WSA 1000Vの非標準ポートトラフィック用のプロキシポートの設定

内容

問題

VMwareでホストされているWSA 1000Vプロキシは、ポート80および443でクライアントトラフィックを正しく処理していましたが、ポート8890などの非標準ポートではトラフィックを処理しませんでした。非標準ポートを使用した宛先へのアクセスが最初にポリシーによってブロックされたとき、WSAはブロックされた要求を正しく記録しました。ただし、IPアドレスとURLを許可ポリシーに追加した後も、トラフィックはまだ失敗し、対応するログはプロキシで生成されませんでした。この動作は、許可ポリシーが作成された後にトラフィックがWSAに到達せず、処理されず、非標準ポートを使用したアプリケーションへのクライアントアクセスに影響を与えていることを示唆しています。

環境

- VMware上でホストされるCisco WSA 1000Vプロキシ
- ソフトウェアバージョン15.0.0
- ポート80および443上のトラフィックは正常に処理されます。
- 非標準ポートトラフィック（ポート8890など）がプロキシによって処理されていない。
- 影響を受ける宛先に設定されたポリシーを許可します。

解決方法

この問題は、IDプロファイル設定で非標準ポートをサポートするようにWSAを設定することで解決されました。必要な非標準ポート番号を含むように、プロキシポートの設定を更新する必要がありました。

設定手順

ステップ1:Web Security Managerインターフェイスにアクセスします。

ステップ2:識別プロファイル設定に移動します。

Web Security Manager > Identification Profilesの順に移動します。

ステップ3：非標準ポートサポートを必要とするIDプロファイルを選択します。

ステップ4:Advanced configuration オプションを展開します。

IDプロファイルページでAdvancedタブを展開します。

ステップ5:プロキシポートを設定します。

ポート設定にアクセスするには、Proxy Portsの横にあるリンクを選択します。

ステップ6：必要な非標準ポート番号を追加します。

クライアントが標準外のポート接続（8890など）に使用する特定のポート番号を追加します。

ステップ7：設定変更を保存し、確定します。

これらの設定変更を実装すると、WSAは指定された非標準ポート上のトラフィックを処理および検査できるようになり、プロキシがクライアント接続を適切に処理して、これらのポートを使用するトラフィックにポリシーを適用できるようになります。

原因

WSA 1000Vは、標準のHTTP（ポート80）ポートとHTTPS（ポート443）ポートのみを含むデフォルトのプロキシポート設定で設定されていました。識別プロファイルプロキシポートの構成に、クライアントアプリケーションで必要な非標準ポートが含まれていませんでした。これらのポートがIdentification Profile Advanced設定で明示的に設定されていなければ、WSAは、宛先に対してallowポリシーが設定されていても、非標準ポートを使用するトラフィックの代行受信、処理

、または適用を行うことができませんでした。

関連コンテンツ

- 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。