VPN 3000 コンセントレータでの IP セキュリティ用の NAT 透過モードの設定

目次

はじめに

Network Address Translation（NAT; ネットワーク アドレス変換）は、アドレス レンジが不足している Internet Protocol Version 4（IPv4; インターネット プロトコル バージョン 4）の問題を解決するために開発されたものです。 現在、ホーム ユーザおよびスモール オフィスのネットワークでは、登録済アドレスを購入せず、代わりに NAT を使用しています。 企業では、内部リソースを保護するために NAT を単独で、あるいはファイアウォールと組み合わせて実装しています。

、最も一般に設定された NAT ソリューションは多数対 1、1 つの単一ルーティング可能な（パブリック）アドレスへの複数のプライベートアドレスをマップします; これは別名ポート アドレス変換（PAT）です。 この関連付けはポート レベルで実装されています。 PAT ソリューションは、ポートを使用しない IP セキュリティのトラフィックの場合には問題が発生します。

前提条件

要件

このドキュメントに関しては個別の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco VPN 3000 コンセントレータ
- Cisco VPN 3000 クライアント リリース 2.1.3 以降
- NAT-T 用の Cisco VPN 3000 クライアントおよびコンセントレータ リリース 3.6.1 以降

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 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。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

セキュリティ ペイロードのカプセル化

プロトコル 50（Encapsulating Security Payload（ESP））では、暗号化およびカプセル化された IP セキュリティのパケットを処理します。 多くの PAT デバイスは、ESP では動作しません。これは、これらのデバイスが Transmission Control Protocol（TCP; 伝送制御プロトコル）、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）でだけ動作するようにプログラムされているためです。 さらに、PAT デバイスでは、複数の Security Parameter Index（SPI; セキュリティ パラメータ インデックス）をマッピングできません。 VPN 3000 クライアントの NAT 透過モードでは、ESP を UDP 内にカプセル化し、これをネゴシエートしたポートに送ることにより、問題を解決します。 VPN 3000 コンセントレータでアクティブにする属性の名前は、IPSec through NAT です。

また IETF標準（まだ書き込み現在のドラフト ステージでこの技術情報）である新しいプロトコル NAT-T はポート 4500 で UDP の IPsecパケット、それを動作しますカプセル化しますが。 そのポートは設定できません。

NAT 透過モードの仕組み

VPN コンセントレータで IP セキュリティの透過モードをアクティブにすると、外部からは見えないフィルタ ルールが作成され、パブリック フィルタに適用されます。 次に、VPN クライアントが接続するときに、設定されているポート番号が VPN クライアントに透過的に渡されます。着信側では、このポートからの UDP 着信トラフィックが IP セキュリティに直接渡されて処理されます。 トラフィックが復号化され、またカプセル化が解除されて、通常どおりルーティングされます。 発信側では、IP セキュリティによって暗号化、カプセル化が行われ、UDP ヘッダーに適用されます（そのように設定されている場合）。 ランタイムフィルタ規則は 3 つの状態以下の適切なフィルタから無効になり、削除されます: 時 IPSec over UDP がグループのために無効である、グループが削除されるか、またはそのポートの UDP（ユーザ· データグラム· プロトコル）SA 上の最後のアクティブIPSec が削除される時。 非アクティブであることが原因で NAT デバイスがポートのマッピングをクローズしないようにするために、キープアライブが送信されます。

IPSec over NAT-T が VPN コンセントレータでイネーブルになっていると、VPN コンセントレータおよび VPN クライアントでは UDP カプセル化の NAT-T モードを使用します。 NAT-T は、IKE ネゴシエーションの際に VPN クライアントと VPN コンセントレータとの間の NAT デバイスを自動検出することにより動作します。 NAT-T が動作するには、VPN コンセントレータと VPN クライアントの間の UDP ポート 4500 がブロックされていないようにする必要があります。 さらに、すでにそのポートを使用中の以前の IPSec/UDP 設定を使用している場合には、その以前からの IPSec/UDP 設定を別の UDP ポートを使用するよう再設定する必要があります。 NAT-T は IETF の草案であるため、マルチベンダーのデバイスを使用しているときには、他のベンダーがこの規格を採用している場合にだけ機能します。

NAT-T は、IPSec over UDP/TCP とは異なり、VPN クライアント接続と LAN-to-LAN 接続の両方で動作します。 また、NAT-T は Cisco IOS(R) ルータと PIX ファイアウォール デバイスでもサポートされています。

NAT-T を動作させるために IPSec over UDP をイネーブルにする必要はありません。

NAT 透過モードの設定

VPN コンセントレータで NAT 透過モードを設定するには、次の手順に従ってください。

注: IPSec over UDP は、グループを基本として設定しますが、IPSec over TCP/NAT-T はグローバルに設定します。

1. IPSec over UDP の設定VPN コンセントレータで、**Configuration > User Management > Groups** の順に選択します。グループを追加するには、[Add] を選択します。 既存のグループを変更するには、そのグループを選択して、**[Modify]** をクリックします。IPSec タブをクリックして、**IPSec through NAT** をチェックし、**IPSec through NAT UDP Port** を設定します。 IPSec through NAT のデフォルト ポートは 10000 です（発信元および宛先）。しかし、この設定は変更できます。
2. IPSec over NAT-T と IPSec over TCP のいずれかまたは両方の設定は次のように行います。VPN コンセントレータで、**Configuration > System > Tunneling Protocols > IPSec > NAT Transparency** の順に選択します。[IPSec over NAT-T and/or TCP] チェック ボックスをチェックします。

すべてがイネーブルになる場合は、次の優先順位に従ってください。

1. IPSec over TCP
2. IPSec over NAT-T
3. IPSec over UDP

NAT 透過モードを使用するための Cisco VPN クライアントの設定

IPSec over UDP や NAT-T を使用するには、Cisco VPN クライアント 3.6 以降で IPSec over UDP をイネーブルにする必要があります。 IPSec over UDP の場合は VPN コンセントレータによって UDP ポートが割り当てられます。また、NAT-T の場合は UDP ポートが 4500 に固定されます。

IPSec over TCP を使用するには、VPN クライアントでこれをイネーブルにして、使用するポートを手作業で設定する必要があります。

関連情報

- Cisco VPN 3000 シリーズ コンセントレータに関するサポート ページ
- Cisco VPN 3000 シリーズ クライアントに関するサポート ページ
- IPSec に関するサポート ページ
- テクニカルサポート - Cisco Systems