セキュアアクセスパスワードで保護されたZIPファイルのダウンロード設定

内容

お問い合わせ内容

Cisco Secure Accessに移行した後、ユーザはパスワードで保護された（暗号化された）ZIPファイルをダウンロードできません。セキュアアクセスサービスを介して暗号化されたファイルのコンテンツにアクセスしようとすると、ダウンロードが一貫して失敗します。この問題は、カテゴリベースのブロッキング、SSLインスペクションコントロール、サンドボックス機能などの複数のセキュリティルールを備えたC8200デバイスでインターネットに送信されるトラフィックポリシーを設定しているにもかかわらず発生します。

Secure Accessの移行前にアクセス可能であった、パスワードで保護されたZIPファイルにアクセスしようとすると、ダウンロードが完全に失敗します。この問題は複数のトンネルグループで継続し、設定されている15箇所すべてに影響します。

環境

- Cisco Secure Access(Secure Access OrgID:8320925)
- C8200デバイスによるインターネット経由のトラフィックポリシーの管理
- 15の拠点にまたがる複数のトンネルグループ（TK-TGなど）
- 有効および無効の両方の設定を持つSSLインスペクションポリシー
- 特定のポリシーでサンドボックスセキュリティプロファイルを有効にする
- 特定のアクセスルールで設定されたIPSプロファイル

解決策

Cisco Secure Accessでパスワード保護されたZIPファイルのダウンロードを許可するための解決策には、暗号化ファイルへのアクセスを許可の設定と、必要に応じて適切な回避策の実装が含まれます。

プライマリ設定方法

ステップ1:Cisco Secure Accessポリシー設定へのアクセス

Cisco Secure Accessダッシュボードで、影響を受けるトラフィックを処理する特定のアクセスポリシーに移動します。

ステップ2：暗号化されたファイルアクセスの有効化

ポリシーの詳細設定で、Allow access to encrypted filesオプションを見つけて有効にします。この設定はルール単位で構成され、その特定のポリシーを使用して暗号化されたコンテンツにアクセスできるかどうかを制御します。

ステップ3：設定の適用

ポリシーの変更を保存して適用し、ユーザトラフィックに対してアクティブにします。

代替回避策

プライマリ方式で問題が解決しない場合は、次のセクションで説明する回避策を実行します。

ステップ1：影響を受けるURLを特定する

パスワードで保護されたZIPファイルがホストされている特定のURLまたはドメインを特定し、ダウンロードエラーの原因を特定します。

ステップ2：非暗号化解除リストの設定

識別されたURLを、Cisco Secure Access設定のDo Not Decryptリストに追加します。これにより、これらの特定のURLでのSSLインスペクションが防止されます。

ステップ3:SSLインスペクションバイパスポリシーの作成

SSLインスペクションが無効になっているアクセスポリシーが、これらのURLへのトラフィックを処理するように設定されていることを確認します。

このポリシーには次のものが必要です。

- SSLインスペクションが無効
- すべてのセキュリティプロファイルが無効
- SSLインスペクションが有効なポリシーよりも高い優先順位

ポリシー設定のリファレンス

次のサブセクションで概説したポリシーの順序とそれぞれの設定は、適切なトラフィック処理の基準として使用できます。

ポリシー1：カテゴリベースのブロッキングルール

- ポリシー名：IA-To-InternetContentBlock
- IPSプロファイル：なし

- 目的：特定のコンテンツカテゴリをブロックする
- ターゲット：すべてのトンネルグループ

ポリシー2:SSLインスペクションが無効なルール

- ポリシー名：IA-SSL-Inspection-MUKOU
- IPSプロファイル：無効
- セキュリティプロファイル：すべて無効
- ターゲット：すべてのトンネルグループ

ポリシー3:SSLインスペクションが有効なルール

- ポリシー名：IA-SSL-Inspection
- IPSプロファイル：有効
- セキュリティプロファイル：サンドボックス機能が有効
- ターゲット：すべてのトンネルグループ

重要な設定に関する注意事項

暗号化ファイルへのアクセスを許可する機能に相当するグローバル設定はありません。この設定は、必要に応じて個々のアクセスポリシーで設定する必要があります。暗号化されたファイルアクセスを必要とする各ポリシーでは、詳細設定の構成でこの設定を明示的に有効にする必要があります。

設定の変更をテストする際には、機能を検証する前に、Cisco Secure Accessインフラストラクチャ全体にポリシーを伝播するための十分な時間を確保してください。サービスインシデントまたはメンテナンス時間帯はテスト結果に影響を与える可能性があるため、トラブルシューティングの際に考慮する必要があります。

原因

この問題は、Cisco Secure Accessがデフォルトで、セキュリティ対策として暗号化ファイルへのアクセスをブロックするために発生します。SSLインスペクションが有効になっていて、パスワードで保護されたコンテンツや暗号化されたコンテンツが見つかった場合、このようなアクセスを許可するように明示的に設定されていない限り、サービスによってダウンロードが阻止されます。アクセスポリシーの[詳細設定]にある[暗号化されたファイルへのアクセスを許可する]はこの動作を制御し、この設定を有効にしないと、暗号化されたZIPファイルと同様のコンテンツがダウンロード処理中にブロックされます。

さらに、検査プロセスが暗号化されたコンテンツを適切に処理できない場合、SSL検査ポリシーによって暗号化されたファイルのダウンロードが妨げられる可能性があり、該当するURLに対して暗号化ファイルアクセス設定またはSSL検査バイパスが必要になります。

関連コンテンツ

- 高度なセキュリティ制御
- 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。