UmbrellaプロキシがNinjaアプリケーションの接続をブロック

内容

お問い合わせ内容

Cisco Umbrella経由で接続すると、ダウンロードしたセットアップファイルを使用してリモートシステムを実行できない。アプリケーションがUmbrella保護の下で機能せず、特にリモートシステムへのアクセスに影響する。Cisco Umbrellaプロキシが無効になっている場合、同じリモートシステムが問題なく正常に動作します。

トラブルシューティングの試みには、システムセキュリティと宛先がANYに設定された別のポリシーを使用したテストも含まれましたが、問題は解決しませんでした。さらに、ゼロトラストアクセス(ZTA)経由のトラフィックのルーティングが試行されましたが、問題は変化しませんでした。トラフィックはTCP/443のセキュアアクセスを通過することを許可されましたが、エンドポイントでは接続がブロックされました。

環境

- プロキシ機能を有効にしたCisco Umbrella
- ゼロトラストアクセス(ZTA)の設定
- TCP/443トラフィック用に設定されたセキュアアクセスポリシー

解決策

この問題を解決するには、Umbrellaプロキシから特定のNinjaOne関連ドメインを除外して、リモートアクセスアプリケーションに直接接続できるようにする必要があります。

手順1：影響を受けるドメインを特定する

パケットキャプチャとHARファイルを分析すると、NinjaOne関連のドメインがUmbrellaプロキシの影響を受けていることがわかります。

- ninjarmm.net
- ninjarmm.com
- app.ninjarmm.com
- ninjaone.com
- agent-app.ninjaone.com

ステップ2：ドメイン除外を設定します。

Secure Web Gateway(SWG)インターネットセキュリティポリシーとZTAインターネットトラフィックのステアリングの両方から、特定されたドメインを除外します。この設定変更により、これらのドメインはUmbrellaプロキシをバイパスし、直接接続を確立できます。


注:Do Not Decrypt(DND)リスト設定は、この問題を解決するには効果的ではないことが確認されています。トラフィックのステアリングと除外が推奨されるアプローチです。

ステップ3：設定変更の適用

InnjaOne関連のトラフィックをプロキシ処理から除外するには、Umbrella設定でドメイン除外を実装します。これにより、リモートアクセスアプリケーションは必要なサービスへの直接接続を確立できます。

ステップ4：解決の検証

適用除外を適用した後に、リモートアクセスアプリケーションの機能をテストして、他のトラフ

ィックに対するUmbrella保護を維持しながら、適切な接続が復元されることを確認します。

原因

この問題は、トラフィックがCisco Umbrellaプロキシ経由でルーティングされるときに、NinjaOneリモートアクセスアプリケーションがプロキシ接続を拒否するために発生します。このアプリケーションが正常に機能するには、特定のNinjaOneドメインに直接接続する必要があります。これらの接続がUmbrellaを介してプロキシされると、リモートアクセスサービスは必要な通信チャネルを確立できず、トラフィックを許可するようにセキュリティポリシーが設定されていても、アプリケーション障害が発生します。

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。