Umbrellaコンポーネントでポートアドレス変換(PAT)を使用する場合のポート枯渇のトラブルシューティング

内容

はじめに

このドキュメントでは、ローミングクライアントや仮想アプライアンス(VA)を使用しているUmbrellaのお客様と、ポートアドレス変換を使用するファイアウォールでポートが使い果たされるという問題について説明します。これは、多数のローミングクライアントがある環境や、VAを通過する大量のトラフィックがある環境で発生する可能性が高くなります。症状としては、DNSクエリの応答が遅くなったり、タイムアウトになったりすることがあります。

原因

ローミングクライアントも仮想アプライアンスも、DNSクエリに対する応答をキャッシュしません。さらに、ローミングクライアントは、ネットワーク環境を分析し、ヘルスチェックとして頻繁に「プローブ」DNS要求を送信します。

推奨事項

- Umbrellaダッシュボードのドメイン管理で内部ドメインが正しく設定されていることを確認します。高頻度のクエリの量を減らすには、Active Directoryゾーン（およびその他の内部ゾーン）を含める必要があります。
- ファイアウォールのPAT設定の一部を確認します。
  - UDPセッションタイムアウトが長いと問題になる可能性があります。通常、UDPセッションのタイムアウトは約15秒に設定することを推奨します。ただし、ネットワーク上の他のアプリケーションでUDPが頻繁に使用されている場合は、タイムアウト時間が長くなる可能性があるので注意してください。
  - ファイアウォールによっては、PATプールのサイズを増やして同時接続数を増やすことができます。
- VA専用に使用できるIPアドレスがある場合は、ファイアウォールでPATの代わりに1:1 NATを使用します。注：「1:1 NAT」は「Direct NAT」とも呼ばれますが、これは誤った名前です。正確な技術用語は「1:1 NAT」です。

- IPごとの接続制限を確認します。多くの場合、問題のデバイスに適用されるとは予想されないポリシーが実際に制限を適用しています。確認方法については、次のセクションを参照してください。

ASAのIPごとの接続制限を確認する

次の手順を実行します。

- パケットがファイアウォールでドロップされた理由を確認するために、キャプチャを使用してASAを設定します。

```
capture asp type asp-drop all match ip any host 208.67.222.222
```

- 対象のIPに対してドロップされているパケットを探します。接続制限理由は「Drop-reason: (conn-limit)」と表示されます。
- 次のコマンドを使用して、ホストの接続制限を確認します。

```
show local-host detail | begin <IP Address of VA or roaming client>
```

  - この数はある制限（つまり999）で固定されていて、増加することはありませんか。その場合は、接続の制限を示します。
- これを適用しているサービスポリシーを確認します。見つかった場合は、ポリシーマップを確認します。

```
show run service-policy, show policy-map NAME
```

  - （たとえば）ホストごとの接続制限を1000に設定するポリシーマップ「NAME」が見つかった場合、より多くの接続が使用可能になるまで、デバイスからの新しいDNSパケットがドロップされます。UDPはステートレスであり、再試行は行われません。
- 解決するには、そのサービスポリシーを削除します（サービスポリシー名は内部にありません）。 接続は、この例では1Kの制限を超えて開始する必要があります。 これは、ローミングクライアントよりもVAの方が高速で発生します。

その他の推奨事項

これらの推奨事項が役に立たない場合は、次の回避策が考えられます。

1. Umbrellaダッシュボード – >レポート – >上位の宛先レポートを使用して、過去24時間以内に多数の要求があった1つ以上のドメインを特定します。
2. Umbrellaダッシュボード – > Configuration —> Domain Managementで、1つ以上の大容量ドメインをリストに追加し、「Applies to」を「All Appliances and Devices」に設定します。
3. その後、これらのドメインに対するクエリは、VAによってローカルDNSに転送されます。

理想的には、ローカルDNSは208.67.220.220/208.67.222.222のUmbrella DNSに転送するように設定する必要がありますが、外部DNSに転送するように設定することもできます。
4. ローカルDNSは、権限を持つドメインのクエリーを処理します。
5. ローカルDNSが非ローカルドメインのクエリを受け入れると仮定して、これらの他のドメインのクエリは外部DNSに転送されます。

これは、ローカルDNSではDNSの結果をキャッシュできますが、ローミングクライアントと仮想アプライアンスではキャッシュできないためです。この回避策を使用すると、トラフィックが増加し、内部DNSの負荷が高くなることに注意してください。そのため、これらのDNSが過負荷にならないように注意して監視してください。

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。