SSL復号化とネットワークトンネルを使用したセキュアアクセスZTNA設定同期エラー

内容

問題

Cisco Secure Client Zero Trust Access(ZTA)は正常に登録されますが、HTTP 502応答と「BadResponse」サーバ接続状態との設定同期中に失敗します。Windows 11エンドポイントからのDART口グには、登録は成功したが、設定の同期が繰り返し失敗したことが示されています。この問題が発生するのは、エンドポイントがMeraki AutoVPNトンネルを使用してセキュアアクセス/Umbrellaプロキシを使用して企業ネットワークパスに接続されている一方で、同じエンドポイントがプロキシまたはトンネルインフラストラクチャを使用せずにホームネットワークで設定の同期を正常に完了した場合だけです。

環境

- Cisco Secure Client ZTAバージョン5.1.16.4434
- Windows 11 Enterpriseエンドポイント
- AutoVPN統合を備えたMeraki MXアプライアンス
- ネットワークトンネルゲートウェイ(NTG)を使用したセキュアアクセス(SSE)
- Umbrella DNSおよびセキュアアクセスWebセキュリティ
- 企業ネットワークパスでのSSL復号化およびHTTPSインスペクションの有効化
- システムが提供したDo Not Decrypt List(DND)が最初に構成されていません

解決方法

設定同期の失敗は、セキュアアクセスのネットワークトンネルを使用する際に、ZTA関連ドメインに適切なSSL復号化バイパスを実装することで解決されました。

ステップ1:SSL復号化の影響を特定する

ZTAドメインに関連する復号化イベントのセキュアアクセスのアクティビティ検索ログを確認して、SSL復号化が設定の同期エラーの原因となっていることを確認します。

ステップ2：システム提供のDNDリストを設定する

Network Tunnels Gateway(NTG)をセキュアアクセスで使用する場合、SSLインスペクションからZTA関連のトラフィックを適切にバイパスするために、System Provided DNDを有効にする必要があります。

Secure Access Dashboard > Secure > Do Not Decrypt Listsの順に移動し、System Provided Do Not Decryptリストを変更します。

ステップ3:ZTAドメインのセキュリティプロファイルの作成

System Provided DND Listを使用して、必要なZTA関連ドメインを新しいセキュリティプロファイルに追加します。

- zpc.sse.cisco.com
- *.zpc.sse.cisco.com
- ztna.sse.cisco.com
- acme.sse.cisco.com
- devices.api.umbrella.com

ステップ4：テストルールへのセキュリティプロファイルの適用

ZTAドメインがバイパスされる新しく作成されたセキュリティプロファイルをテストルールに割り当て、設定を検証します。

手順5：構成の同期の検証

企業ネットワークからZTA登録と設定の同期をテストします。これで、HTTP 502エラーなしで同期が正常に完了します。

ステップ6:Merakiチームとの調整

包括的なカバレッジについては、Merakiサポートと連携して、Secure Accessインスペクションからバイパス可能な公式のZTA関連URLおよびドメインを検証します。次のMerakiドキュメントを参照してください。

- クラウド接続用のアップストリームファイアウォールルール
- MerakiダッシュボードURLの更新 – PCIコンプライアンス

原因

設定の同期に失敗した原因は、SSL復号化と、企業ネットワーク上でのゼロトラストアクセストラフィックのプロキシ化です。ネットワークトンネルゲートウェイ(NTG)をセキュアアクセスとともに使用する場合は、System Provided Do Not Decrypt List(DND)を使用して、ZTA関連ドメインをバイパスする必要があります。 このバイパス設定がない場合、SSLインスペクションは証明書チェーンを変更し、ZTAコントロールプレーンの通信を妨害します。これにより、クライアントは設定の同期試行中にHTTP 502応答を受信します。

関連コンテンツ

- セキュアアクセスの復号化とSSLの問題のトラブルシューティング
- セキュアアクセスゼロトラストクライアントベースの登録サービス

- セキュアアクセスのためのZTAドメインの要件
- セキュアアクセスエラー登録問題のトラブルシューティング
- セキュアクライアント設定同期エラーのトラブルシューティング
- トラブルシューティングのための詳細なZTNAログの収集
- 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。