ネットワーク中断後のWSAアップストリームプロキシのヘルスチェックの問題

内容

問題

長時間のネットワーク中断の後、FQDNで指定されたアップストリームプロキシを使用するように設定されたCisco Webセキュリティアプライアンス(WSA)が、アップストリームプロキシへのトラフィックの転送を再開できず、代わりにトラフィックを直接送信する可能性があります。この問題は、ネットワークの停止中にWSAがアップストリームプロキシを「デッド」とマークした場合に発生しますが、ネットワーク接続が復元された後でも、アップストリームプロキシがいつ再び使用可能になったかをWSAが認識できなくなります。

確認された具体的な症状は次のとおりです。

- WSAがFQDNおよび「Failure Handling = go Direct」によるアップストリームプロキシで設定されている
- アップストリームプロキシとDNSサーバの両方への接続に影響を与える長期的なネットワーク中断
- ネットワークの回復後、アクセスログにはDEFAULT_PARENTタグが表示されず、トラフィックがアップストリームプロキシをバイパスし続けることを示します
- 同じ環境内の別のアプライアンスが正常に動作している間に、あるWSAアプライアンスで問題が発生する

環境

- Cisco Webセキュリティアプライアンス(WSA)Sシリーズ
- AsyncOS 14.5.2-011（該当バージョン）
- ハードウェア： S695

- FQDN仕様で設定されたアップストリームプロキシ
- 「直接実行」として設定された障害処理
- L2スイッチインフラストラクチャを使用したネットワーク環境

解決方法

この問題は、CSCwi13124の修正を含むバージョンにAsyncOSをアップグレードすることで解決されます。このバグは、次のAsyncOSバージョンで修正されています。

- AsyncOS 15.5.0-566
- AsyncOS 15.5.0-710

現在のバージョンのための一時的な回避策

即座にアップグレードできない環境では、応答しないアップストリームプロキシをチェックするための最大アイドルタイムアウトを調整することで、一時的な緩和策を使用できます。

ステップ1:CLIにアクセスし、高度なプロキシ設定に移動します。

```
cli -> advancedproxyconfig -> MISCELLANEOUS
```

ステップ2：最大アイドルタイムアウト設定を変更します。

```
"Enter maximum idle timeout for checking unresponsive upstream proxy (in seconds)"
```

ステップ3:デフォルトの最大値（86400秒/24時間）をより小さい値に減らして、ヘルスチェックの間隔を短くします。

即時リカバリ方式

問題が現在トラフィックフローに影響している場合は、次のコマンドを使用すると、ただちにアップストリームプロキシ機能を復元できます。

ステップ1：診断メニューにアクセスします。

```
CLI > diagnostic > PROXY > kick
```

これにより、プロキシプロセスが再起動され、通常のアップストリームプロキシ動作が復元されます。

検証およびテストの手順

問題が存在するかどうか、またはアップグレード後に解決したかどうかをテストするには、次の手順を確認します。

ステップ1：ベースラインモニタリングの確立

アクセスログとプロキシログをモニタして、WSAがトラフィックをアップストリームプロキシに送信していることを確認します。トラフィックがアップストリームプロキシ側に到達していることを確認します。

ステップ2：ネットワーク中断のシミュレーション

アップストリームプロキシへの通常のトラフィックフローを確認した後、次の接続を切断します。

- WSAからアップストリームプロキシへの接続
- WSAからDNSサーバへの接続

ステップ3：障害検出の監視

プロキシログとシステムログで次のインジケータを確認します。

- プロキシログは、アップストリームプロキシを「。.. declared dead」として表示できます。

- システムログに「Critical: Reached maximum failures querying DNS server ...」と表示される場合がある

ステップ4：中断状態の管理

プロキシプロセスを再起動せずに、ステップ2の「disconnected」状態を維持し、約10時間リクエストの生成を続行します。

ステップ5：接続の復元

約10時間後、手順2で切断した接続を復元します。

ステップ6：リカバリ動作の監視

ステップ5が完了したら、プロキシプロセスを再起動せずにアクセスログとプロキシログをモニタします。

- 固定システム：トラフィックはアップストリームプロキシを経由して流れ始め、プロキシログは通常のヘルスステータスの遷移を示します
- 該当システム：アクセスログには、アップストリームプロキシをバイパスし続けるトラフィックが表示され、プロキシログには「。.. was sick, now healthy」または「。.. was healthy, now sick」のメッセージは表示されません

原因

この問題の根本的な原因は、アップストリームプロキシのヘルスチェックメカニズムの論理的な欠陥です。WSAは、設定されているアップストリームプロキシが「停止した」（応答しない）と判断すると、指数関数的なバックオフアルゴリズムを実装して、障害が発生するたびにヘルスチェック間隔を2倍にします。この間隔は、最大24時間（86400秒）に達する可能性があります。

この問題は、これらの延長されたインターバルの間にアップストリームプロキシが再び使用可能になったときに発生します。プロキシが回復して正常に応答しているとしても、WSAは完全に設定された時間間隔が経過するまでヘルスチェックを実行しません。これにより、アップストリームプロキシの使用を再開する代わりに、最大24時間にわたって直接トラフィックルーティングが継続される可能性があります。

この動作は、次の場合にWSA設定に影響します。

- アップストリームプロキシはDNSホスト名/FQDNで指定されます（IPアドレスではありません）
- 障害処理が「直接実行」に設定されている
- 拡張ネットワークの中断は、アップストリームプロキシとDNSサーバ接続の両方に影響します

Cisco Bug ID:CSCwi13124

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。