ASA VPNロードバランシングディレクタの選択プロセス

内容

概要

このドキュメントでは、Cisco 5500-Xシリーズ適応型セキュリティアプライアンス(ASA)を使用したVPNロードバランシングシナリオにおけるディレクタ選出プロセスについて説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメント内の情報は、ソフトウェア バージョン 9.2 を実行している Cisco ASA 5500-X に基づきます。

> **注**：このドキュメントは、この機能がバージョン 7.0(1) で初めて導入されて以降のすべてのソフトウェア バージョンにも適用されます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

VPN ロード バランシングは、ネットワーク トラフィックを仮想クラスタ内のデバイス間で均等に分散させるために使用されるメカニズムです。ロード バランシングは単純な分散に基づいており、アカウントのスループット使用率などの要素を考慮しません。ロードバランシングクラスタは、ディレクタと1つ以上のセカンダリデバイスの2つ以上のデバイスで構成され、これらのデバイスを同じように設定する必要はありません。

ロード バランシング アルゴリズム

ロード バランシング アルゴリズムの概要を以下に示します。

- ディレクタデバイスは、内部IPアドレスの昇順でセカンダリクラスタメンバーのソートされたリストを維持します。
- 負荷は、各セカンダリ クラスタ メンバーから提供される整数パーセンテージ（アクティブ セッション数/最大セッション数の値）として計算されます。
- ディレクタデバイスは、IPSec/Secure Sockets Layer(SSL)VPNトンネルを、他のデバイスよりも1 %高くなるまで、最初に最も負荷の低いデバイスにリダイレクトします。
- ディレクタデバイスは、すべてのセカンダリクラスタメンバーがディレクタデバイスよりも1 %高い場合にのみ、自身にリダイレクトされます。

1つのディレクタと2つのセカンダリクラスタメンバーを含む例を次に示します。

- すべてのノードが 0% の負荷で始まり、すべてのパーセンテージが最も近い 0.5% に丸められます。
- すべてのメンバーの負荷がダイレクタ・デバイスよりも1%高い場合、ダイレクタ・デバイスが接続を取得します。
- ディレクタデバイスが接続を取得しない場合、セッションは現在ロード率が最も小さいバックアップデバイスによって取得されます。
- すべてのメンバーの負荷パーセンテージが同じ場合は、セッション数が最も少ないバックアップ デバイスがセッションを取得します。
- すべてのメンバーの負荷パーセンテージが同じでセッション数も同じ場合は、IP アドレスが最も低いバックアップ デバイスがセッションを取得します。

ディレクタ選定プロセス

VPN負荷分散ディレクタの選択プロセスは、クラスタ外部ネットワークで実行されます。外部ネットワークで交換されるデータには、次の2種類があります。

- ディレクタディスカバリに使用されるクラスタIPアドレスのアドレス解決プロトコル(ARP)パケットが交換されます。ディレクタを検出するためにクラスタIPアドレスに送信される

ARPパケットの最大数は次のとおりです。

(10 - priority) + 1 です。

ここで、*priority は* **vpn load-balancing CLI コマンドの priority サブコマンドで設定されます。**

- Hello 要求/応答メッセージの外部で UDP パケットが交換されます。ポート番号は、**cluster port load-balancing サブコマンドで指定され、デフォルトで 9023** に設定されます。

例として、ロードバランシングデバイスのプライオリティが*5*の場合、どのディレクタデバイスもクラスタIPアドレスを所有しているかどうかを確認するために、最大6つのARPパケットの送信が試行されます。ディレクタデバイスが検出されると、ASAはそれ以上のARPメッセージを送信せず、15秒待機してからUDP Hello要求を送信します。その後、ディレクタデバイスはUDP Hello応答で応答します。

リブート シナリオに関する警告

ロード バランシング クラスタ内に 2 つの ASA が存在するリブート状況では：

- リブート前は、ASA-1またはASA-2のいずれかがディレクタでした。
- ASA-1 がリブートされます。
- ASA-2は、以前はディレクタでなかった場合はディレクタになります。
- ASA-1は、リブート後にメンバとしてクラスタに参加するだけです。

ロード バランシング アルゴリズムは、クラスタ デバイスの外部インターフェイスが接続されるスイッチの設定の影響も受ける可能性があります。たとえば、スイッチに接続されたデバイスがリブートされると、スパニングツリー アルゴリズムが接続の遅延を引き起こす可能性があります。

ヒント：spanning-tree port fast コマンドがプロセスの高速化に役立ちます。

場合によっては、ロードバランシングが有効になっている新しくリブートされたASAが、スイッチの接続遅延により現在のディレクタデバイスに到達できないため、ディレクタデバイスになろうとします (ディレクタデバイスがすでに存在する場合でも) 。ARPコリジョンの結果、ディレクトリの競合が検出されると、メディアアクセス制御(MAC)アドレスの低いASAが優先されますが、MACアドレスの高いASAはディレクタデバイスの役割を放棄します。

ディレクタの再選出プロセス

ディレクタデバイスの再選出を引き起こす状況は2つあります。

クラスタから削除されたディレクタデバイス

ASA 上の機能を無効にすると、ブロードキャスト メッセージがすべてのクラスタ メンバーに送信されて変更が通知され、前述の選出プロセスが実行されます。

Directorデバイスがクラスタメンバーの Helloメッセージに応答しない

ディレクタデバイスがクラスタメンバーHelloメッセージに応答しない場合、ディレクタが存在しなくなったことを検出するのに約20秒かかります。Hello メッセージは 5 秒ごとに送信されます（設定不可）。 クラスタメンバーが4つのHelloメッセージの後にディレクタデバイスから応答を受信しない場合、選出プロセスがトリガーされます。

トラブルシュート

> **注：debug コマンドを使用する前に、「**debug コマンドの重要な情報」を参照してください。

次の debug コマンドは、システムに伴う問題をトラブルシューティングする場合に役に立つ可能性があります。

- **debug fsm 255：このコマンドは、一般的な有限状態マシン デバッグをアクティブにするために使用します。**非アクティブにするには、**no debug all コマンドを入力します。**
- **debug menu vpnlb 3：このコマンドは、VPN ロード バランシングのデバッグ トレースをアクティブにするために使用します。**非アクティブにするには、**debug menu vpnlb 3 コマンドを再度入力します。**
- **debug menu vpnlb 4：このコマンドは、VPN ロード バランシング関数トレースをアクティブにするために使用します。**非アクティブにするには、debug menu vpnlb 4 コマンドを再度入力します。

関連情報

- **ロード バランシングの概要**
- **テクニカル サポートとドキュメント – Cisco Systems**