# Dépannage des problèmes d'inspection du pare-feu de stratégie basé sur la zone IOS pour le protocole PPTP avec GRE

## Contenu



## Introduction

Ce document décrit un problème trouvé avec le ZBF (Zone-Based Firewall), d'où le ZBF n'inspecte pas correctement le protocole PPTP (Point-to-Point Tunneling Protocol) avec GRE (Generic Routing Encapsulation) .

## Conditions préalables

### Conditions requises

Cisco vous recommande de connaître la configuration ZBF de Cisco dans les routeurs IOS.

### Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeurs à services intégrés (ISR G1)
- IOS 15M&T

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

## Informations générales

Le protocole PPTP est une méthode de mise en oeuvre des réseaux privés virtuels. PPTP utilise

un canal de contrôle sur TCP et un tunnel GRE qui fonctionne pour encapsuler des paquets PPP.

Un tunnel PPTP est initié à l'homologue sur le port TCP 1723. Cette connexion TCP est ensuite utilisée pour initier et gérer un second tunnel GRE vers le même homologue.

Le tunnel GRE est utilisé pour transporter des paquets PPP encapsulés, ce qui permet le tunnel de tout protocole pouvant être transporté dans PPP.  IF, NetBEUI et IPX sont inclus.

# Problème : Dépannage des problèmes d'inspection du pare-feu de stratégie basé sur la zone IOS pour le protocole PPTP avec GRE

Il est confirmé que le ZBF n'inspecte pas le trafic PPTP avec le trafic GRE et ceci parce qu'il n'ouvre pas les trous de broches requis pour permettre le passage du trafic de retour, voici un exemple de configuration ZBF type pour l'inspection du protocole PPTP avec le trafic GRE :

```
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
```

> **Note**: Prenez en compte que dans l'exemple de configuration, la connexion PPTP est initiée du LAN à la zone WAN.

> **Note**: Même si la connexion TCP du protocole PPTP est affichée comme établi dans la sortie **show policy-firewall sessions** du ZBF, la connexion PPTP ne fonctionne pas par le routeur.

# Solution

Afin de permettre les connexions VPN PPTP avec GRE via le ZBF, vous devez modifier l'action **d'inspection** des règles ZBF pour une action **pass** dans les deux directions du flux de trafic dans les zones-paires concernées, comme suit :

```
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
```

Après avoir appliqué cette modification de configuration ZBF, la connexion VPN PPTP avec GRE fonctionnera correctement via ZBF.

## Informations connexes

Pour autoriser le trafic du protocole GRE et ESP (Encapsulating Security Payload) via un pare-feu de stratégie basé sur une zone, utilisez l'action **pass**. Le GRE et les protocoles ESP ne prennent pas en charge l'inspection dynamique et si vous utilisez l'action **inspect** sur ZBF, le trafic pour ces protocoles est abandonné.

Guide de configuration de la sécurité : Pare-feu de stratégie basé sur les zones, Cisco IOS version 15M&T

## Bogue associé

CSCtn52424 ZBF ENH : Mettre en oeuvre l'inspection du protocole PPTP avec le transfert GRE dynamique