WAAS - Identificação e solução de problemas do WCCP

Capítulo: Troubleshooting de WCCP

Este artigo descreve como solucionar problemas do WCCP.

Co

Art
En
trá
So
Oti
Tro
Tro
Tro
Tro
Tro
Tro
Tro
Tro
So
Tro
Tro
Tro
So
So
So
So
So
Tro

Contents

Os seguintes sintomas indicam possíveis problemas de WCCP:

- O WAE não está recebendo tráfego (pode ser devido a uma configuração incorreta do WCCP)
- Os usuários finais não podem acessar seus aplicativos de servidor (pode ser devido à retenção de tráfego)
- Lentidão da rede quando o WCCP está habilitado (pode ser devido ao descarte de pacotes pelo roteador ou ao alto uso da CPU do roteador)

- Uso muito alto da CPU do roteador (pode ser devido ao redirecionamento no software em vez de no hardware)

Problemas com o WCCP podem resultar de problemas com o roteador (ou do dispositivo de redirecionamento) ou do dispositivo WAE. É necessário examinar a configuração do WCCP no roteador e no dispositivo WAE. Primeiro, examinaremos a configuração do WCCP no roteador e, em seguida, verificaremos a configuração do WCCP no WAE.

Troubleshooting de WCCP no Roteador

Esta seção aborda a solução de problemas nos seguintes dispositivos:

- Switches Catalyst 6500 Series e os roteadores ISR e 3700 Series
- Roteadores ASR 1000 Series

Troubleshooting de WCCP nos Catalyst 6500 Series Switches e nos ISR e 3700 Series Routers

Comece a solução de problemas verificando a interceptação do WCCPv2 no switch ou roteador usando o comando IOS **show ip wccp** da seguinte maneira:

```
Router# show ip wccp
Global WCCP information:
   Router information:
       Router Identifier:                  10.88.81.242
       Protocol Version:                   2.0

   Service Identifier: 61
       Number of Service Group Clients:    1                   <-----Client = WAE
       Number of Service Group Routers:    1
       Total Packets s/w Redirected:       68755               <-----Increments for software-
based redirection
         Process:                          2                   <-----
         Fast:                             0                   <-----
         CEF:                              68753               <-----
       Service mode:                       Open
       Service access-list:                -none-
       Total Packets Dropped Closed:       0
       Redirect access-list:               -none-
       Total Packets Denied Redirect:      0                   <-----Match service group but not
redirect list
       Total Packets Unassigned:           0
       Group access-list:                  -none-
       Total Messages Denied to Group:     0
       Total Authentication failures:      0                   <-----Packets have incorrect
service group password
       Total Bypassed Packets Received:    0
--More--
```

Em plataformas que usam redirecionamento baseado em software, verifique se os contadores Redirecionados do Total Packets s/w estão aumentando na saída do comando acima. Em plataformas que usam redirecionamento baseado em hardware, esses contadores não devem estar aumentando muito. Se você estiver vendo esses contadores incrementarem significativamente em plataformas baseadas em hardware, o WCCP pode ser configurado incorretamente no roteador (o WCCP GRE é processado no software por padrão), ou o roteador pode estar voltando para o redirecionamento de software devido a problemas de recursos de

hardware, como ficar sem recursos de TCAM. É necessária mais investigação se você vir esses contadores incrementando em uma plataforma baseada em hardware, o que pode levar ao alto uso da CPU.

O contador Total de pacotes negados de redirecionamento é incrementado para pacotes que correspondem ao grupo de serviços, mas não correspondem à lista de redirecionamento.

O contador de falhas de autenticação total é incrementado para pacotes recebidos com a senha incorreta do grupo de serviços.

Nos roteadores em que o redirecionamento do WCCP é executado no software, continue verificando a interceptação do WCCPv2 no roteador usando o comando IOS **show ip wcccp 61 detail** da seguinte maneira:

```
Router# show ip wccp 61 detail
WCCP Client information:
       WCCP Client ID:          10.88.81.4
       Protocol Version:        2.0
       State:                   Usable                                  <-----Should be Usable
       Initial Hash Info:       00000000000000000000000000000000
                                00000000000000000000000000000000
       Assigned Hash Info:      FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                                FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
       Hash Allotment:          256 (100.00%)                           <-----Buckets handled by
this WAE
       Packets s/w Redirected:  2452
       Connect Time:            01:19:46                                <-----Time WAE has been
in service group
       Bypassed Packets
         Process:               0
         Fast:                  0
         CEF:                   0
```

Verifique se o estado WAE no grupo de serviços 61 é Usável. Verifique se os hash buckets estão atribuídos ao WAE no campo Hash Allotment. O percentual informa quantos dos hash buckets totais são tratados por este WAE. O tempo que o WAE esteve no grupo de serviços é relatado no campo Tempo de conexão. O método de atribuição de hash deve ser usado com redirecionamento baseado em software.

Você pode determinar qual WAE no farm tratará uma solicitação específica usando o comando IOS oculto **show ip wccp** *service* **hash** *dst-ip src-ip dst-port src-port* no roteador da seguinte maneira:

```
Router# show ip wccp 61 hash 0.0.0.0 10.88.81.10 0 0
WCCP hash information for:
   Primary Hash:   Src IP: 10.88.81.10
   Bucket:   9
   WCCP Client: 10.88.81.12                                  <-----Target WAE
```

Nos roteadores em que o redirecionamento do WCCP é executado no hardware, continue verificando a interceptação do WCCPv2 no roteador usando o comando IOS **show ip wcccp 61 detail** da seguinte maneira:

```
Cat6k# sh ip wccp 61 detail
WCCP Client information:
```

```
   WCCP Client ID:          10.88.80.135
   Protocol Version:        2.0
   State:                   Usable
   Redirection:             L2
   Packet Return:           GRE                    <-----Use generic GRE for hardware-based
platforms
   Packets Redirected:    0
   Connect Time:          1d18h
   Assignment:            MASK                     <-----Use Mask for hardware-based
redirection

   Mask  SrcAddr    DstAddr    SrcPort DstPort
   ----  -------    -------    ------- -------
   0000: 0x00001741 0x00000000 0x0000  0x0000       <-----Default mask

   Value SrcAddr    DstAddr    SrcPort DstPort CE-IP
   ----- -------    -------    ------- ------- -----
   0000: 0x00000000 0x00000000 0x0000  0x0000  0x0A585087 (10.88.80.135)
   0001: 0x00000001 0x00000000 0x0000  0x0000  0x0A585087 (10.88.80.135)
   0002: 0x00000040 0x00000000 0x0000  0x0000  0x0A585087 (10.88.80.135)
   0003: 0x00000041 0x00000000 0x0000  0x0000  0x0A585087 (10.88.80.135)
```

Você deseja ver o método de atribuição de máscara para roteadores que sejam capazes de redirecionamento de hardware.

Para salvar os recursos TCAM no roteador, considere alterar a máscara WCCP padrão para se adequar ao ambiente de rede. Considere estas recomendações:

- Use o menor número possível de bits de máscara ao usar a ACL de redirecionamento WCCP. Um número menor de bits de máscara quando usados em conjunto com a ACL de redirecionamento resulta em menor utilização da TCAM. Se houver 1 a 2 clientes WCCP em um cluster, use um bit. Se houver 3 a 4 clientes WCCP, use 2 bits. Se houver 5 a 8 clientes WCCP, use 3 bits e assim por diante.
- Não recomendamos o uso da máscara padrão WAAS (0x1741). Para implantações de data center, o objetivo é balancear a carga das filiais no data center em vez de nos clientes ou hosts. A máscara certa minimiza o peering do WAE do data center e, portanto, dimensiona o armazenamento. Por exemplo, use 0x100 a 0x7F00 para data centers de varejo que tenham /24 redes de filiais. Para grandes empresas com um /16 por empresa, use 0x10000 a 0x7F0000 para balancear a carga das empresas no data center corporativo. Na filial, o objetivo é equilibrar os clientes que obtêm seus endereços IP via DHCP. O DHCP geralmente emite endereços IP do cliente incrementando do endereço IP mais baixo da sub-rede. Para equilibrar melhor os endereços IP atribuídos por DHCP com a máscara, use 0x1 a 0x7F para considerar somente os bits de ordem mais baixa do endereço IP do cliente para alcançar a melhor distribuição.

Os recursos TCAM consumidos por uma lista de acesso de redirecionamento WCCP são um produto do conteúdo dessa ACL multiplicado em relação à máscara de bit WCCP configurada. Portanto, há contenção entre o número de buckets WCCP (que são criados com base na máscara) e o número de entradas na ACL de redirecionamento. Por exemplo, uma máscara de 0xF (4 bits) e uma ACL de permissão de redirecionamento de 200 linhas podem resultar em 3200 (2^4 x 200) entradas de TCAM. A redução da máscara para 0x7 (3 bits) reduz o uso da TCAM em 50% (2^3 x 200 = 1600).

As plataformas da série Catalyst 6500 e da série Cisco 7600 são capazes de lidar com o redirecionamento de WCCP no software e no hardware. Se os pacotes estiverem sendo inadvertidamente redirecionados no software, quando você espera redirecionamento de

hardware, isso pode resultar em uso de CPU de roteador muito alto.

Você pode inspecionar as informações do TCAM para determinar se o redirecionamento está sendo tratado no software ou no hardware. Use o comando IOS **show tcam** da seguinte maneira:

```
Cat6k# show tcam interface vlan 900 acl in ip

* Global Defaults not shared


Entries from Bank 0


Entries from Bank 1

    permit       tcp host 10.88.80.135 any
    punt         ip any any (8 matches)              <-----Packets handled in software
```

As correspondências de "busca" representam solicitações não tratadas no hardware. Essa situação pode ser causada pelos seguintes erros:

- Atribuição de hash em vez de máscara
- Redirecionamento de saída em vez de entrada
- Redirecionar exclusão em
- Endereço MAC WAE desconhecido
- Usando um endereço de loopback para o destino genérico do túnel GRE

No exemplo a seguir, as entradas de rota de política mostram que o roteador está fazendo o redirecionamento completo de hardware:

```
Cat6k# show tcam interface vlan 900 acl in ip

* Global Defaults not shared


Entries from Bank 0


Entries from Bank 1

   permit       tcp host 10.88.80.135 any
   policy-route tcp any 0.0.0.0 255.255.232.190 (60 matches)         <-----These entries show
hardware redirection
   policy-route tcp any 0.0.0.1 255.255.232.190 (8 matches)
   policy-route tcp any 0.0.0.64 255.255.232.190 (16 matches)
   policy-route tcp any 0.0.0.65 255.255.232.190 (19 matches)
   policy-route tcp any 0.0.1.0 255.255.232.190
   policy-route tcp any 0.0.1.1 255.255.232.190
   policy-route tcp any 0.0.1.64 255.255.232.190
   policy-route tcp any 0.0.1.65 255.255.232.190
   policy-route tcp any 0.0.2.0 255.255.232.190
   policy-route tcp any 0.0.2.1 255.255.232.190
   policy-route tcp any 0.0.2.64 255.255.232.190
   policy-route tcp any 0.0.2.65 255.255.232.190 (75 matches)
   policy-route tcp any 0.0.3.0 255.255.232.190 (222195 matches)
```

O HIA (Here I Am) do WAE deve inserir a mesma interface pela qual o MAC do WAE é conhecido. Recomendamos que você use uma interface de loopback e não uma interface

diretamente conectada na lista de roteadores WAE.

Troubleshooting de WCCP nos ASR 1000 Series Routers

Os comandos para solucionar problemas do WCCP nos roteadores Cisco ASR 1000 Series são diferentes dos outros roteadores. Esta seção mostra os comandos que você pode usar para obter informações de WCCP no ASR 1000.

Para exibir informações do WCCP do processador de rota, use os comandos **show platform software wccp rp ative** da seguinte maneira:

```
ASR1000# sh platform software wccp rp active
Dynamic service 61
Priority: 34, Number of clients: 1                          <-----Number of WAE clients
Assign Method: Mask, Fwd Method: GRE, Ret Method: GRE       <-----Assignment, forwarding, and
return methods
L4 proto: 6, Use Source Port: No, Is closed: No
Dynamic service 62
Priority: 34, Number of clients: 1                          <-----
Assign Method: Mask, Fwd Method: GRE, Ret Method: GRE       <-----
L4 proto: 6, Use Source Port: No, Is closed: No
```

O exemplo a seguir mostra comandos adicionais que você pode usar para examinar informações do processador de encaminhamento:

```
ASR1000# sh platform software wccp fp active ?
  <0-255>     service ID
  cache-info  Show cache-engine info
  interface   Show interface info
  statistics  Show messaging statistics
  web-cache   Web-cache type
  |           Output modifiers
  <cr>
```

Para exibir estatísticas de pacotes redirecionados para cada interface, use o comando **show platform software wccp interface counters** da seguinte maneira:

```
ASR1000# sh platform software wccp interface counters
Interface GigabitEthernet0/1/2
       Input Redirect Packets  = 391
       Output Redirect Packets  = 0
Interface GigabitEthernet0/1/3
       Input Redirect Packets  = 1800
       Output Redirect Packets  = 0
```

Use o comando **show platform software wccp web-cache counters** para exibir informações do cache WCCP da seguinte maneira:

```
ASR1000# sh platform software wccp web-cache counters
Service Group (0, 0) counters
       unassigned_count = 0
       dropped_closed_count = 0
       bypass_count = 0
       bypass_failed_count = 0
```

```
        denied_count = 0
        redirect_count = 0
```

Para exibir detalhes de baixo nível, use os seguintes comandos:

- **show platform so interface F0 brief**
- **show platform software wccp f0 interface**
- **debug platform software wccp configuration**

Para obter mais informações, consulte o white paper "Deploying and Troubleshooting Web Cache Control Protocol Version 2 on Cisco ASR 1000 Series Aggregation Services Routers" (Implantação e solução de problemas do protocolo de controle de cache da Web versão 2 nos roteadores de serviços de agregação Cisco ASR 1000 Series)

Troubleshooting de WCCP no WAE

Comece a solução de problemas no WAE usando o comando **show wccp services**. Você deseja ver os serviços 61 e 62 configurados, da seguinte forma:

```
WAE-612# show wccp services
Services configured on this File Engine
        TCP Promiscuous 61
        TCP Promiscuous 62
```

Em seguida, verifique o status do WCCP usando o comando **show wccp status**. Você deseja ver que o WCCP versão 2 está ativado e ativo da seguinte forma:

```
WAE-612# show wccp status
WCCP version 2 is enabled and currently active
```

Examine as informações do farm do WCCP usando o comando **show wccp wide-area-engine**. Esse comando mostra o número de WAEs no farm, seus endereços IP, um dos quais é o WAE principal, roteadores que podem ver os WAEs e outras informações, da seguinte forma:

```
WAE612# show wccp wide-area-engine
Wide Area Engine List for Service: TCP Promiscuous 61

Number of WAE's in the Cache farm: 3
Last Received Assignment Key IP address: 10.43.140.162     <-----All WAEs in farm should have
same Key IP
Last Received Assignment Key Change Number: 17
Last WAE Change Number: 16
Assignment Made Flag = FALSE

        IP address = 10.43.140.162       Lead WAE = YES  Weight = 0
        Routers seeing this Wide Area Engine(3)
                10.43.140.161
                10.43.140.166
                10.43.140.168

        IP address = 10.43.140.163       Lead WAE = NO  Weight = 0
        Routers seeing this Wide Area Engine(3)
                10.43.140.161
                10.43.140.166
```

```
               10.43.140.168

       IP address = 10.43.140.164       Lead WAE = NO  Weight = 0
       Routers seeing this Wide Area Engine(3)
               10.43.140.161
               10.43.140.166
               10.43.140.168
. . .
```

Examine as informações do roteador usando o comando **show wccp routers**. Verifique se há comunicação bidirecional com roteadores habilitados para WCCP e se todos os roteadores mostram a mesma KeyIP e KeyCN (número de alteração), como a seguir:

```
WAE-612# show wccp routers

Router Information for Service: TCP Promiscuous 61
       Routers Seeing this Wide Area Engine(1)
       Router Id       Sent To         Recv ID     KeyIP        KeyCN  MCN
       10.43.140.161   10.43.140.161   00203A21    10.43.140.162  17    52   <-----Verify
routers have same KeyIP and KeyCN
       10.43.140.166   10.43.140.166   00203A23    10.43.140.162  17    53
       10.43.140.168   10.43.140.165   00203A2D    10.43.140.162  17    25
       Routers not Seeing this Wide Area Engine
               -NONE-
       Routers Notified of from other WAE's
               -NONE-
       Multicast Addresses Configured
               -NONE-
. . .
```

Nos casos em que o WAE não é a camada 2 adjacente ao roteador, ou um endereço de loopback é usado, é necessário usar rotas estáticas ou um gateway padrão para suportar o WCCP.

Para examinar a distribuição do bucket de hash no grupo de serviços, use o comando **show wccp flows tcp-promíscuo** da seguinte maneira:

```
wae# sh wccp flows tcp-promiscuous
Flow counts for service: TCP Promiscuous 61
Bucket                              Flow Counts
  0- 11:     0     0     0     0     0     0     0     0     0     0     0     0
 12- 23:     0     0     0     0     0     0     0     0     0     0     0     0
 24- 35:     0     0     0     0     0     0     0     0     0     0     0     0
 36- 47:     0     0     0     0     0     0     0     0     0     0     0     0
 48- 59:     0     0     0     0     0     0     0     0     0     0     0     0
 60- 71:     0     0     0     0     0     0     0     0     0     0     0     0
 72- 83:     0     0     0     0     0     0     0     0     0     0     0     0
 84- 95:     0     0     0     0     0     0     0     0     0     0     0     0
 96-107:     0     0     0     0     0     0     0     0     0     0     0     0
108-119:     0     0     0     0     0     0     0     0     0     0     0     0
120-131:     0     0     0     0     0     0     0     0     0     0     0     0
132-143:     0     0     0     0     0     0     0     0     0     0     0     0
144-155:     0     0     0     0     0     0     0     0     0     0     0     0
156-167:     0     0     0     0     0     0     0     0     0     0     0     0
168-179:     0     0     0     0     0     0     0     0     0     0     0     0
180-191:     0     0     0     0     0     0     0     0     0     0     0     0
192-203:     0     0     0     0     0     0     0     0     0     0     0     0
204-215:     0     0     0     0     0     0     0     0     0     0     0     0
216-227:     0     0     0     0     0     0     0     0     0     0     0     0
228-239:     0     0     0     0     0     0     0     0     0     3     0     0
```

```
240-251:     0     0     0     0     0     0     0     0     0     0     0     0
252-255:     0     0     0     0
```

Como alternativa, você pode usar a versão resumida do comando para ver informações semelhantes, bem como informações de fluxo de desvio:

```
wae# sh wccp flows tcp-promiscuous summary
Flow summary for service: TCP Promiscuous 61
Total Buckets
OURS = 256

  0- 59: 0000000000 0000000000 0000000000 0000000000 0000000000 0000000000
 60-119: 0000000000 0000000000 0000000000 0000000000 0000000000 0000000000
120-179: 0000000000 0000000000 0000000000 0000000000 0000000000 0000000000
180-239: 0000000000 0000000000 0000000000 0000000000 0000000000 0000000000
240-255: 0000000000 000000

BYP  = 0

  0- 59: .......... .......... .......... .......... .......... ..........
 60-119: .......... .......... .......... .......... .......... ..........
120-179: .......... .......... .......... .......... .......... ..........
180-239: .......... .......... .......... .......... .......... ..........
240-255: .......... ......

AWAY = 0

  0- 59: .......... .......... .......... .......... .......... ..........
 60-119: .......... .......... .......... .......... .......... ..........
120-179: .......... .......... .......... .......... .......... ..........
180-239: .......... .......... .......... .......... .......... ..........
240-255: .......... ......
. . .
```

Use o comando **show wccp gre** para exibir estatísticas de pacotes GRE da seguinte maneira:

```
WAE-612# show wccp gre
Transparent GRE packets received:              5531561         <-----Increments for WCCP GRE
redirection
Transparent non-GRE packets received:          0               <-----Increments for WCCP L2
redirection
Transparent non-GRE non-WCCP packets received: 0               <-----Increments for ACE or PBR
redirection
Total packets accepted:                        5051            <-----Accepted for optimization;
peer WAE found
Invalid packets received:                      0
Packets received with invalid service:         0
Packets received on a disabled service:        0
Packets received too small:                    0
Packets dropped due to zero TTL:               0
Packets dropped due to bad buckets:            0
Packets dropped due to no redirect address:    0
Packets dropped due to loopback redirect:      0
Pass-through pkts dropped on assignment update:0
Connections bypassed due to load:              0
Packets sent back to router:                   0
GRE packets sent to router (not bypass)        0               <-----Handled with WCCP
negotiated return egress
Packets sent to another WAE:                   0
GRE fragments redirected:                      0
```

```
GRE encapsulated fragments received:           0
Packets failed encapsulated reassembly:        0
Packets failed GRE encapsulation:              0
--More--
```

Se o redirecionamento de WCCP estiver funcionando, qualquer um dos dois primeiros contadores deve estar aumentando.

Os pacotes não-GRE transparentes receberam incrementos de contador para os pacotes que são redirecionados usando o método de encaminhamento de redirecionamento de Camada 2 do WCCP.

Os pacotes não-WCCP transparentes de GRE receberam incrementos de contador para pacotes que são redirecionados por um método de interceptação não-WCCP (como ACE ou PBR).

O contador Total de pacotes aceitos indica os pacotes aceitos para otimização porque a descoberta automática encontrou um WAE par.

Os pacotes GRE enviados ao contador do roteador (não desvio) indicam os pacotes que foram tratados usando o método de saída de retorno negociado do WCCP.

Os pacotes enviados para outro contador WAE indicam que a proteção de fluxo está ocorrendo quando outro WAE é adicionado ao grupo de serviços e começa a lidar com uma atribuição de bucket que estava sendo tratada anteriormente por outro WAE.

Verifique se os métodos de saída que estão sendo usados são os esperados usando o comando **show egress-methods** da seguinte maneira:

```
WAE674# show egress-methods

Intercept method : WCCP

 TCP Promiscuous 61 :
     WCCP negotiated return method : WCCP GRE

                       Egress Method      Egress Method
     Destination        Configured           Used
     -----------  ----------------------  -------------
     any          WCCP Negotiated Return  WCCP GRE               <-----Verify these are
expected

 TCP Promiscuous 62 :
     WCCP negotiated return method : WCCP GRE

                       Egress Method      Egress Method
     Destination        Configured           Used
     -----------  ----------------------  -------------
     any          WCCP Negotiated Return  WCCP GRE               <-----Verify these are
expected
```

As incompatibilidades do método de saída podem ocorrer nas seguintes condições:

- O método de saída de retorno negociado está configurado, mas o WCCP negocia o método de retorno da Camada 2 e apenas a devolução do GRE é suportada pelo WAAS.
- O método de saída GRE genérico está configurado, mas o método de interceptação é Camada 2 e somente o GRE WCCP é suportado como o método de interceptação quando a

saída GRE genérica está configurada.

Em qualquer um desses casos, um alarme secundário é acionado e cancelado quando a incompatibilidade é resolvida alterando o método de saída ou a configuração do WCCP. Até que o alarme seja cancelado, o método de saída de encaminhamento IP padrão é usado.

O exemplo a seguir mostra a saída do comando quando existe uma incompatibilidade:

```
WAE612# show egress-methods
Intercept method : WCCP
 TCP Promiscuous 61 :
     WCCP negotiated return method : WCCP GRE

                      Egress Method      Egress Method
     Destination       Configured           Used
     -----------  ---------------------  -------------
     any          Generic GRE            IP Forwarding                    <-----Mismatch

     WARNING:  WCCP has negotiated WCCP L2 as the intercept method for     <-----Warning if
mismatch occurs
               which generic GRE is not supported as an egress method
               in this release. This device uses IP forwarding as the
               egress method instead of the configured generic GRE
               egress method.
 TCP Promiscuous 62 :

     WCCP negotiated return method : WCCP GRE
                      Egress Method      Egress Method
     Destination       Configured           Used
     -----------  ---------------------  -------------
     any          Generic GRE            IP Forwarding                    <-----Mismatch

     WARNING:  WCCP has negotiated WCCP L2 as the intercept method for     <-----Warning if
mismatch occurs
               which generic GRE is not supported as an egress method
               in this release. This device uses IP forwarding as the
               egress method instead of the configured generic GRE
               egress method.
```

Para os roteadores Catalyst 6500 Sup720 ou Sup32, recomendamos o uso do método genérico de saída GRE, que é processado em hardware. Além disso, recomendamos usar um túnel multiponto para facilitar a configuração, em vez de um túnel ponto a ponto para cada WAE. Para obter detalhes sobre a configuração do túnel, consulte a seção Configurando uma Interface de Túnel GRE em um Roteador no *Guia de Configuração do Cisco Wide Area Application Services*.

Para exibir as estatísticas do túnel GRE para cada roteador de interceptação, use o comando **show statistics generic-gre** da seguinte maneira:

```
WAE# sh stat generic
Tunnel Destination:                          10.10.14.16
Tunnel Peer Status:                          N/A
Tunnel Reference Count:                      2
Packets dropped due to failed encapsulation:  0
Packets dropped due to no route found:        0
Packets sent:                                 0
Packets sent to tunnel interface that is down: 0
Packets fragmented:                           0
```

A falha em garantir que os pacotes de saída de um WAE não sejam reinterceptados pode levar a um loop de redirecionamento. Se um WAE detectar seu próprio ID retornado no campo de opções de TCP, um loop de redirecionamento ocorreu e resulta na seguinte mensagem de syslog:

```
%WAAS-SYS-3-900000: 137.34.79.11:1192 - 137.34.77.196:139 - opt_syn_rcv: Routing Loop detected -
Packet has our own devid. Packet dropped.
```

Você pode pesquisar no arquivo syslog.txt instâncias deste erro usando o comando **find** da seguinte maneira:

```
WAE-612# find match “Routing Loop” syslog.txt
```

Esse erro também é exibido nas estatísticas de fluxo de TFO disponíveis no comando **show statistics filtering** da seguinte maneira:

```
WAE-612# show statistics filtering
. . .
Syn packets dropped with our own id in the options:   8         <-----Indicates a redirection
loop
. . .
```

Se você estiver fazendo o redirecionamento de saída no roteador, à medida que o tráfego sai do roteador, ele será redirecionado de volta para o WAE, que redirecionará o pacote para fora do roteador, causando um loop de roteamento. Se o WAE e os servidores do data center estiverem em VLANs diferentes e o WAE da filial e os clientes estiverem em VLANS diferentes, você poderá evitar um loop de roteamento usando a seguinte configuração de roteador na VLAN WAE:

```
ip wccp redirect exclude in
```

Se o WAE compartilha a mesma VLAN com seus clientes ou servidores adjacentes, você pode evitar loops de roteamento usando o método de devolução negociado ou retorno GRE genérico para plataformas onde o redirecionamento WCCP é executado no hardware. Ao usar a devolução GRE genérica, o WAE usa um túnel GRE para devolver o tráfego ao roteador.

Troubleshooting de IDs de Serviço Configuráveis e Timeouts de Variável na Versão 4.4.1

NOTE: As IDs de serviço configuráveis do WCCP e os recursos de tempo limite de detecção de falha variável foram introduzidos no WAAS versão 4.4.1. Esta seção não se aplica a versões anteriores do WAAS.

Todos os WAEs em um farm WCCP devem usar o mesmo par de IDs de serviço WCCP (o padrão é 61 e 62), e esses IDs devem corresponder a todos os roteadores que estão suportando o farm. Um WAE com IDs de serviço WCCP diferentes daqueles configurados nos roteadores não tem permissão para ingressar no farm e o alarme "Router Unreachable" existente é ativado. Da mesma forma, todos os WAEs em um farm devem usar o mesmo valor para o tempo limite de detecção de falha. Um WAE gera um alarme se você configurá-lo com um valor incompatível.

Se você vir um alarme de que um WAE não pode ingressar em um farm de WCCP, verifique se as IDs de serviço do WCCP configuradas no WAE e os roteadores no farm correspondem. Nos

WAEs, use o **comando show wccp wide-area-engine** para verificar as IDs de serviço configuradas. Nos roteadores, você pode usar o comando IOS **show ip wccp**.

Para verificar se o WAE tem conectividade com o roteador, use os comandos **show wccp services detail** e **show wccp router detail**.

Além disso, você pode habilitar a saída de depuração do WCCP no WAE usando os comandos **debug ip wccp event** ou **debug ip wccp packet**.

Se você vir um alarme secundário "Roteador inutilizável" para um WAE, isso pode significar que o valor de tempo limite de detecção de falha variável definido no WAE não é suportado pelo roteador. Use o comando **show alarm minor detail** para verificar se o motivo do alarme é "Intervalo de temporizador incompatível com o roteador":

```
WAE# show alarm minor detail

Minor Alarms:
-------------
       Alarm ID                 Module/Submodule               Instance
  ---------------             --------------------          ---------------
  1 rtr_unusable              WCCP/svc051/rtr2.192.9.161

    Jan 11 23:18:41.885 UTC, Communication Alarm, #000005, 17000:17003
    WCCP router 2.192.9.161 unusable for service id: 51 reason: Timer interval       <-----Check
reason
mismatch with router                                                                 <-----
```

No WAE, verifique o tempo limite de detecção de falha configurado da seguinte maneira:

```
WAE# show wccp services detail

Service Details for TCP Promiscuous 61 Service
       Service Enabled                    : Yes
       Service Priority                   : 34
       Service Protocol                   : 6
       Application                        : Unknown
       Service Flags (in Hex)             : 501
       Service Ports                      :      0     0     0     0
                                          :      0     0     0     0
       Security Enabled for Service       : No
       Multicast Enabled for Service      : No
       Weight for this Web-CE             : 1
       Negotiated forwarding method       : GRE
       Negotiated assignment method       : HASH
       Negotiated return method           : GRE
       Negotiated HIA interval            : 2 second(s)
       Negotiated failure-detection timeout  : 30 second(s)          <-----Failure detection
timeout configured
. . .
```

No roteador, verifique se a versão do IOS suporta o timeout de detecção de falha variável. Em caso afirmativo, você pode verificar a configuração usando o comando **show ip wccp *xx* detail**, onde *xx* é a ID do serviço WCCP. Há três resultados possíveis:

- O WAE está usando o tempo limite de detecção de falha padrão de 30 segundos e o roteador está configurado da mesma forma ou não suporta o tempo limite variável: A saída do roteador não mostra detalhes sobre a configuração de tempo limite. Essa configuração funciona bem.

- O WAE está usando o tempo limite de detecção de falha não padrão de 9 ou 15 segundos e o roteador não suporta o tempo limite variável: O campo State mostra "NOT Usable" e o WAE não pode usar o roteador. Altere o tempo limite de detecção de falha do WAE para o valor padrão de 30 segundos usando o comando de configuração global **wccp tcp failure-detection 30**.
- O WAE está usando o tempo limite de detecção de falha não padrão de 9 ou 15 segundos e o roteador suporta o tempo limite variável: O campo de tempo limite do cliente mostra o tempo limite de detecção de falha configurado, que corresponde ao WAE. Essa configuração funciona bem.

Se o farm do WCCP estiver instável devido à oscilação do link, pode ser porque o tempo limite de detecção de falha do WCCP é muito baixo.