Cisco TrustSec の設定

この章の内容は、次のとおりです。

Cisco TrustSec の概要

Cisco TrustSec のアーキテクチャ

Cisco TrustSec 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なネットワークを構築することができます。 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。

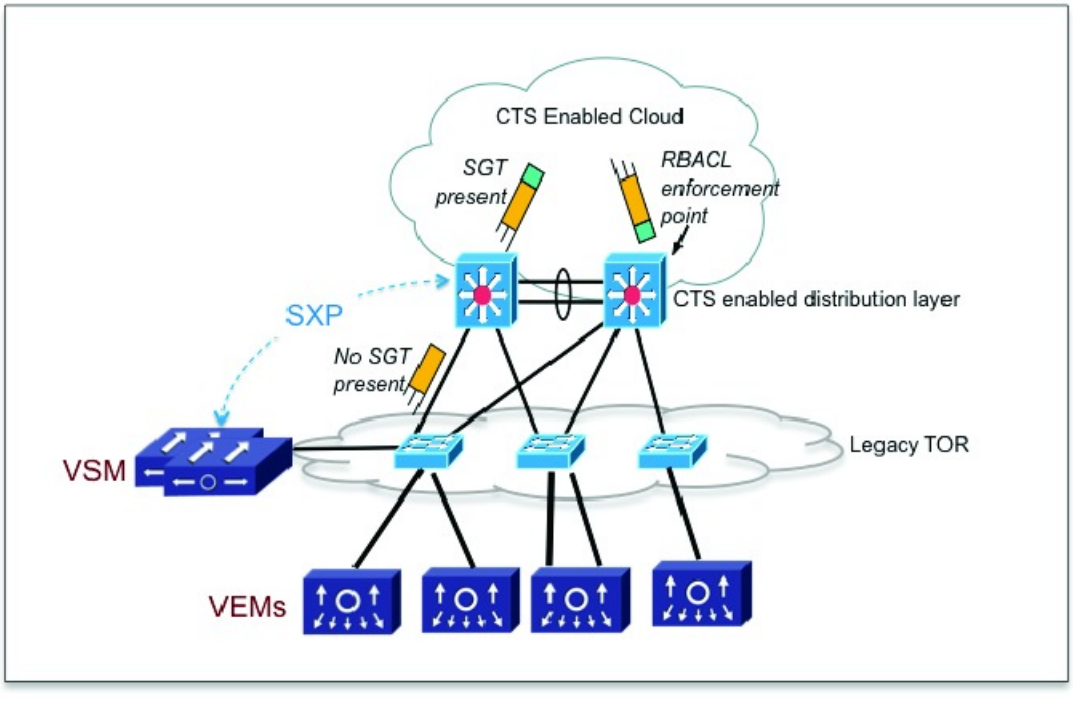
Cisco TrustSec は、認証時に取得したデバイスおよびユーザ識別情報を使用して、パケットがネットワークに入るときにそのパケットを分類またはタギングします。 これらのパケットは、データパスで識別し、セキュリティおよびその他のポリシー条件を適用できるように、Cisco TrustSec ネットワークへの入口でタグ付けされます。 このタグは、Security Group Tag（SGT; セキュリティ グループ タグ）と呼ばれることもあります。エンドポイント装置が SGT に応じてトラフィックを

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、パケットが宛先へのパス上で最初の Cisco TrustSec 対応デバイスに入るときのことです。出力とは、パス上で最後の Cisco TrustSec 対応デバイスから出るときのことです。

次の図に、Cisco TrustSec クラウドの例を示します。

図 *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、各デバイスのアイデンティティを検証します。
- **許可**：認証されたデバイスのアイデンティティに基づいて、Cisco TrustSec ネットワークのリソースへのアクセス権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。

SGACL と SGT

Security Group Access List（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。 Cisco 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け取ることができます。 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。

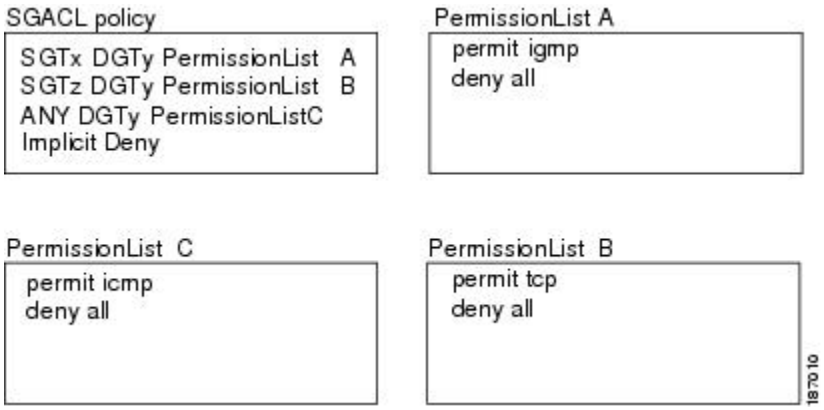
Cisco TrustSec はセキュリティ グループに、Security Group Tag（SGT; セキュリティ グループ タグ）という 16 ビットの固有のタグを割り当てます。 Cisco NX-OS デバイス内の SGT の数は認証済みのネットワーク エンティティの数に制限されます。 SGT は全社内の送信元の許可を示す単一ラベルです。 範囲は Cisco TrustSec ネットワーク内でグローバルです。

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。

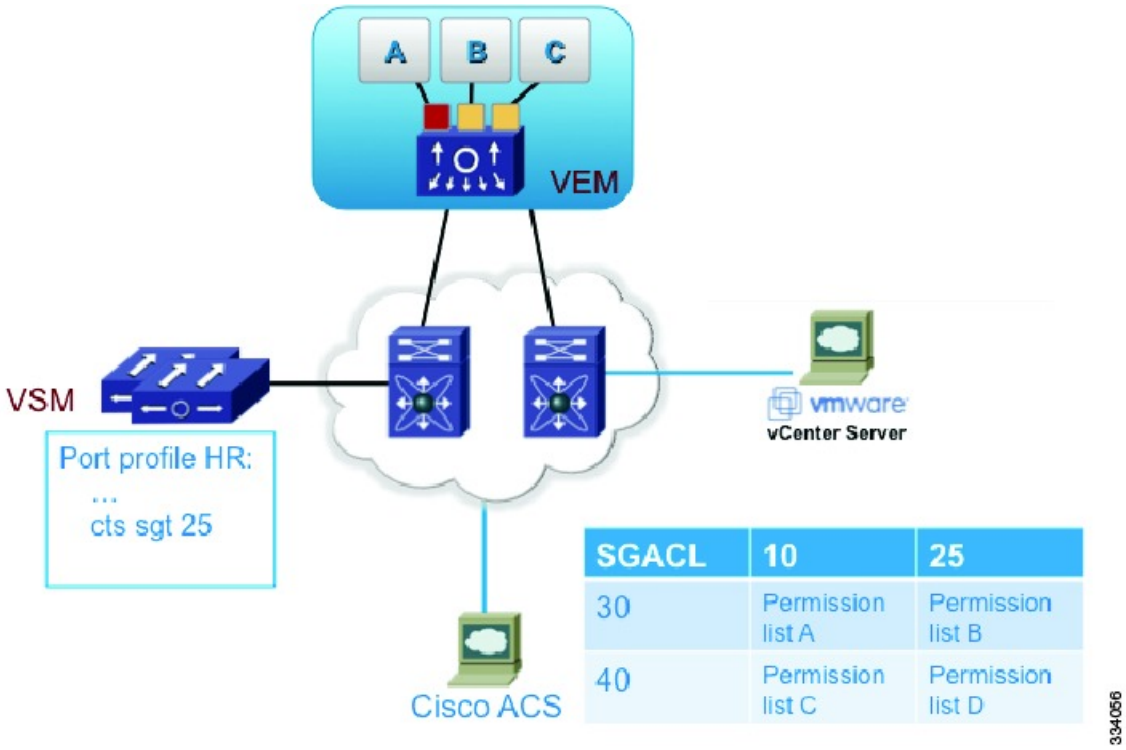
Cisco TrustSec はセキュリティ グループ間のアクセス コントロール ポリシーを定義します。 Cisco TrustSec は、ネットワーク内のデバイスをセキュリティ グループに割り当て、セキュリティ グループ間およびセキュリティ グループ内でアクセス コントロールを適用することにより、ネットワーク内でアクセス コントロールを行います。 次の図に、SGACL ポリシーの例を示します。

図 *2*： *SGACL* ポリシーの例



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

図 3 : *Cisco TrustSec* ネットワークでの *SGT* と *SGACL*



Cisco 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。 Cisco TrustSec 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、設定されているアクセス コントロール エントリ（ACE）の数は次のようにして決まります。

ACE 数 =（指定された発信元の数）X（指定された宛先の数）X（指定された許可の数）

Cisco TrustSec では、次の式を使用します。

ACE 数 = 指定された許可の数

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、SGACL を適用できるように、パケットの SGT を判断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 を判断できます。

- 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、そのパケットにとってネットワーク 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、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。
- 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 を判断するようにポリシーを手動で設定できます。 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。

Cisco Nexus 1000V 上での SGT の伝播のための SXP

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 プロトコルは、アップストリーム Cisco TrustSec 対応スイッチまで、仮想マシンと対応する SGT の IP アドレスを伝播するために使用されます。 出力側では、Cisco TrustSec 対応ディストリビューション スイッチの出力インターフェイスで、ロール ベース アクセス コントロール（RBACL）が適用されます。

SXP で SGT を伝播するには、次の手順を実行します。

- **SXP 接続の設定**：SXP スピーカーまたは SXP リスナーとして SXP 接続の各ピアを設定する必要があります。 スピーカー デバイスはリスナー デバイスに SXP 情報（IP-SGT マッピング）を配布します。 Cisco Nexus 1000V の Cisco TrustSec では、Cisco Nexus 1000V はすべてのピア接続で SXP スピーカーとして設定されます。
- **IP-SGT マッピングの追跡と取得**：仮想マシンに手動で SGT を割り当てる必要があります。 SGT の設定は、ポート プロファイルまたは仮想イーサネット インターフェイスに割り当てられます。 仮想マシンを起動すると、ポートプロファイルに割り当てられた SGT の設定が、仮想マシンに関連付けられます。

  ポートに割り当てられた IP アドレスを Cisco Nexus 1000V で追跡できるように、IP デバイス トラッキングと DHCP スヌーピングを設定する必要があります。 IP デバイス トラッキングと DHCP スヌーピングの両方を設定した場合、両方の送信元から学習した情報が使用され、すべてのインターフェイスの IP アドレスが取得されます。
- **SXP による IP-SGT マッピングの伝達**：SXP プラットフォームで、IP-SGT マッピングは SXP のローカル データベースに保存され、SXP によって SXP リスナーに配信されます。 新しい IP-SGT マッピングが作成されると、Cisco Nexus 1000V はローカル データベースで新しい IP-SGT マッピングを確認するか、コピーします。 その後、変更が SXP によってアップストリーム SXP リスナーに伝達されます。

SXP 接続を手動で設定するには、次の作業を行う必要があります。

- SXP データの整合性と認証が必要になる場合は、ピア デバイスの両方に同じ SXP パスワードを設定する必要があります。 SXP パスワードは各ピア接続に対して明示的に指定することも、デバイスに対してグローバルに設定することもできます。 SXP パスワードは必須ではありません。
- 各ピアを SXP 接続に SXP スピーカーまたは SXP リスナーとして設定する必要があります。スピーカー デバイスはリスナー デバイスに SXP 情報を渡します。
- 送信元 IP アドレスを指定して各ピアの関係付けに使用したり、特定の送信元 IP アドレスを設定していないピア接続に対してデフォルトの送信元 IP アドレスを設定したりすることができます。

Cisco TrustSec のライセンス要件

次の表に、この機能のライセンス要件を示します。

機能	ライセンス要件
Cisco TrustSec	この機能には、Advanced ライセンスが必要です。 Cisco Nexus 1000V のライセンス要件の詳細については、『*Cisco Nexus 1000V License Configuration Guide*』を参照してください。

Cisco TrustSec の前提条件

Cisco TrustSec の前提条件は次のとおりです。

- Cisco TrustSec 機能をイネーブルにする必要があります。
- Cisco TrustSec SXP をイネーブルにする必要があります。
- Advanced Services ライセンスをインストールする必要があります。

Cisco TrustSec の注意事項と制約事項

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 IPv4 アドレスだけをサポートします。
- Cisco Nexus 1000V の VSM は、常にすべてのピア接続で SXP スピーカーとして設定されます。

- 仮想マシンに SGT を割り当てるには、ポート プロファイルまたは vEthernet インターフェイスで SGT の相互作用を手動で設定する必要があります。 これは、管理インターフェイスまたはイーサネット インターフェイスではサポートされません。
- DVS のシステム全体で最大 2048 の IP-SGT マッピングを学習できます。 これは、DHCP スヌーピングと、ARP および IP トラフィック インスペクションによる個々の仮想マシンのデバイス トラッキングで学習したエントリの両方を合計した数です。
- IP-SGT マッピングは最大 64 の SXP ピア デバイスに伝達できます。

デフォルト設定

表 *1*：*Cisco TrustSec* のデフォルト設定

パラメータ	デフォルト
Cisco TrustSec	Disabled
SXP	Disabled
SXP デフォルト パスワード	なし
SXP 復帰期間	120 秒
SXP リトライ期間	60 秒
デバイス トラッキング	Enabled
インターフェイスの削除ホールド タイマー	60 秒

Cisco TrustSec の設定

Cisco TrustSec 機能のイネーブル化

Cisco TrustSec を設定する前に、Cisco Nexus 1000V で Cisco TrustSec 機能をイネーブルにする必要があります。

はじめる前に

- EXEC モードで CLI にログインしていること。
- Advanced Services ライセンスがインストールされていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **[no] feature cts**	Cisco TrustSec 機能をイネーブルに（no 形式を使用した場合はディセーブルに）します。
ステップ 3	switch(config)# **show cts**	（任意） Cisco TrustSec の設定を表示します。
ステップ 4	switch(config)# **show feature**	（任意） 機能がイネーブルになったステータスを表示します。
ステップ 5	**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。

次に、Cisco TrustSec 機能をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature cts
switch(config)# show cts
CTS Global Configuration
==============================
CTS support : enabled
CTS device identity : not configured
SGT : 0
CTS caching support : disabled

Number of CTS interfaces in
DOT1X mode : 0
Manual mode : 0
switch(config)#

switch(config)# show feature
Feature Name Instance State
-------------------- -------- --------
cts 1 enabled
dhcp-snooping 1 enabled
http-server 1 enabled
lacp 1 disabled
netflow 1 disabled
network-segmentation 1 disabled
port-profile-roles 1 disabled
private-vlan 1 disabled
segmentation 1 disabled
sshServer 1 enabled
tacacs 1 disabled
telnetServer 1 enabled
vtracker 1 disabled
switch(config)#
```

Cisco TrustSec SXP のイネーブル化

Cisco Nexus 1000V で、Cisco TrustSec SXP をイネーブルにできます。

はじめる前に

- EXEC モードで CLI にログインしていること。
- Cisco TrustSec 機能をイネーブルにする必要があります。
- Advanced Services ライセンスをインストールする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# [**no**] **cts sxp enable**	Cisco TrustSec SXP 機能をイネーブルに（no 形式を使用した場合はディセーブルに）します。 デフォルトではディセーブルになっています。
ステップ 3	switch(config)# **show cts sxp**	（任意） Cisco TrustSec SXP の設定を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に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て、変更を継続的に保存します。

次に、Cisco TrustSec SXP をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# cts sxp enable
switch(config)# show cts sxp
CTS SXP Configuration:
SXP enabled
SXP default password configured
SXP retry timeout:60
SXP reconcile timeout:120
Minimum SXP Version: 1
Maximum SXP Version:1
switch(config)#
```

Cisco TrustSec デバイス トラッキングの設定

デバイストラッキングを設定して、仮想イーサネットポート上でアドレス解決プロトコル（ARP）および IP トラフィックを調べることで、仮想マシンの IP アドレスの学習をイネーブルにできます。

はじめる前に

- EXEC モードで CLI にログインしていること。
- Cisco TrustSec SXP をイネーブルにする必要があります。
- Cisco TrustSec 機能をイネーブルにする必要があります。
- Advanced Services ライセンスをインストールする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **cts device tracking**	Cisco TrustSec のデバイス トラッキングをイネーブルにします。 （注） Cisco Nexus 1000V は、VEM での ARP/IP トラフィック インスペクションおよび DHCP スヌーピングからの IP アドレスの追跡をサポートします。 Cisco TrustSec デバイス トラッキングは、VEM での ARP/IP トラフィック インスペクションを使用して IP アドレスを追跡します。 Cisco TrustSec デバイス トラッキングで DHCP スヌーピングからの IP アドレスの追跡をイネーブルにするには、DHCP スヌーピング機能もイネーブルにする必要があります。 デフォルトでは、デバイス トラッキングはイネーブルです。
ステップ 3	switch(config)# **show cts device tracking**	（任意） Cisco TrustSec デバイス トラッキングの設定を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に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て、変更を継続的に保存します。

次に、Cisco TrustSec デバイス トラッキングを設定する例を示します。

```
switch# configure terminal
switch(config)# cts device tracking
enabled
switch(config)#
```

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。 Cisco 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。

はじめる前に

- EXEC モードで CLI にログインしていること。
- Cisco TrustSec SXP をイネーブルにする必要があります。
- Cisco TrustSec 機能をイネーブルにする必要があります。
- Advanced Services ライセンスをインストールする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **cts sxp default password** [**word** | **7**] *password*	次のオプションを使用して SXP のデフォルト パスワードを設定します。 • **word**：デフォルト パスワードを暗号化しないことを指定します。 • **7**：デフォルト パスワードを暗号化することを指定します。 デフォルトでは、SXP パスワードは使用されません。
ステップ 3	switch(config)# **show cts sxp**	（任意） SXP の設定を表示します。
ステップ 4	switch(config)# **show running-config cts**	（任意） Cisco TrustSec の実行コンフィギュレーションを表示します。

	コマンドまたはアクション	目的
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に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て、変更を継続的に保存します。

次に、デフォルト SXP パスワードを設定する例を示します。

```
switch# configure terminal
switch(config)# cts sxp default password 7 CiscoPassword
switch(config)# cts cts sxp
CTS SXP Configuration:
SXP enabled
SXP default password configured
SXP retry timeout:60
SXP reconcile timeout:120
Minimum SXP Version: 1
Maximum SXP Version:1
```

デフォルトの SXP 送信元 IPv4 アドレスの設定

Cisco NX-OS ソフトウェアは、送信元 IPv4 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 IPv4 アドレスを使用します。 デフォルト SXP 送信元 IPv4 アドレスを設定しても、既存の TCP 接続には影響しません。

はじめる前に

- EXEC モードで CLI にログインしていること。
- Cisco TrustSec SXP をイネーブルにする必要があります。
- Cisco TrustSec 機能をイネーブルにする必要があります。
- Advanced Services ライセンスをインストールする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	**cts sxp default password** *password*	SXP のデフォルト パスワードを設定します。
ステップ 3	switch(config)# **cts sxp default source-ip** *src-ip-addr*	SXP のデフォルトの送信元 IPv4 アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 4	switch(config)# **show cts sxp**	（任意） SXP の設定を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に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て、変更を継続的に保存します。

次に、デフォルトの SXP 送信元 IPv4 アドレスを設定する例を示します。

```
switch# configure terminal
switch# cts sxp default password xyzexy
switch(config)# cts sxp default source-ip  10.78.1.73
switch(config)# show cts sxp
CTS SXP Configuration:
SXP enabled
SXP default password configured
Default Source IP Address:10.78.1.73
SXP retry timeout:60
SXP reconcile timeout:120
Minimum SXP Version: 1
Maximum SXP Version:1
switch(config)#
```

ポート プロファイルでの Cisco TrustSec SGT の設定

ポート プロファイル設定の一部として、または vEthernet インターフェイスに固有の Cisco TrustSec Security Group Tag（SGT）を設定できます。 その後、SGT はポート プロファイルを継承するすべての仮想マシンに関連付けられます。

はじめる前に

- EXEC モードで CLI にログインしていること。
- Cisco TrustSec SXP をイネーブルにする必要があります。
- Cisco TrustSec 機能をイネーブルにする必要があります。
- Advanced Services ライセンスをインストールする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **port-profile** *name*	名前付きポート プロファイルのポート プロファイル コンフィギュレーション モードを開始します。 ポート プロファイルが存在しない場合は、作成されます。
ステップ 3	switch(config-port-prof)# **cts sgt** *tag*	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* 形式の 16 進数値で表したデバイスのローカル SGT です。 範囲は、1 ～ 65519 です。
ステップ 4	switch(config-port-prof)# **show cts sxp sgt-map**	（任意） IP アドレスから Cisco TrustSec の SGT へのマッピングを表示します。
ステップ 5	switch(config-port-prof)# **show running-configuration port-profile** *name*	（任意） ポート プロファイル設定を表示します。
ステップ 6	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に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て、変更を継続的に保存します。

次に、ポート プロファイル設定の一部として Cisco TrustSec SGT を設定する例を示します。

```
switch# configure terminal
switch(config)# port-profile kumar
switch(config-port-prof)# cts stg 6766
switch(config-port-prof)# show cts sxp sgt-map
switch(config-port-prof)# show running-config port-profile kumar
!Command: show running-config port-profile kumar
!Time: Wed Sep 26 22:58:16 2012
version 4.2(1)SV2(1.1)
port-profile type vethernet kumar
vmware port-group
switchport mode access
switchport access vlan 353
cts sgt 6766
no shutdown
system vlan 353
state enabled
switch(config-port-prof)#
```

次に、vEthernet インターフェイスに Cisco TrustSec SGT を設定する例を示します。

```
switch# configure terminal
switch(config)# port-profile kumar
switch(config-port-prof)# capability l3control
switch(config-port-prof)# vmware port-group
switch(config-port-prof)# switchport mode access
switch(config-port-prof)# switchport access vlan 353
switch(config-port-prof)# cts sgt 6766
switch(config-port-prof)# no shutdown
```

```
switch(config-port-prof)# system vlan 353
switch(config-port-prof)# state enabled
switch(config-port-prof)# show running-config interface vethernet 1
!Command: show running-config interface Vethernet1
!Time: Wed Sep 26 22:59:39 2012
version 4.2(1)SV2(1.1)
interface Vethernet1
inherit port-profile kumar
description VMware VMkernel, vmk1
vmware dvport 65 dvswitch uuid "c1 0c 33 50 36 73 e3 9b-26 5f db 02 b3 79 cc b8"
vmware vm mac 0050.5665.7F77
cts sgt 888
switch(config)#
```

Cisco TrustSec SXP のピア接続の設定

スピーカーおよびリスナーの両方のデバイスで SXP 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、両方のデバイスで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、Cisco 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。 SXP 送信元アドレスは Cisco NX-OS デバイスから開始される各 TCP 接続によって異なる可能性があります。

（注） Cisco Nexus 1000V では SXP スピーカー モードだけがサポートされます。 したがって、リスナーで SXP ピアを設定する必要があります。

はじめる前に

- EXEC モードで CLI にログインしていること。
- Cisco TrustSec SXP をイネーブルにする必要があります。
- Cisco TrustSec 機能をイネーブルにする必要があります。
- Advanced Services ライセンスをインストールする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# [**no**] **cts sxp connection peer** *peer-ip-address* **source** *source-ip-address*] **password** {[**default**] | [**none** [**required**]	SXP アドレス接続を設定します。 • **source**：送信元の IPv4 アドレスを指定します。 デフォルトの送信元は、**cts sxp default source-ip** コマンドを使用して設定した IPv4 アドレスです。

	コマンドまたはアクション	目的
	password} [**mode** {**listener**} [**vrf** { **default** | **management**}]	• **password**：次のオプションを使用して、SXP が接続に使用するパスワードを指定します。 ◦ **default**：**cts sxp default password** コマンドを使用して設定したデフォルトの SXP パスワードを使用します。 ◦ **none**：パスワードを使用しません。 ◦ **required**：このコマンドで指定したパスワードを使用します。 • **mode**：リモート ピア デバイスのロールを指定します。 Cisco Nexus 1000V は接続のスピーカーとしてのみ動作するため、リスナーとしてピアを設定する必要があります。 • **vrf** キーワードでは、ピアに対する VRF を指定します。 デフォルトは、デフォルトの仮想ルーティングおよび転送（VRF）インスタンスです。
ステップ 3	switch(config)# **show cts sxp connection**	（任意） SXP 接続とステータスを表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に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て、変更を継続的に保存します。

次に、Cisco TrustSec ピア接続を設定する例を示します。

```
switch# configure terminal
switch(config)#  cts sxp connection peer 1.2.3.4 password none mode listener vrf management
switch(config)# show cts sxp connection
```

スタティック IP-SGT バインディングの設定

IP ホスト アドレスとセキュリティ グループ タグ（SGT）のスタティック バインディングを定義できます。 スタティック IP-SGT バインディングは VRF のコンテキストで設定され、デフォルト VRF に適用されます。 スタティック IP-SGT バインディングは、SXP やローカルで認証済みのホストなどのソースから得られたダイナミック バインディングよりも優先されます。 特定のホスト IP アドレスについて唯一の既知のバインディングがスタティック IP-SGT バインディングの場合、このバインディングが SXP ピアにエクスポートされます。 スタティック IP-SGT バインディングは VRF のコンテキストで設定されるため、SXP ピアにエクスポートできるように、同じ VRF でスタティック IP-SGT バインディングを設定する必要があります。

はじめる前に

- EXEC モードで CLI にログインしていること。
- Cisco TrustSec SXP をイネーブルにする必要があります。
- Cisco TrustSec 機能をイネーブルにする必要があります。
- Advanced Services ライセンスをインストールする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **cts role-based sgt-map** *ip-address* **sgt** *sgt*	IP ホスト アドレスとセキュリティ グループ タグ（SGT）のスタティック バインディングを設定します。 • *ip-address*：ホストの IP アドレスを指定します。 • *sgt*：IP アドレスに対応する SGT を指定します。 指定できる範囲は 1 ～ 65519 です。
ステップ 3	switch(config)# **vrf context**	（任意） VRF のコンテキストで IP-SGT バインディングを指定します。デフォルトはデフォルト VRF です。
ステップ 4	switch(config)# **show cts role-based sgt-map**	（任意） IP アドレスから Cisco TrustSec の SGT へのマッピングを表示します。
ステップ 5	switch(config)# **show cts ipsgt entries**	（任意） SXP SGT エントリを表示します。
ステップ 6	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に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て、変更を継続的に保存します。

次に、スタティック IP-SGT バインディングを設定する例を示します。

```
switch# configure terminal
switch(config)# cts role-based sgt-map 1.1.1.1 100
switch(config)# vrf context management
switch(config-vrf)# cts role-based sgt-map 2.2.2.3 200
switch(config-vrf)# exit
```

```
switch(config)# show cts role-based sgt-map
IP ADDRESS SGT VRF/VLAN SGT CONFIGURATION
1.1.1.1 100 vrf:1 CLI Configured
2.2.2.3 200 vrf:2 CLI Configured
cinquedia(config)# show cts ipsgt entries
Interface SGT IP ADDRESS VRF Learnt
-------------- ------ ---------------- ---------- ---------
- 100 1.1.1.1 default Cli Configured
- 200 2.2.2.3 management Cli Configured

switch(config)# show cts ipsgt entries vrf management
Interface SGT IP ADDRESS Pushed Learnt
-------------- ------ ---------------- ---------- ---------
Vethernet1 888 10.10.101.10 Yes DHCP
10.78.1.78 Yes Device Tracking
Vethernet2 6766 10.78.1.76 Yes Device Tracking
- 545 99.10.10.10 Yes Cli Configured
```

SXP リトライ期間の変更

SXP リトライ期間によって、Cisco 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、Cisco 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 再試行期間を 0 秒に設定するとタイマーは無効になり、接続は再試行されません。

はじめる前に

- EXEC モードで CLI にログインしていること。
- Cisco TrustSec SXP をイネーブルにする必要があります。
- Cisco TrustSec 機能をイネーブルにする必要があります。
- Advanced Services ライセンスをインストールする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **cts sxp retry-period** *seconds*	SXP リトライ タイマー期間を指定します。 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	switch(config)# **show cts sxp**	（任意） SXP の設定を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に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

	コマンドまたはアクション	目的
		ションにコピーして、変更を継続的に保存します。

次に、SXP リトライ期間を設定する例を示します。

```
switch# configure terminal
switch(config)# cts sxp retry-period 60
switch(config)# show cts sxp
CTS SXP Configuration:
SXP enabled
SXP retry timeout:60
SXP reconcile timeout:120
Minimum SXP Version: 1
Maximum SXP Version:1
switch(config)#
```

インターフェイスの削除ホールド タイマーの変更

インターフェイスの削除ホールド タイマーの時間は、インターフェイスが関与していない状態になってから、そのインターフェイスが IP-SGT マッピングを保持する時間を決定します。 タイマーの期限が切れると、IP-SGT マッピングはインターフェイスとピアから削除されます。

はじめる前に

- EXEC モードで CLI にログインしていること。
- Cisco TrustSec SXP をイネーブルにする必要があります。
- Cisco TrustSec 機能をイネーブルにする必要があります。
- Advanced Services ライセンスをインストールする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# [**no**] **cts interface delete-hold** *seconds*	インターフェイスの削除ホールドタイマーの期間を指定します。 デフォルト値は 60 秒（1 分）です。 範囲は 0 ～ 64000 です。 タイマーが 0 に設定されている場合、IP-SGT マッピングはただちに削除されます。 このコマンドの **no** 形式を使用すると、インターフェイスが関与していない状態になってもタイマーが開始

	コマンドまたはアクション	目的
		されず、IP-SGTエントリが常にインターフェイス上で保持されるようになります。
ステップ 3	switch(config)# **show cts interface delete-hold timer**	（任意） インターフェイスの削除ホールドタイマーの時間を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に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て、変更を継続的に保存します。

次に、インターフェイスの削除ホールド タイマーを設定する例を示します。

```
switch# configure terminal
switch(config)# cts interface delete-hold 60
switch(config)# show cts interface delete-hold timer
60
switch(config)#
```

Cisco TrustSec の設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	目的
show cts	Cisco Nexus 1000V での Cisco TrustSec のグローバル設定を表示します。
show cts sxp	Cisco TrustSec SXP の設定を表示します。
show cts device tracking	Cisco TrustSec デバイス トラッキングの設定を表示します。
show cts sxp connection	Cisco TrustSec SXP の接続を表示します。
show cts role-based sgt-map	IP アドレスから Cisco TrustSec の SGT へのマッピングを表示します。
show cts ipsgt entries	SXP SGT エントリを表示します。
show cts interface delete-hold timer	Cisco TrustSec インターフェイスの削除ホールドタイマー期間を表示します。

コマンド	目的
show running-configuration cts	Cisco TrustSec の実行コンフィギュレーション情報を表示します。

Cisco TrustSec の機能の履歴

機能名	機能名	リリース
Cisco TrustSec	4.2(1)SV2(1.1)	この機能が導入されました。