Stealthwatch v7.0 の ISE 統合機能の拡張

pxGrid クライアント証明書を取得するプロセスの変更

V7.0 以降の Stealthwatch は、Stealthwatch 中央管理で生成された証明書署名要求（CSR）によって作成されたクライアント証明書のみをインポートします。詳細については、『Configuring Cisco ISE or ISE-PIC』のガイドを参照してください。

> 以前の Stealthwatch バージョンからアップグレードする場合、pxGrid クライアント証明書はそのまま ISE との接続を確立するために使用できます。ただしセキュリティ上の理由から、CSR によって pxGrid クライアント証明書を再作成することが推奨されます。

ISE 統合オプション

Stealthwatch では pxGrid との統合が強化され、データの取得および ISE との相互通信に使用できる機能と情報トピックが追加されています。これらの統合オプションが設定可能になり、システムのニーズに合わせてオンまたはオフにできるようになりました。

ISE 設定ページには、次の統合オプションが含まれています。

- 緩和アクション用の ANC（適応型ネットワーク制御）
- 強化された TrustSec コンテキストの静的 TrustSec 分類
- ユーザ セッション

ISE 接続ステータスに、pxGrid への接続ステータスと、有効になっている情報トピックに対するサブスクリプション ステータスが表示されるようになりました。

変更された緩和アクション

エンドポイント保護サービス（EPS）の隔離/隔離解除を使用した緩和アクションは、ISE 適応型ネットワーク制御（ANC）サービスおよびホストへの ANC ポリシー割り当てによる緩和アクションに置き換えられます。

ANC による緩和アクションの新しいアプローチに対応するように、ISE の設定を変更する必要があります。具体的には、ANC ポリシーを設定し、[EPSStatus] 属性ではなく [ANC ポリシー（ANC Policy）] 属性を使用するように ISE ポリシー セットを変更する必要があります。さらに SMC の pxGrid ユーザが SMC で ANC 機能を登録および使用するには、pxGrid サービスで ANC グループを設定する必要があります。ISE で ANC を設定する方法については、『Setup Adaptive Network Control』を参照してください。

強化された TrustSec コンテキスト

Stealthwatch v7.0 では、これまで同様にユーザ セッションからダイナミック TrustSec 分類を取得できるだけでなく、ISE から TrustSec の静的エンドポイント分類（IP と SGT のバインディング）を取得できます。これにより、認証プロセスで TrustSec コンテキストを使用できない環境（データセンター サーバのように静的に分類されたエンドポイント、トポロジ ベースの分類、ISE が SXP プロセスによって外部システムから学習したコンテキストなど）で、セキュリティ グループ タグ（TrustSec ID）とセキュリティ グループ名（TrustSec 名）を使用したフローの増強が可能です。

EAP チェーン セッションのサポート

Stealthwatch v7.0 は、EAP チェーン認証から派生した ISE セッションのトラッキングをサポートします。EAP チェーン セッションが正常に検出されるためには、EAP チェーン プロセスでユーザ認証が成功する必要があります。ユーザ認証が失敗したセッションは Stealthwatch で追跡されません。

パフォーマンスおよびスケーラビリティ サポートの改善

Stealthwatch v7.0 では、ISE セッションの処理に関連する大幅な改善が行われています。これにより、ハイエンド FC/SMC アプライアンス プラットフォームのアクティブ セッションを 2,000,000 までサポートできます。詳細については、『ISE Integration Scalability Support』ドキュメントを参照してください。

著作権情報

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図などの図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。