

ユーザー管理

エグゼクティブ・サマリ

IT 組織は、Blue Coat ProxySG アプライアンスに搭載の MACH5 テクノロジーの WAN 最適化を実装することで、インターネット・ゲートウェイの近くや支店/拠点、データ・センタ、さらには個別のエンド・ポイントに至るまで、分散型環境のあらゆるユーザーに対するビジネス・アプリケーションの配信を加速化しながら保護します。ブルーコートの WAN 最適化ソリューションの一環として、ProxySG アプライアンスは透過型 ADN (アプリケーション配信ネットワーク)における WAN 最適化を実行するため、管理者は既存のネットワーク・インフラストラクチャに WAN 最適化ソリューションをシームレスに導入できます。

透過型 ADN とは

導入される WAN 最適化ソリューションは通常、多数のエッジ・サイト(支店/拠点)からアクセスされる 1 つ以上のコアな場所から構成されます。エッジの ProxySG アプライアンスがコアの ProxySG アプライアンスと通信する場合、その通信は ADN トンネルと呼ばれる接続を介して行われます。コア ProxySG アプライアンスがインライン導入されていて、透過型 ADN トンネルが設定されている場合、その通信はネットワークで透過的になり、元のクライアントからの要求の宛先 IP アドレスとポートの両方が保持されます。Blue Coat SGOS の [reflect-client-ip]機能が有効な場合は、接続の送信元 IP も保持されます。

透過型 ADN を導入すべき理由

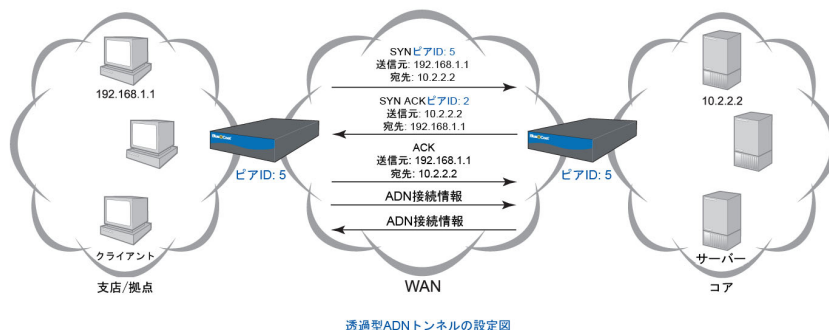
透過型 ADN 導入の重要な利点は、WAN を介する転送および接続の情報を保持できることです。これは、ネットワーク上のトラフィックの可視性を得る上で不可欠です。代替ソリューションとして明示型 ADN トンネルを使用する ADN を導入すると、エッジとコアのアプライアンス間の WAN トラフィックがすべて固定ポートに送信され、アプライアンスのアドレスが送信元および宛先 IP アドレスとして表示されます。導入の多くで問題ありませんが、多くの顧客が、トラフィック・フロー内の IP およびポート情報の可視性が必要なネットワーク管理ツール(Netflow など)を使用していたり、単に IP または宛先ポートによって特別に実施されるネットワーク・ポリシー(セキュリティ、ルーティング、トラフィック・シェーピング)を設定していたりします。そのため、明示型のトンネリング・ソリューションを提供するだけのベンダでは十分な対応ができません。透過型 ADN ではこの情報が保持されるため、管理者は既存のネットワークを変更せずシームレスに導入することができます。

透過型 ADN のもう 1 つの利点は、ネットワーク内のピアごとに ADN ルーティング情報を設定する必要がないことです。透過型 ADN に導入されている ProxySG アプライアンスでは、ADN ピアの自動検出が可能です。ただし、ADN ノードは、ADN Manager を使用して、ADN 内でメンバーシップを確立するために登録する必要があります。

透過型 ADN の仕組み

透過型 ADN を利用するには、コア ProxySG アプライアンス(複数可)を物理的にインラインで導入するか、または仮想的にインラインで導入する(WCCP などを使用)必要があります。これにより、コア ProxySG アプライアンスの先にあるサーバーに対する要求を透過的にインターセプトできます。透過型 ADN の主な機能により、クライアントの送信元 IP だけでなく、サーバーの宛先 IP およびポートを維持することができます。これは、透過型 ADN トンネルと [reflect-client-ip]機能によって実現されます。送信元 IP を保持するには、エッジ ProxySG アプライアンスの [reflect-client-ip]オプションを有効にする必要があります。[reflect-client-ip]機能を有効にすると、ProxySG アプライアンスがサーバー側の要求を送信する際に、クライアントの送信元 IP アドレスが保持されます。

この機能は、透過型 ADN ソリューションとは無関係な機能です。透過型 ADN トンネルで宛先 IP とポートを保持するには、これらの接続が自身を ADN 接続であると認識する独自の方法を実装する必要があります。それには、接続の確立時に TCP オプション・ヘッダを使用します。エッジ ProxySG アプライアンスは、コア ProxySG アプライアンスへの接続を開始するとき、SYN パケットに自身のピア ID が含まれる TCP オプション・ヘッダを挿入します。これにより、コア ProxySG アプライアンスがエッジ ProxySG アプライアンスの ADN メンバーシップを確認でき、その接続を ADN 接続として識別できるようになります。SYN を送信している ProxySG アプライアンスが受信側の ProxySG アプライアンスと同じ ADN の一部でない場合、ADN トンネルが確立されず、コア ProxySG アプライアンスは、その接続を標準のフォワード・プロキシ(非 ADN)接続として処理します。SYN を送信している ProxySG アプライアンスが受信側の ProxySG アプライアンスと同じ ADN の一部であった場合、コア ProxySG アプライアンスが SYN ACK を返します。SYN ACK には、自身を識別する TCP オプション・ヘッダと自身のピア ID が含まれます。エッジ ProxySG アプライアンスは、コア ProxySG アプライアンスの ADN メンバーシップを確認したら、ACK で応答することにより TCP ハンドシェイクを完了します。この時点で、両方のアプライアンスがそれぞれを識別したことになります。ADN トンネルを使用する次のステップは、プロトコル、バイト・キャッシュ辞書、およびその他の情報の交換です。これは、先ほど確立された ADN トンネルを介して行われます。



ADN トンネルの確立および辞書サイズの調整に使用される TCP オプション・フラグは、ADN のピアしか認識できません。何らかの理由で、TCP オプション・ヘッダが含まれるパケットがオリジン・サーバーまたは ADN の一部でないその他のアプライアンスによって受信された場合、それは無視されます。

ブルーコートのアプライアンスの特長

認証済みのセキュアな透過型 ADN トンネル

ブルーコートの透過型 ADN トンネルは、ADN コンテンツにアクセスするための単純かつ拡張可能なメカニズムを提供します。セキュリティ強化のため、Blue Coat ProxySG アプライアンスは、相互認証、および ProxySG アプライアンスがトラフィックの加速化を図るユーザーとサーバーの認証をサポートしています。また、ブルーコートは、SSL を使用してアプライアンス間で通信を暗号化するセキュアな ADN トンネルを提供できる唯一のベンダでもあります。これらの技術を組み合わせることで、ブルーコートは、セキュリティ、可視性、およびパフォーマンスにおける従来のトレードオフを解消するソリューションを提供します。

シンプルな導入

透過型 ADN では、ADN の導入に必要な設定作業を最小限に抑えられる上、現在のネットワーク管理ツールおよびポリシーを使い続けることができます。ADN のネットワーク・トラフィックには可視性があるため、管理者は既存のネットワーク・インフラストラクチャへの影響を最小限に留めながら、ProxySG アプライアンスを導入することができます。これでさらに高速な導入ができるようになり、何百ものアプライアンスの導入を成功させる、重要な要素が手に入ります。