セキュアアクセスクライアントベースのZTAポスチャ設定および動作仕様

内容

お問い合わせ内容

インターネットアクセスに使用する際に、Cisco Secure Accessクライアントベースのゼロトラストアクセス(ZTA)ポスチャ機能の特定の動作と設定機能に関して、疑問が生じました。具体的な懸念事項は次のとおりです。

- オペレーティングシステムのポスチャ要件が、デバイスが必要なOSバージョンを満たしていない場合でもZTAモジュールを使用してインターネットの宛先にアクセスできる、最大365日の設定可能な猶予期間をサポートしているかどうか。
- ファイアウォール、システムパスワードなど、オペレーティングシステム以外のポスチャ要件が満たされない場合に宛先アクセスの即時ブロックが発生するかどうか。
- Secure Access GUIインターフェイスを使用して、ポスチャ要件の障害に対してカスタムの警告メッセージまたはブロック以外のアクション（モニタリングなど）を設定できるかどうか。

環境

- Cisco Secure Access with Zero Trust Access(ZTNA)機能
- クライアントベースのZTAポスチャ実装
- インターネットアクセスの使用例
- オペレーティングシステム、ファイアウォール、システムパスワードの条件を含むポスチャ要件

解決策

次のセクションで説明する内容は、Secure AccessクライアントベースのZTAポスチャ動作と設定機能に関するものです。

オペレーティングシステムのポスチャ猶予期間

説明されているオペレーティングシステムのポスチャ要件の動作は正しいです。オペレーティングシステム(OS)のポスチャ条件を設定する場合、最大365日の設定可能な猶予期間がサポートされます。この猶予期間中、必要なOSバージョンを満たしていないデバイスは、ターゲットバージョンにアップグレードする間、ZTAモジュールを使用してインターネットの宛先にアクセスできます。

オペレーティングシステム以外のポスチャ要件

オペレーティングシステム以外のポスチャ条件（ファイアウォール、システムパスワード、その他のセキュリティ制御など）では、これらの要件が満たされないと、宛先へのアクセスがただちにブロックされます。これらのポスチャタイプは、オペレーティングシステムの要件で使用可能な猶予期間機能をサポートしていません。

ポスチャ障害アクションとカスタムメッセージ

ポスチャ要件の失敗に対するアクションは、アクセスポリシー設定によって制御されます。

アクセスポリシーは、次のような複数のアクションタイプをサポートしています。

- プライベート ネットワーク間で
- Block
- 警告
- 分離

ポスチャ障害のカスタム警告メッセージと通知ページは、アクセスポリシーセキュリティプロファイル設定で設定できます。警告と通知のページ管理は、通知ページの管理に関するドキュメントと設定インターフェイスを使用して行います。

つまり、ブロッキング以外のアクション（Warnアクションによるモニタリングなど）が使用可能であり、ブロッキングアクションのみが可能であるという最初の評価に反して設定可能であることを意味します。

原因

この疑問は、オペレーティングシステムのポスチャ要件とその他のポスチャタイプの動作の違いを理解する必要があることと、Secure AccessのGUIインターフェイスでは即座に認識できない、ポスチャ障害の処理に使用できる設定オプションを明確にすることから生じました。

関連コンテンツ

- 安全なアクセスのための通知ページの管理に関するドキュメント
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。