Cisco TrustSec SXP の設定

Cisco TrustSec SXP について

Cisco TrustSec を使用すると、組織はアイデンティティベースのアクセス コントロールを通じて、人、場所、時を問わずネットワークとサービスをセキュリティで保護できます。 このソリューションでは、データの整合性および機密保持サービス、ポリシーベースの管理、中央集中型のモニタリング、トラブルシューティング、およびレポーティング サービスも提供されます。 TrustSec をカスタマイズされたプロフェッショナル サービスと組み合わせると、ソリューションの導入と管理を簡素化できます。CTS は、Cisco ボーダレス ネットワークの基盤となるセキュリティ コンポーネントです。

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 デバイスのドメイン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。 ドメイン内の各デバイスは、そのピアによって認証されます。 ドメイン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、ネットワークに入るようにセキュリティ グループ（SG）がパケットを分類するために認証中に取得したデバイスおよびユーザ クレデンシャルを使用します。 このパケット分類は、Cisco TrustSec ネットワークへの進入時にパケットにタグを付けることで維持されます。 これにより、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、エンドポイントデバイスはこの SGT に基づいてトラフィックをフィルタリングできるので、ネットワークへのアクセス コントロール ポリシーの適用が可能になります。

Cisco TrustSec アーキテクチャのコンポーネントの 1 つが、セキュリティ グループベースのアクセス コントロールです。 セキュリティ グループ ベースのアクセス コントロール コンポーネント

で、Cisco TrustSec ドメインのアクセス ポリシーは、トポロジとは無関係で、ネットワーク アドレスではなく送信元デバイスおよび宛先デバイスのロール（セキュリティ グループ番号で指定）に基づいています。個々のパケットには、送信元のセキュリティ グループ番号のタグが付けられます。

シスコ デバイスは SGT 交換プロトコル（SXP）を使用して、Cisco TrustSec 向けのハードウェア サポートがないネットワーク デバイスに SGT を伝播します。 SXP は、すべてのスイッチで CTS ハードウェアがアップグレードされるのを防ぐためのソフトウェア ソリューションです。 WLC では、TrustSec アーキテクチャの一部として SXP がサポートされます。 SXP は、CTS 対応のスイッチに SGT 情報を送信します。SGT で示されたロール情報に従って、適切なロールベース アクセス コントロール リスト（RBACL）をアクティブにすることができます。 デフォルトでは、コントローラは常にスピーカー モードで動作します。 ネットワーク上で SXP を実装するには、出口のディストリビューション スイッチのみを CTS 対応にすればよく、他のすべてのスイッチは CTS 非対応でかまいません。

SXP は、任意のアクセス レイヤとディストリビューション スイッチ間、または 2 つのディストリビューション スイッチ間で動作します。 SXP は TCP をトランスポート層として使用します。 アクセス レイヤ スイッチ上でネットワークに join している任意のホスト（クライアント）に対する CTS-enabled 認証は、CTS 対応ハードウェアを備えたアクセス スイッチの場合と同様に実行されます。 アクセス レイヤ スイッチは CTS 対応ハードウェアではありません。 したがって、データ トラフィックがアクセス レイヤ スイッチを通過するとき、そのトラフィックの暗号化または暗号による認証は行われません。 SXP は、認証されたデバイス（つまりワイヤレス クライアント）の IP アドレスと、対応する SGT をディストリビューション スイッチに渡すために使用されます。ディストリビューション スイッチが CTS 対応ハードウェアの場合は、そのディストリビューション スイッチがアクセス レイヤ スイッチに代わってパケットに SGT を挿入します。 ディストリビューション スイッチが CTS 対応ハードウェアでない場合は、ディストリビューション スイッチの SXP が、CTS ハードウェアを備えたすべてのディストリビューション スイッチに IP-SGT マッピングを渡します。 出口側では、ディストリビューション スイッチの出力 L3 インターフェイスで RBACL が適用されます。

次に、Cisco TrustSec SXP に関する注意事項を示します。

- SXP は次のセキュリティ ポリシーでのみサポートされます。
  - WPA2-dot1x
  - WPA-dot1x
  - 802.1x（Dynamic WEP）
  - RADIUS サーバを使用した MAC フィルタリング
  - RADIUS サーバを使用した Web 認証によるユーザ認証
- SXP は IPv4 クライアントと IPv6 クライアントの両方でサポートされます。
- コントローラは常にスピーカー モードで動作します。

Cisco TrustSec の詳細については、http://www.cisco.com/en/US/netsol/ns1051/index.html を参照してください。

Cisco TrustSec SXP の制約事項

- SXP は FlexConnect アクセス ポイントではサポートされません。
- SXP がサポートされるのは、中央認証を使用し、中央でスイッチされるネットワークだけです。
- デフォルトでは、SXP はローカル モードのみで動作する AP 向けにサポートされています。
- デフォルトパスワードの設定は、コントローラとスイッチの両方で一致している必要があります。
- 耐障害性は AP でのローカル スイッチングが必要になるため、この機能はサポートされません。
- ユーザをローカル認証するための静的 IP-SGT マッピングはサポートされません。
- IP-SGT マッピングでは、外部 ACS サーバを使用した認証が必要です。
- 自動アンカー モビリティ モードのコントローラはモビリティ メッセージを介してクライアント IP-SGT 情報を更新しません。 両方のコントローラの接続スイッチ間には、IP-SGT マッピングを更新するために、SXP 接続が確立されている必要があります。

Cisco TrustSec SXP の設定（GUI）

ステップ 1 [Security] > [TrustSec SXP] の順に選択して、[SXP Configuration] ページを開きます。 このページでは、次の SXP 設定の詳細が表示されます。

- [Total SXP Connections]：設定されている SXP 接続の数。
- [SXP State]：SXP 接続のステータス（有効または無効）。
- [SXP Mode]：コントローラの SXP モード。 SXP 接続では、コントローラは常にスピーカー モードに設定されています。
- [Default Password]：SXP メッセージの MD5 認証用パスワード。 パスワードには 6 文字以上を含めることをお勧めします。
- [Default Source IP]：管理インターフェイスの IP アドレス。 SXP は、すべての新規 TCP 接続に対してデフォルトの送信元 IP アドレスを使用します。
- [Retry Period]：SXP 再試行タイマー。 デフォルト値は 120 秒（2 分）です。 有効な範囲は 0 ～ 64000 秒です。 SXP 再試行期間によって、コントローラが SXP 接続を再試行する間隔が決まります。 SXP 接続が正常に確立されなかった場合、コントローラは SXP 再試行期間タイマーの終了後に、新しい接続の確立を試行します。 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。

このページでは、SXP 接続について次の情報も表示されます。

- [Peer IP Address]：ピアの IP アドレス、つまりコントローラが接続するネクスト ホップ スイッチの IP アドレス。 新しいピア接続を設定しても、既存の TCP 接続に影響はありません。
- [Source IP Address]：送信元の IP アドレス、つまりコントローラの管理 IP アドレス。
- [Connection Status]：SXP 接続のステータス。

ステップ 2 [SXP State]ドロップダウン リストで、[Enabled] を選択して Cisco TrustSec SXP を有効にします。

ステップ 3 SXP 接続に使用するデフォルト パスワードを入力します。 パスワードには 6 文字以上を含めることをお勧めします。

ステップ 4 [Retry Period] ボックスに、Cisco TrustSec ソフトウェアが SXP 接続を再試行する間隔を秒単位で入力します。

ステップ 5 [Apply] をクリックします。

新規 SXP 接続の作成（GUI）

ステップ 1 [SECURITY] > [TrustSec SXP] の順に選択し、[New] をクリックして [SXP Connection > New] ページを開きます。

ステップ 2 [Peer IP Address] テキスト ボックスに、コントローラが接続するネクスト ホップ スイッチの IP アドレスを入力します。

ステップ 3 [Apply] をクリックします。

Cisco TrustSec SXP の設定（CLI）

- 次のコマンドを入力して、コントローラ上で SXP を有効または無効にします。
  config cts sxp {**enable** | **disable**}
- 次のコマンドを入力して、SXP メッセージの MD5 認証のデフォルト パスワードを設定します。
  config cts sxp default password *password*
- 次のコマンドを入力して、コントローラが接続するネクスト ホップ スイッチの IP アドレスを設定します。
  config cts sxp connection peer *ip-address*
- 次のコマンドを入力して、接続を試みる間隔を設定します。

config cts sxp retry period *time-in-seconds*

- 次のコマンドを入力して、SXP 接続を削除します。

  config cts sxp connection delete *ip-address*

- 次のコマンドを入力して、SXP の設定の概要を確認します。

  show cts sxp summary

  以下に類似した情報が表示されます。

```
SXP State..................................... Enable
SXP Mode...................................... Speaker
Default Password.............................. ****
Default Source IP............................. 209.165.200.224
Connection retry open period ................. 120
```

- 次のコマンドを入力して、設定された SXP 接続のリストを参照します。
  show cts sxp connections

  以下に類似した情報が表示されます。

```
Total num of SXP Connections..................... 1
SXP State..................................... Enable
Peer IP            Source IP           Connection Status
---------------    ---------------     -----------------
209.165.200.229   209.165.200.224              On
```

- 次の手順のいずれかに従って、コントローラと Cisco Nexus 7000 シリーズ スイッチ間に接続を確立します。

  - 次のコマンドを入力します。

    1. **config cts sxp version sxp version 1 または 2** *1*
    2. **config cts sxp disable**
    3. **config cts sxp enable**

  - コントローラで SXP バージョン 2 が使用され、Cisco Nexus 7000 シリーズ スイッチでバージョン 1 が使用されている場合、接続を確立するために再試行間隔を設定する必要があります。 始めは短い試行間隔を設定することを推奨します。 デフォルトは 120 秒です。