開始します。*list-name* 引数には、大文字と小文字を区別して、最大 32 文字の英数字で値を指定します。
ステップ 3	**deny all** **例：** switch(config-rbacl)# deny all	すべてのトラフィックを拒否します。
	deny icmp **例：** switch(config-rbacl)# deny icmp	Denies Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）トラフィックを拒否します。
	deny igmp **例：** switch(config-rbacl)# deny igmp	Denies Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）トラフィックを拒否します。
	deny all **例：** switch(config-rbacl)# deny ip	IP トラフィックを拒否します。
	deny tcp [{**dest** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number* | **range** *port-number1 port-number2*}] **例：** switch(config-rbacl)# deny tcp src lt 10	TCP トラフィックを拒否します。デフォルトではすべての TCP トラフィックが拒否されます。*port-number*、*port-number1*、*port-number2* の引数の範囲は 0 ～ 65535 です。
	deny udp [{**dest** | **src**} {{**eq** | **gt** | **lt** | **neq**} ***port-number*** | **range** *port-number1 port-number2*}] **例：** switch(config-rbacl)# deny udp dest eq 100	UDP トラフィックを許可します。デフォルトではすべての UDP トラフィックが拒否されます。*port-number*、*port-number1*、*port-number2* 引数の範囲は、0 ～ 65535 です。

	コマンド	目的
ステップ 4	**permit all** **例：** switch(config-rbacl)# permit all	すべてのトラフィックを許可します。
	permit icmp **例：** switch(config-rbacl)# permit icmp	ICMP トラフィックを許可します。
	permit igmp **例：** switch(config-rbacl)# permit igmp	IGMP トラフィックを許可します。
	permit ip **例：** switch(config-rbacl)# permit ip	IP トラフィックを許可します。
	permit tcp [{**dest** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number* | **range** *port-number1 port-number2*}] **例：** switch(config-rbacl)# permit tcp	TCP トラフィックを許可します。デフォルトではすべての TCP トラフィックが許可されます。*port-number*、*port-number1*、*port-number2* の引数の範囲は 0 ～ 65535 です。*port-number2* 引数の値は、*port-number1* 引数よりも大きい値にする必要があります。
	permit udp [{**dest** | **src**} {{**eq** | **gt** | **lt** | **neq**} ***port-number*** | **range** *port-number1 port-number2*}] **例：** switch(config-rbacl)# permit udp dest ne 2000	UDP トラフィックを許可します。デフォルトではすべての UDP トラフィックが許可されます。*port-number*、*port-number1*、*port-number2* の引数の範囲は 0 ～ 65535 です。*port-number2* 引数の値は、*port-number1* 引数よりも大きい値にする必要があります。
ステップ 5	**exit** **例：** switch(config-rbacl)# exit switch(config)#	ロールベース アクセスリスト コンフィギュレーション モードを終了します。
ステップ 6	**cts role-based sgt** {*sgt-value* | **any** | **unknown**} **dgt** {*dgt-value* | **any** | **unknown**} **access-list** *list-name* **例：** switch(config)# cts role-based sgt 3 dgt 10 access-list MySGACL	SGT 値と SGACL をマッピングします。sgt-value 引数と dgt-value 引数の範囲は、0 ～ 65520 です。 **（注）** SGT と SGACL をマッピングするには、あらかじめ SGACL を作成しておく必要があります。
ステップ 7	**show cts role-based access-list** **例：** switch(config)# show cts role-based access-list	（任意）Cisco TrustSec SGACL の設定を表示します。
ステップ 8	**copy running-config startup-config** **例：** switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ダウンロードされた SGACL ポリシーの表示

Cisco TrustSec のデバイス証明書と AAA の設定後、Cisco Secure ACS からダウンロードされた Cisco TrustSec SGACL ポリシーを検証できます。NX-OS ソフトウェアは、インターフェイスに対する認証および許可を通じて、SXP によって、または IPv4 アドレスおよび SGACL SGT の手動マッピングから新しい SGT を学習すると、SGACL ポリシーをダウンロードします。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switchto vdc** コマンドを使用します）。

Cisco TrustSec がイネーブルになっていることを確認します（「Cisco TrustSec 機能のイネーブル化」[p.9-13] を参照）。

手順の概要

1. **show cts role-based access-list**

詳細な手順

	コマンド	目的

ステップ 1	`show cts role-based access-list`
	
	例：
	`switch# show cts role-based access-list`
		Cisco TrustSec SGACL を表示します（Cisco Secure ACS からダウンロードされたものと NX-OS デバイスに手動で設定されたものの両方）。

ダウンロードされた SGACL ポリシーのリフレッシュ

Cisco Secure ACS によって NX-OS デバイスにダウンロードされた SGACL ポリシーをリフレッシュできます。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switchto vdc** コマンドを使用します）。

Cisco TrustSec がイネーブルになっていることを確認します（「Cisco TrustSec 機能のイネーブル化」[p.9-13] を参照）。

手順の概要

1. **cts refresh role-based-policy**
2. **show cts role-based policy**

詳細な手順

	コマンド	目的

ステップ 1	`cts refresh policy`
	
	例：
	`switch# cts refresh policy`
		Cisco Secure ACS からの Cisco TrustSec SGACL をリフレッシュします。

ステップ 2	`show cts role-based policy`
	
	例：
	`switch# show cts role-based policy`
		（任意）Cisco TrustSec SGACL ポリシーを表示します。

SXP の設定

SGT Exchange Protocol（SXP）を使用すると、Cisco TrustSec のハードウェア サポートがないネットワーク デバイスに SGT を伝播 できます。ここでは、ネットワーク内の NX-OS デバイスに Cisco TrustSec SXP を設定する手順について説明します。

ここでは、次の内容について説明します。

Cisco TrustSec SXP の設定プロセス

Cisco TrustSec SXP の設定手順は次のとおりです。

ステップ 1　Cisco TrustSec 機能をイネーブルにします（「Cisco TrustSec 機能のイネーブル化」[p.9-13] を参照）。

ステップ 2　VRF に対する SGACL ポリシーの強制をイネーブルにします（「VRF に対する SGACL ポリシーの強制のイネーブル化」[p.9-29] を参照）。

ステップ 3　Cisco TrustSec SXP をイネーブルにします（「Cisco TrustSec SXP のイネーブル化」[p.9-37] を参照）。

ステップ 4　スピーカー ピアとリスナー ピア に接続を設定します（「Cisco TrustSec SXP のピア接続の設定」[p.9-38] を参照）。

（注）　SXP には管理（mgmt 0）接続は使用できません。

Cisco TrustSec SXP のイネーブル化

ピアの接続を設定する前に、Cisco TrustSec SXP をイネーブルにする必要があります。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switchto vdc** コマンドを使用します）。

Cisco TrustSec がイネーブルになっていることを確認します（「Cisco TrustSec 機能のイネーブル化」[p.9-13] を参照）。

手順の概要

1. **config t**
2. **cts sxp enable**

3. **exit**
4. **show cts sxp**
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	`config t`
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	`cts sxp enable`
	
	例：
	`switch(config)# cts sxp enable`
		Cisco TrustSec の SXP をイネーブルにします。

ステップ 3	`exit`
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	`show cts sxp`
	
	例：
	`switch# show cts sxp`
		（任意）SXP の設定を表示します。

ステップ 5	`copy running-config startup-config`
	
	例：
	`switch# copy running-config startup-config`
		（任意）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Cisco TrustSec SXP のピア接続の設定

SXP トランザクションのピア接続を設定する必要があります。パスワード保護を使用している場合は、必ず両エンドに同じパスワードを使用してください。

（注） デフォルトの SXP 送信元 IP アドレスが設定されていない場合に、接続の SXP 送信元アドレスを指定しないと、NX-OS ソフトウェアは既存のローカル IP アドレスから SXP 送信元 IP アドレスを抽出します。その NX-OS デバイスから開始される各 TCP 接続で SXP 送信元アドレスが異なる可能性があります。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switchto vdc** コマンドを使用します）。

Cisco TrustSec がイネーブルになっていることを確認します（「Cisco TrustSec 機能のイネーブル化」[p.9-13] を参照）。

SXP がイネーブルになっていることを確認します（「Cisco TrustSec SXP のイネーブル化」[p.9-37] を参照）。

VRF に対する SGACL ポリシーの強制がイネーブルになっていることを確認します（「VRF に対する SGACL ポリシーの強制のイネーブル化」[p.9-29] を参照）。

手順の概要

1. **config t**
2. **cts sxp connection peer** *peer-ipv4-addr* [**source** *src-ipv4-addr*] **password** {**default** | **none** | **required** *password*} **mode** {**speaker** | **listener**} [**vrf** *vrf-name*]
3. **exit**
4. **show cts sxp**
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**cts sxp connection peer** *peer-ipv4-addr* [**source** *src-ipv4-addr*] **password** {**default** | **none** | **required** *password*} **mode** {**speaker** | **listener**} [**vrf** *vrf-name*] **例：** `switch(config)# cts sxp connection peer 10.10.1.1 source 20.20.1.1 password default mode speaker`	SXP アドレス接続を設定します。**vrf** キーワードによってピアに VRF を提供します。 **（注）** SXP には管理（mgmt 0）インターフェイスを使用できません。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**show cts sxp** **例：** `switch# show cts sxp`	（任意）SXP の設定を表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

デフォルトの SXP パスワードの設定

デフォルトでは、SXP は接続のセットアップ時にパスワードを使用しません。NX-OS デバイスにデフォルトの SXP パスワードを設定できます。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switchto vdc** コマンドを使用します）。

Cisco TrustSec がイネーブルになっていることを確認します（「Cisco TrustSec 機能のイネーブル化」[p.9-13] を参照）。

SXP がイネーブルになっていることを確認します（「Cisco TrustSec SXP のイネーブル化」[p.9-37] を参照）。

手順の概要

1. **config t**
2. **cts sxp default password** *password*
3. **exit**
4. **show cts sxp**
5. **show running-config cts**
6. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**cts sxp default password** *password* **例：** `switch(config)# cts sxp default password A2Q3d4F5`	SXP のデフォルト パスワードを設定します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**show cts sxp** **例：** `switch# show cts sxp`	（任意）SXP の設定を表示します。
ステップ 5	**show running-config cts** **例：** `switch# show running-config cts`	（任意）実行コンフィギュレーションの SXP 設定を表示します。
ステップ 6	**copy running-config startup-config** **例：** `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

デフォルトの SXP 送信元 IP アドレスの設定

NX-OS ソフトウェアは、送信元 IP アドレスが指定されないと、新規の TCP 接続すべてにデフォルトの送信元 IP アドレスを使用します。デフォルト SXP 送信元 IP アドレスを設定しても、既存の TCP 接続には影響しません。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switchto vdc** コマンドを使用します）。

Cisco TrustSec がイネーブルになっていることを確認します（「Cisco TrustSec 機能のイネーブル化」[p.9-13] を参照）。

SXP がイネーブルになっていることを確認します（「Cisco TrustSec SXP のイネーブル化」[p.9-37] を参照）。

手順の概要

1. **config t**
2. **cts sxp default source-ip** *src-ip-addr*
3. **exit**
4. **show cts sxp**
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**cts sxp default source-ip** *src-ip-addr* **例：** `switch(config)# cts sxp default source-ip 10.10.3.3`	SXP のデフォルトの送信元 IP アドレスを設定します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**show cts sxp** **例：** `switch# show cts sxp`	（任意）SXP の設定を表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SXP 復帰期間

ピアが SXP 接続を終了すると、内部ホールドダウン タイマーが開始されます。内部ホールドダウン タイマーが終了する前にピアが再接続すると、SXP 復帰期間タイマーが開始されます。SXP 復帰期間タイマーがアクティブな間、NX-OS ソフトウェアは前回の接続で学習した SGT マッピング エントリを保持し、無効なエントリを削除します。デフォルト値は 120 秒（2 分）です。SXP 復帰期間を 0 秒に設定すると、タイマーがディセーブルになり、前回の接続のすべてのエントリが削除されます。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switchto vdc** コマンドを使用します）。

Cisco TrustSec がイネーブルになっていることを確認します（「Cisco TrustSec 機能のイネーブル化」[p.9-13] を参照）。

SXP がイネーブルになっていることを確認します（「Cisco TrustSec SXP のイネーブル化」[p.9-37] を参照）。

手順の概要

1. **config t**
2. **cts sxp reconcile-period** *seconds*
3. **exit**
4. **show cts sxp**
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**cts sxp reconcile-period** *seconds* **例：** `switch(config)# cts sxp reconcile-period 180`	SXP 復帰タイマーを変更します。デフォルト値は 120 秒（2 分）です。範囲は 0 ～ 64000 です。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**show cts sxp** **例：** `switch# show cts sxp`	（任意）SXP の設定を表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SXP リトライ期間の変更

SXP リトライ期間によって、NX-OS ソフトウェアが SXP 接続を再試行する頻度が決まります。SXP 接続が正常に確立されなかった場合、NX-OS ソフトウェアは SXP リトライ期間タイマーの終了後に、新たな接続の確立を試行します。デフォルト値は 60 秒（1 分）です。SXP リトライ期間を 0 秒に設定すると、タイマーがディセーブルになり、再試行は実行されません。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switchto vdc** コマンドを使用します）。

Cisco TrustSec がイネーブルになっていることを確認します（「Cisco TrustSec 機能のイネーブル化」[p.9-13] を参照）。

SXP がイネーブルになっていることを確認します（「Cisco TrustSec SXP のイネーブル化」[p.9-37] を参照）。

手順の概要

1. **config t**
2. **cts sxp retry-period** *seconds*

3. **exit**
4. **show cts sxp**
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例**： switch# config t switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**cts sxp retry-period** *seconds* **例**： switch(config)# cts sxp retry-period 120	SXP リトライ タイマーを変更します。デフォルト値は 60 秒（1 分）です。範囲は 0 ～ 64000 です。
ステップ 3	**exit** **例**： switch(config)# exit switch#	コンフィギュレーション モードを終了します。
ステップ 4	**show cts sxp** **例**： switch# show cts sxp	（任意）SXP の設定を表示します。
ステップ 5	**copy running-config startup-config** **例**： switch# copy running-config startup-config	（任意）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Cisco TrustSec 設定の確認

Cisco TrustSec の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show cts	Cisco TrustSec の情報を表示します。
show cts credentials	EAP-FAST の Cisco TrustSec 証明書を表示します。
show cts environment-data	Cisco TrustSec の環境データを表示します。
show cts interface	インターフェイスの Cisco TrustSec 設定を表示します。
show cts pacs	デバイス キー ストア内の Cisco TrustSec 許可情報と PAC を表示します。
show cts role-based access-list	Cisco TrustSec の SGACL 情報を表示します。
show cts role-based enable	Cisco TrustSec の SGACL 強制の状態を表示します。
show cts role-based policy	Cisco TrustSec の SGACL ポリシー情報を表示します。
show cts role-based sgt-map	Cisco TrustSec SGACL SGT マップの設定を表示します。
show cts sxp	Cisco TrustSec SXP の情報を表示します。
show running-config cts	実行コンフィギュレーションの Cisco TrustSec 情報を表示します。

このコマンドの出力フィールドについての詳細は、『*Cisco NX-OS Security Command Reference, Release 4.0*』を参照してください。

Cisco TrustSec の設定例

ここでは次の内容について説明します。

Cisco TrustSec のイネーブル化

Cisco TrustSec をイネーブルにする例を示します。

```
switch# config t
switch(config)# feature dot1x
switch(config)# feature cts
switch(config)# cts device-id device1 password Cisco321
```

シード NX-OS デバイスへの Cisco TrustSec AAA の設定

次の例では、シード デバイスに Cisco TrustSec の AAA を設定します。

```
switch# config t
switch(config)# radius-server host 10.10.1.1 key Cisco123 pac
switch(config)# aaa group server radius Rad1
switch(config-radius)# server 10.10.1.1
switch(config-radius)# use-vrf management
switch(config-radius)# exit
switch(config)# aaa authentication dot1x default group Rad1
switch(config)# aaa authorization cts default group Rad1
```

インターフェイスに対する Cisco TrustSec 認証のイネーブル化

次の例では、インターフェイスに対して、クリア テキスト パスワードを使用する Cisco TrustSec 認証をイネーブルにします。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

次の例では、インターフェイスに対して、クリア テキスト パスワードを使用する Cisco TrustSec 認証をイネーブルにします。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

手動での Cisco TrustSec 認証の設定

次の例では、インターフェイスに手動で Cisco TrustSec 認証を設定します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# cts manual
switch(config-if-cts-manual)# sap pmk abcdef modelist gmac
switch(config-if-cts-manual)# policy static sgt 0x20
switch(config-if-cts-manual)# exit
switch(config)# interface ethernet 2/2
switch(config-if)# cts manual
switch(config-if-cts-manual)# policy dynamic identity device2
switch(config-if-cts-manual)# exit
switch(config-if)#
```

VRF に対する Cisco TrustSec ロールベース ポリシー強制の設定

次の例では、デフォルト VRF に対して Cisco TrustSec のロールベース ポリシー強制をイネーブルにします。

```
switch# config t
switch(config)# cts role-based enforcement
switch(config)# show cts role-based enable
```

デフォルト以外の VRF に対する Cisco TrustSec ロールベース ポリシー強制の設定

次の例では、デフォルト以外の VRF に対して Cisco TrustSec のロールベース ポリシー強制をイネーブルにします。

```
switch# config t
switch(config)# vrf context test
switch(config-vrf)# cts role-based enforcement
switch(config-vrf)# exit
switch(config)# show cts role-based enable
```

VLAN に対する Cisco TrustSec ロールベース ポリシー強制の設定

次の例では、VLAN に対して Cisco TrustSec のロールベース ポリシー強制をイネーブルにします。

```
switch# config t
switch(config)# vlan 10
switch(config-vlan)# cts role-based enforcement
switch(config-vlan)# exit
switch(config)# show cts role-based enable
```

デフォルト VRF に対する IPv4 アドレスと SGACL SGT のマッピングの設定

次の例では、デフォルト VRF に対して Cisco TrustSec ロールベース ポリシーの IPv4 アドレス対 SGACL SGT マッピングを手動で設定します。

```
switch# config t
switch(config)# cts role-based sgt-map 10.1.1.1 20
```

デフォルト以外の VRF に対する IPv4 アドレスと SGACL SGT のマッピングの設定

次の例では、デフォルト以外の VRF に対して Cisco TrustSec ロールベース ポリシーの IPv4 アドレス対 SGACL SGT マッピングを手動で設定します。

```
switch# config t
switch(config)# vrf context test
switch(config-vrf)# cts role-based sgt-map 30.1.1.1 30
switch(config-vrf)# exit
switch(config)#
```

VLAN に対する IPv4 アドレスと SGACL SGT のマッピングの設定

次の例では、VLAN に対して Cisco TrustSec ロールベース ポリシーの IPv4 アドレス対 SGACL SGT マッピングを手動で設定します。

```
switch# config t
switch(config)# vlan 10
switch(config-vlan)# cts role-based sgt-map 20.1.1.1 20
switch(config-vlan)# exit
switch(config)#
```

Cisco TrustSec SGACL の手動設定

次の例では、Cisco TrustSec SGACL を手動で設定します。

```
switch# config t
switch(config)# cts role-based access-list abcd
switch(config-rbacl)# permit icmp
switch(config-rbacl)# exit
switch(config)# cts role-based sgt 10 dgt 20 access-list abcd
```

レイヤ 3 Cisco TrustSec の設定

レイヤ 3 Cisco TrustSec の設定例を示します。

```
switch# config t
switch(config)# cts l3 spi 1000 10.2.2.2/24
switch(config)# interface ethernet 2/3
switch(config-if)# cts l3 spi 1000
```

SXP の設定

次の例では、switch1 に、デフォルト VRF の SXP を設定します。

```
switch1# config t
switch1(config)# cts sxp enable
switch1(config)# cts role-based enforcement
switch1(config)# cts sxp connection peer 10.1.2.3 password none mode speaker
```

次の例では、switch2 に、デフォルト VRF の SXP を設定します。

```
switch2# config t
switch2(config)# cts sxp enable
switch2(config)# cts role-based enforcement
switch2(config)# cts sxp connection peer 10.2.3.4 password none mode listener
```

デフォルト設定

表 9-1 に Cisco TrustSec パラメータのデフォルトの設定値を示します。

表 9-1　Cisco TrustSec パラメータのデフォルト値

パラメータ	デフォルト
Cisco TrustSec	ディセーブル
SXP	ディセーブル
SXP デフォルト パスワード	なし
SXP 復帰期間	120 秒（2 分）
SXP リトライ期間	60 秒（1 分）
キャッシング	ディセーブル

その他の参考資料

Cisco TrustSec の実装に関する詳細情報については、次を参照してください。

- 関連資料（p.9-47）

関連資料

関連事項	タイトル
Cisco Secure ACS	Cisco Secure Access Control Server Engine Solution のマニュアル
コマンド リファレンス	『*Cisco NX-OS Security Command Reference, Release 4.0*』
802.1X	第 7 章「802.1X の設定」