特定のサイトを閲覧した際の 502/504 GATEWAY_TIMEOUT エラー

目次

質問：

特定のサイトを参照する場合に 502/504 GATEWAY_TIMEOUT エラーが表示されるのはなぜですか。

症状： ユーザは、特定の Web サイトをブラウズする際に 502 または 504 のゲートウェイ タイムアウト エラーを受信しています。

ユーザが Web サイトをブラウズする際に 502 または 504 のゲートウェイ タイムアウト エラーを受信しています。 アクセス ログに「NONE/504」または「NONE/502」が表示されます。

サンプル アクセス ログ ライン：

1233658928.496 153185 10.10.70.50 **NONE/504** 1729 GET http://www.example.com/ - DIRECT/www.example.com - .....

WSA が 502 または 504 のゲートウェイ タイムアウト エラーを返す原因は複数あります。 これらのエラー応答は似ていますが、これらの間にあるわずかな違いを理解することが重要です。

発生する可能性のあるシナリオ タイプの例を次に示します：

- **502**： WSA は Web サーバとの間に TCP 接続を確立しようとしましたが、SYN/ACK を受信しませんでした。
- **504**： WSA は Web サーバとの接続を終端する TCP リセット（RST）を受信しています。
- **504**： WSA は、DNS のような Web サーバとの通信が失敗する前に必要なサービスからの応答を受け取っていません。
- **504**： WSA は Web サーバとの間に TCP 接続を確立して GET 要求を送信しましたが、WSA は HTTP 応答を受信しません。

次に各シナリオの例と潜在的な問題に関する詳細を示します：

502： WSA は Web サーバとの間に TCP 接続を確立しようとしましたが、SYN/ACK を受信しませんでした。
Web サーバが WSA の SYN パケットに応答しなければ、一定量の試行の後に、クライアントに 502 のゲートウェイ タイムアウト エラーが送信されます。

この問題の一般的な原因は次のとおりです：
1. Web サーバまたは Web サーバのネットワークで問題が発生しています。
2. WSA ネットワークのネットワーク問題により、SYN パケットがインターネットに到達することが阻害されています。
3. ファイアウォールやそれに類似したデバイスが WSA SYN パケットや Web サーバの SYN/ACK をドロップしています。
4. IP スプーフィングが WSA でイネーブルにされますが、正しく設定されていません（リターン パスのリダイレクトなし）。

トラブルシューティングの手順：

まず、WSA が Web サーバで ICMP ping を実行できるかどうかを確認します。 これは、次の CLI コマンドを使用して実行できます：
WSA> *ping www.example.com*
ping が失敗しても、サーバがダウンしていることを意味するわけではありません。 ICMP パケットがパスのどこかでブロックされていることを示している場合もあります。 ping が成功する場合は、WSA に Web サーバへの接続の基本レイヤ 3 レベルがあることが確実にわかります。 telnet テストにより、WSA に Web サーバへのポート 80 での TCP 接続を確立する機能があるかどうかを確認します。 telnet テストの実行については、この文書の手順を参照してください。

ネットワークの問題またはファイアウォールのブロック
ping は成功するが telnet は失敗する場合、ファイアウォールなどのフィルタリング デバイスが、このトラフィックがネットワークを通じて取得されることを阻害している可能性があります。 ファイアウォール ログまたはファイアウォールからのパケット キャプチャあるいはその両方を、さらに詳細に分析することを推奨します。
IP スプーフィングがイネーブルだが正しく設定されていない
WSA または telnet テストを介した明示的なプロキシが正常に完了した場合、これは WSA が Web サーバと直接通信できることを意味しますが、クライアントが IP スプーフィングを使用して WSA を介してプロキシする場合は問題があります。

クライアントの IP スプーフィングなしの場合：
- WSA は送信元として独自の IP アドレスを使用して Web サーバに SYN を送信します。 パケットが復帰した場合、直接 WSA に送信されます。

クライアントの IP スプーフィングがある場合：
- WSA は SYN を送信しますが、代わりに送信元としてクライアントの IP を使用します。 特別なネットワークの設定なしで、応答パケットが WSA ではなくクライアントに送信されます。
- クライアント IP スプーフィングを使用するには、パケットが正しくリダイレクトされることを促進するためのきわめて特殊な方法でネットワークを設定する必要があります。 Web サーバのリターン パス パケットが WSA ではなくクライアントに送信されると、WSA はサーバの SYN/ACK を確認できず、クライアントに 502 ゲートウェイ タイムアウト エラーを送り返します。

504： WSA は Web サーバとの接続を終端する TCP リセット（RST）を受信しています。

WSA が Web サーバへのアップストリームの接続で TCP リセット パケットを受信すると、WSA はクライアントに対して 504 のゲートウェイ タイムアウト エラーを送信します。

この問題の一般的な原因は次のとおりです：
1. シスコのレイヤ 4 トラフィック モニタ（L4TM）が、WSA のプロキシが Web サーバに接続

するのを妨げています。
2. ファイアウォール、IDS、IPS、または他のパケット インスペクション デバイスが WSA を妨げています。

トラブルシューティングの手順：
最初に、TCP RST が L4TM から送信されているのか別のデバイスから送信されているのかを判別します。
L4TM がこのトラフィックを妨げている場合、[Monitor] > [L4 Traffic Monitor] を選択すると、トラフィックが GUI のレポートに表示されます。 それ以外の場合、RST はさまざまなデバイスから送信されています。
L4TM ブロック：
L4TM がブロックされている場合は、WSA プロキシも実行しているポートでブロックしないことが推奨されています。 これには複数の理由があります：
1. WSA プロキシは、問題が発生した場合は単に TCP 接続をリセットするのではなく、友好的なエラー メッセージを出します。 これは、エンド ユーザがブロックされた場合の混乱を抑える役割を果たします。
2. WSA プロキシには特定の内容をスキャンしてブロックする機能があり、一方 L4TM はブラックリスティングされた IP アドレスに一致するすべてのトラフィックをブロックします。
L4TM をプロキシ ポートでブロックしないように設定するには、[GUI] > [Security Services] > [L4 Traffic Monitor] を実行します。
サイトが既知の不正な Web サイトだがトラフィックが許可される理由がある場合、そのサイトは以下でホワイト リストされている可能性があります：
[GUI] > [Web Security Manager] > [L4 Traffic Monitor] > [Allow List]

ファイアウォール / IDS / IPS ブロッキング：
ネットワーク上の別のデバイスが WSA の Web サーバへの接続を妨げる場合、次を分析することが推奨されます：
1. ファイアウォール ブロックのログ
2. 問題時の入力パケット キャプチャおよび出力パケット キャプチャ

ブロックのログは、デバイスが WSA を妨げているかどうかを迅速に確認する場合があります。 ファイアウォール、IPS、または IDS がトラフィックをブロックし、適切にログを取らない場合があります。 この場合、TCP RST の発信元を検証する唯一の方法は、デバイスからの入力と出力のキャプチャを取得します。 RST に入力インターフェイスが送信され、パケットが出力側を移動していない限り、最終的にセキュリティ デバイスが原因となります。

504： WSA は Web サーバとの間に TCP 接続を確立して GET 要求を送信しましたが、WSA は HTTP 応答を受信しません。

WSA が HTTP GET を送信しますが、応答を受け取らない場合、WSA はクライアントに 504 ゲートウェイ タイムアウト エラーを送信します。

この問題の一般的な原因は次のとおりです：

- ファイアウォール、IDS、IPS、または他のパケット インスペクション デバイスは、TCP 接続を許可していますが、HTTP コンテンツが Web サーバに到達するのを妨げています。 この場合、telnet テストはブロックされているタイプの HTTP データを分離するのに役立つ可能性があります。

ファイアウォールのブロックのログは、デバイスが WSA をブロックしているかどうか、およびその原因を迅速に確認できます。 ファイアウォール、IPS、または IDS がトラフィックをブロックし、適切にログを取らない場合があります。 この場合、TCP RST の発信元を検証する唯一の方法は、デバイスからの入力と出力のキャプチャを取得します。 RST に入力インターフェイス

が送信され、パケットが出力側を移動していない限り、最終的にセキュリティ デバイスが原因となります。

Telnet を使用した Web サーバとの接続テスト

次のように WSA CLI から **telnet コマンド**を実行します：

[WSA] > [Telnet]
telnet を開始するインターフェイスを選択します。
1. Auto
2. Management (192.168.15.200/24: wsa.hostname.com)
3. P1 (192.168.113.199/24: data.com)
[1] > **3**

リモート ホスト名または IP アドレスを入力します。
[] > **www.example.com**

リモート ポートを入力します。
[25] > **80**

Trying 10.3.2.99...
Connected to www.example.com.
Escape character is '^]'.

注: 赤色の「Connected」メッセージは、TCP が正常に WSA と Web サーバ間で確立されたことを示しています。

HTTP 要求はこの telnet セッションを使用して手動で送信することも可能です。 次は、「Connected」メッセージの後に入力できるサンプル要求です：

GET http://www.example.com HTTP/1.1
HOST: www.example.com
{{Enter}

注: 最後に必ず追加の改行を追加します。これがないとサーバが要求に応答しません。