GREを使用したPPTPプロトコルのIOSゾーンベースポリシーファイアウォール検査の問題のトラブルシューティング

内容

概要

このドキュメントでは、ゾーンベースファイアウォール(ZBF)に関して見つかった問題について説明します。この問題から、ZBFがGeneric Routing Encapsulation(GRE)を使用したPoint-to-Point Tunneling Protocol(PPTP)を適切に検査しません。

前提条件

要件

IOSルータでのCisco ZBF設定に関する知識があることが推奨されます。

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いています。

- サービス統合型ルータ(ISR G1)
- IOS 15M&T

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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

PPTPは、仮想プライベートネットワークの実装方法です。PPTPは、TCP上の制御チャネルと、

PPPパケットをカプセル化するために動作するGREトンネルを使用します。

PPTPトンネルは、TCPポート1723でピアに対して開始されます。このTCP接続は、同じピアへの2番目のGREトンネルを開始および管理するために使用されます。

GREトンネルは、カプセル化されたPPPパケットを伝送するために使用され、PPP内で伝送できる任意のプロトコルのトンネルを許可します。 IFには、NetBEUIとIPXが含まれています。

問題：GREを使用したPPTPプロトコルのIOSゾーンベースポリシーファイアウォール検査の問題のトラブルシューティング

ZBFがGREトラフィックを使用したPPTPを検査しないことが確認されています。これは、リターントラフィックの通過に必要なピンホールが開かないためです。次に、GREトラフィックを使用したPPTPプロトコルの検査のための一般的なZBF設定のの例をを示示します。

```
ip access-list extended 160
permit gre any any

class-map type inspect match-all PPTP-GRE
match access-group 160

policy-map type inspect WAN-LAN-pmap
 class class-default
  drop

policy-map type inspect LAN-WAN-pmap
class type inspect PPTP-GRE
  inspect
 class class-default
  drop

zone security LAN
zone security WAN

zone-pair security LAN-WAN source LAN destination WAN
 service-policy type inspect LAN-WAN-pmap
zone-pair security WAN-LAN source WAN destination LAN
 service-policy type inspect WAN-LAN-pmap
```

注：設定例では、PPTP接続がLANからWANゾーンに開始されることを考慮してください。

注：PPTPのTCP接続がZBFの**show policy-firewall sessionsの出力で確立されたとおりに表示される**が、PPTP接続がルータを介して機能しません。

解決方法

ZBFを介してGREとのPPTP VPN接続を許可するには、次のように、関係するゾーンペアのトラフィックフローの両方向のパスアクションに対するZBFルールの**inspectアクションを変更する必要があります**。

```
ip access-list extended 160
permit gre any any
```

```
class-map type inspect match-all PPTP-GRE
match access-group 160

policy-map type inspect WAN-LAN-pmap
class type inspect PPTP-GRE
  pass
 class class-default
 drop

policy-map type inspect LAN-WAN-pmap
class type inspect PPTP-GRE
  pass
 class class-default
 drop

zone security LAN
zone security WAN

zone-pair security LAN-WAN source LAN destination WAN
 service-policy type inspect LAN-WAN-pmap
zone-pair security WAN-LAN source WAN destination LAN
 service-policy type inspect WAN-LAN-pmap
```

このZBF設定変更を適用すると、GREを使用したPPTP VPN接続はZBFを介して正常に動作します。

関連情報

GREおよびEncapsulating Security Payload(ESP)プロトコルトラフィックがゾーンベースポリシーファイアウォールを通過できるようにするには、**passアクション**を使用します。GREおよびESPプロトコルはステートフルインスペクションをサポートしていません。また、ZBFで**inspectアクションを使用する**と、これらのプロトコルのトラフィックはドロップされます。

セキュリティの設定ガイド：ゾーンベース ポリシー ファイアウォール、Cisco IOS リリース 15M&T

関連するバグ

CSCtn52424 ZBF ENH:ダイナミックGREパススルーによるPPTPのインスペクションの実装