Risoluzione dei problemi di ispezione del firewall per i criteri basati sulle zone IOS per il protocollo PPTP con GRE

Sommario

Introduzione

Questo documento descrive un problema rilevato con il ZBF (Zone-Based Firewall), da cui lo ZBF non ispeziona correttamente il PPTP (Point-to-Point Tunneling Protocol) con GRE (Generic Routing Encapsulation).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza della configurazione di Cisco ZBF nei router IOS.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ISR G1 (Integrated Services Router)
- IOS 15M&T

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il PPTP è un metodo di implementazione delle reti private virtuali. Il PPTP utilizza un canale di controllo su TCP e un tunnel GRE che funziona per incapsulare i pacchetti PPP.

Viene avviato un tunnel PPTP verso il peer sulla porta TCP 1723. Questa connessione TCP viene quindi utilizzata per avviare e gestire un secondo tunnel GRE allo stesso peer.

Il tunnel GRE viene usato per trasportare i pacchetti PPP incapsulati, il che permette il tunnel di tutti i protocolli che possono essere trasportati all'interno del protocollo PPP. IF, NetBEUI e IPX sono inclusi.

Problema: Risoluzione dei problemi di ispezione del firewall per i criteri basati sulle zone IOS per il protocollo PPTP con GRE

Si conferma che la ZBF non ispeziona il PPTP con il traffico GRE e questo perché non apre i fori-pin richiesti per consentire il passaggio del traffico di ritorno. Di seguito è riportato un esempio di una tipica configurazione ZBF per l'ispezione del protocollo PPTP con il traffico 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
```

> **Nota:** Tenere presente che nell'esempio di configurazione la connessione PPTP viene avviata dalla LAN alla zona WAN.

> **Nota:** Anche se la connessione TCP del PPTP viene mostrata come stabilita nell'output **show policy-firewall session** dello ZBF, la connessione PPTP non funziona attraverso il router.

Soluzione

Per consentire le connessioni VPN PPTP con GRE attraverso la ZBF, è necessario modificare l'azione **inspect** delle regole ZBF per un'azione **pass** in entrambe le direzioni del flusso di traffico

nelle coppie di zone interessate, nel modo seguente:

```
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
```

Dopo aver applicato questa modifica alla configurazione ZBF, la connessione VPN PPTP con GRE funzionerà correttamente tramite ZBF.

Informazioni correlate

Per consentire il traffico del protocollo GRE ed ESP (Encapsulating Security Payload) attraverso un firewall dei criteri basato su zone, utilizzare l'azione **pass**. I protocolli GRE ed ESP non supportano l'ispezione con conservazione dello stato e se si utilizza l'azione **inspect** sullo ZBF, il traffico per questi protocolli viene interrotto.

Guida alla configurazione della protezione: Policy Firewall basato su zone, Cisco IOS release 15M&T

Bug correlato

CSCtn52424 ZBF ENH: Implementazione dell'ispezione di PPTP con pass-through GRE dinamico