Guia de solução de problemas de configuração do ZBFW para IOS-XE

Contents

Introduction

Este documento descreve como melhor solucionar problemas do recurso Zone Based Firewall (ZBFW) no Aggregation Services Router (ASR) 1000, com comandos usados para pesquisar os contadores de queda de hardware no ASR. O ASR1000 é uma plataforma de encaminhamento baseada em hardware. A configuração de software do Cisco IOS-XE® programa ASICs de hardware (Quantum Flow Processor - QFP) para executar funcionalidades de encaminhamento de recursos. Isso permite maior throughput e melhor desempenho. A desvantagem é que ele apresenta um desafio maior para solucionar problemas. Os comandos tradicionais do Cisco IOS usados para pesquisar sessões atuais e contadores de queda por meio do Zone-Based Firewall (ZBFW) não são mais válidos, pois as quedas não estão mais no software.

Links e documentação

Referências de comando

- Referências de comandos dos roteadores de serviços de agregação Cisco ASR 1000 Series
- Referências de comandos do Cisco IOS XE 3S

Etapas de Solução de Problemas de Datapth

Para identificar e solucionar problemas de dados, você deve identificar se o tráfego é transmitido corretamente pelo código ASR e Cisco IOS-XE. Especificamente para recursos de firewall, a solução de problemas de dados segue estas etapas:

1. **Verify Configuration** - (Verificar configuração) **Reúna** a configuração e examine a saída para verificar a conexão.

2. **Verify Connection State** - Se o tráfego passar corretamente, o Cisco IOS-XE abre uma conexão no recurso ZBFW. Essa conexão rastreia o tráfego e as informações de estado entre um cliente e um servidor.

3. **Verify Drop Counters** - Quando o tráfego não passa corretamente, o Cisco IOS-XE registra um contador de queda para todos os pacotes descartados. Verifique essa saída para isolar a causa da falha de tráfego.

4. **Registro** - Reúna syslogs para fornecer informações mais granulares sobre compilações de conexão e descartes de pacote.

5. **Packet Trace Dropped Packets** - Use o rastreamento de pacotes para capturar pacotes descartados.

6. **Depurações** - Coletar depurações é a opção mais detalhada. As depurações podem ser obtidas condicionalmente para confirmar o caminho exato de encaminhamento dos pacotes.

Verifique a configuração

A saída do **show tech support firewall** está resumida aqui:

```
-------- show clock --------
-------- show version -------
-------- show running-config --------
-------- show parameter-map type inspect --------
-------- show policy-map type inspect -------
-------- show class-map type inspect --------
-------- show zone security --------
-------- show zone-pair security --------
-------- show policy-firewall stats global --------
-------- show policy-firewall stats zone --------
-------- show platform hardware qfp active feature firewall datapath <submode> --------
-------- show platform software firewall RP <submode> --------
```

Verificar o estado da conexão

As informações de conexão podem ser obtidas para que todas as conexões em ZBFW sejam listadas. Digite este comando:

```
ASR#show policy-firewall sessions platform
--show platform hardware qfp active feature firewall datapath scb any any any any any all any --
[s=session  i=imprecise channel  c=control channel  d=data channel]
 14.38.112.250 41392 14.36.1.206 23 proto 6 (0:0)    [sc]
```

Ele mostra uma conexão telnet TCP de 14.38.112.250 a 14.36.1.206.

> **Note**: Lembre-se de que se você executar esse comando, levará muito tempo se houver muitas conexões no dispositivo. A Cisco recomenda que você execute esse comando com filtros específicos conforme descrito aqui.

A tabela de conexão pode ser filtrada para um endereço de origem ou de destino específico. Usar filtros após o submodo **da plataforma**. As opções a filtrar são:

```
radar-ZBFW1#show policy-firewall sessions platform ?
 all                     detailed information
 destination-port        Destination Port Number
 detail                  detail on or off
 icmp                    Protocol Type ICMP
 imprecise               imprecise information
 session                 session information
 source-port             Source Port
 source-vrf              Source Vrf ID
 standby                 standby information
 tcp                     Protocol Type TCP
 udp                     Protocol Type UDP
 v4-destination-address  IPv4 Desination Address
 v4-source-address       IPv4 Source Address
 v6-destination-address  IPv6 Desination Address
 v6-source-address       IPv6 Source Address
 |                       Output modifiers
 <cr>
```

Esta tabela de conexão é filtrada de modo que somente conexões originadas de 14.38.112.250 sejam exibidas:

```
ASR#show policy-firewall sessions platform v4-source-address 14.38.112.250
--show platform hardware qfp active feature firewall datapath scb 14.38.112.250
any any any any all any --
[s=session  i=imprecise channel  c=control channel  d=data channel]
 14.38.112.250 41392 14.36.1.206 23 proto 6 (0:0)    [sc]
```

Depois que a tabela de conexão é filtrada, as informações detalhadas da conexão podem ser obtidas para uma análise mais abrangente. Para exibir essa saída, use a palavra-chave **detail**.

```
ASR#show policy-firewall sessions platform v4-source-address 14.38.112.250 detail
--show platform hardware qfp active feature firewall datapath scb 14.38.112.250
any any any any all any detail--
[s=session  i=imprecise channel  c=control channel  d=data channel]
 14.38.112.250 41426 14.36.1.206 23 proto 6 (0:0)       [sc]
 pscb : 0x8c5d4f20,  bucket : 64672, fw_flags: 0x204 0x20419441,
       scb state: active, scb debug: 0
 nxt_timeout: 360000, refcnt: 1,  ha nak cnt: 0,  rg: 0, sess id: 117753
 hostdb: 0x0, L7: 0x0, stats: 0x8e118e40, child: 0x0
```

```
l4blk0: 78fae7a7 l4blk1: e36df99c l4blk2: 78fae7ea l4blk3: 39080000
l4blk4: e36df90e l4blk5: 78fae7ea l4blk6: e36df99c l4blk7: fde0000
l4blk8: 0 l4blk9: 1
root scb: 0x0 act_blk: 0x8e1115e0
ingress/egress intf: GigabitEthernet0/0/2 (1021), GigabitEthernet0/0/0 (131065)
current time 34004163065573 create tstamp: 33985412599209 last access: 33998256774622
nat_out_local_addr:port: 0.0.0.0:0 nat_in_global_addr:port: 0.0.0.0:0
syncookie fixup: 0x0
halfopen linkage: 0x0 0x0
cxsc_cft_fid: 0x0
tw timer: 0x0 0x0 0x372ba 0x1e89c181
Number of simultaneous packet per session allowed: 25
  bucket 125084 flags 1 func 1 idx 8 wheel 0x8ceb1120
```

Verificar contadores de queda do firewall

A saída do contador de queda mudou durante XE 3.9. Antes do XE 3.9, os motivos da queda do firewall eram muito genéricos. Depois do XE 3.9, os motivos da queda do firewall foram estendidos para se tornarem mais granulares.

Para verificar os contadores de queda, execute duas etapas:

1. Confirme os contadores de queda global no Cisco IOS-XE. Esses contadores mostram qual recurso derrubou o tráfego. Exemplos de recursos incluem Qualidade de Serviço (QoS - Quality of Service), Conversão de Endereço de Rede (NAT - Network Address Translation), Firewall e assim por diante.

2. Depois que o subrecurso tiver sido identificado, consulte os contadores de queda granular oferecidos pelo subrecurso. Neste guia, o subrecurso que está sendo analisado é o recurso Firewall.

Contadores globais de queda no QFP

O comando básico no qual confiar fornece todas as gotas no QFP:

```
Router#show platform hardware qfp active statistics drop
```

Esse comando mostra as quedas genéricas globalmente no QFP. Essas quedas podem estar em qualquer recurso. Alguns recursos de exemplo são:

```
Ipv4Acl
Ipv4NoRoute
Ipv6Acl
Ipv6NoRoute
NatIn2out
VfrErr
...etc
```

Para ver todas as quedas, inclua contadores que tenham um valor zero, use o comando:

```
show platform hardware qfp active statistics drop all
```

Para limpar os contadores, use este comando. Limpa a saída depois de mostrá-la à tela. Este comando está claro na leitura, portanto a saída é redefinida para zero **depois** de ser exibida na

tela.

```
show platform hardware qfp active statistics drop clear
```

Veja abaixo uma lista de contadores de queda de firewall global QFP e uma explicação:

Motivo da queda global do firewall	Explicação
FirewallPressãoAnterior	A queda do pacote devido à pressão contrária pelo mecanismo de registro.
FirewallZonaInválida	Nenhuma zona de segurança configurada para a interface.
FirewallL4Insp	Falha na verificação da política L4. Consulte a tabela abaixo para obter mais motivos granulares para soltar (motivos para queda do recurso Firewall).
FirewallNoForwardingZone	O firewall não foi inicializado e nenhum tráfego tem permissão para passar.
FirewallNão-sessão	Falha na criação da sessão. Isso pode ser devido ao limite máximo de sessã atingido ou a falha de alocação de memória.
PolíticaFirewall	A política de firewall configurada é solta.
FirewallL4	Falha na inspeção de L4. Consulte a tabela abaixo para obter mais detalhes sobre os motivos da queda do recurso de firewall.
FirewallL7	Queda de pacote devido à inspeção L7. Veja abaixo uma lista de motivos ma granulares de queda de L7 (motivos para queda do recurso Firewall).
FirewallNotInitiator	Não é um iniciador de sessão para TCP, UDP ou ICMP. Nenhuma sessão é criada. Por exemplo, para o ICMP, o primeiro pacote recebido não é ECHO o TIMESTAMP. Para o TCP, não é um SYN. Isso pode acontecer no processamento normal de pacotes ou no processamento impreciso de canais.
FirewallSemNovaSessão	A alta disponibilidade do firewall não permite novas sessões.
FirewallSyncookieMaxDst	Para fornecer proteção de inundação SYN baseada em host, há uma taxa SY por destino como limite de inundação SYN. Quando o número de entradas de destino atinge o limite, novos pacotes SYN são descartados.
FirewallSyncookie	A lógica SYNCOOLIE é acionada. Indica que SYN/ACK com cookie SYN foi enviado e o pacote SYN original foi descartado.
FirewallARStandby	O roteamento assimétrico não está ativado e o grupo de redundância não es no estado ativo.

Contadores de queda de recursos do firewall no QFP

A limitação com o contador de queda global do QFP é que não há granularidade nos motivos da queda, e alguns dos motivos da queda, como **FirewallL4,** ficam tão sobrecarregados a ponto de ser de pouca utilidade para a solução de problemas. Isso foi aprimorado desde então no Cisco IOS-XE 3.9 (15.3(2)S), onde os contadores de queda do recurso Firewall foram adicionados. Isso oferece um conjunto muito mais granular de motivos de queda:

```
ASR#show platform hardware qfp active feature firewall drop all
-----------------------------------------------------------------------------
Drop Reason Packets
-----------------------------------------------------------------------------
Invalid L4 header 0
Invalid ACK flag 0
Invalid ACK number 0
....
```

Abaixo está uma lista dos motivos e explicações da queda do recurso de firewall:

Motivo da queda do recurso de firewall	Explicação
Tamanho do cabeçalho inválido	O datagrama é tão pequeno que não pode conter o cabeçalho da camada 4TCP, U ou ICMP. Ela pode ser causada por: 1. Comprimento do cabeçalho TCP < 20 2. Comprimento do cabeçalho UDP/ICMP < 8
Comprimento de dados UDP inválido	O comprimento do datagrama UDP não corresponde ao comprimento especificado cabeçalho UDP.
Número ACK inválido	Essa queda pode ser causada por um destes motivos: 1. ACK não é igual ao next_seq# do peer TCP. 2. ACK é maior que o SEQ# mais recente enviado pelo peer TCP. No estado TCP SYNSENT e SYNRCVD, é esperado que ACK# seja igual a ISN+1, não é.
Sinalizador ACK inválido	Essa queda pode ser causada por um destes motivos: 1. Sinalizador ACK esperado, mas não definido em estado TCP diferente. 2. Além do sinalizador ACK, outro sinalizador (como o RST) também está definic
Iniciador TCP inválido	Isso acontece quando: 1. O primeiro pacote de um iniciador TCP não é SYN (o segmento TCP não inicia recebido sem uma sessão válida). 2. O pacote SYN inicial tem a flag ACK definida.
SYN com dados	O pacote SYN contém o payload. Não há suporte para isso.
Sinalizadores TCP inválidos	Sinalizadores TCP inválidos podem ser causados por: 1. O pacote SYN inicial do TCP tem flags diferentes de SYN. 2. No estado de escuta TCP, um peer TCP recebe um RST ou um ACK. 3. O pacote de outro respondedor é recebido antes de SYN/ACK. 4. SYN/ACK esperado não é recebido do respondente.
Segmento inválido no estado SYNSENT	Um segmento TCP inválido no estado SYNSENT é causado por: 1. SYN/ACK tem payload. 2. SYN/ACK tem outros flags (PSH, URG, FIN) definidos. 3. Receba um SYN de trânsito com payload. 4. Receba um pacote não-SYN do iniciador.
Segmento inválido no estado SYNRCVD	Um segmento TCP inválido no estado SYNRCVD pode ser causado por: 1. Receba um SYN de retrânsito com payload do iniciador. 2. Receba um segmento inválido que não seja SYN/ACK, RST ou FIN do respondente.
SEQ inválido	Isso ocorre no estado SYNRCVD quando os segmentos vêm do iniciador. É causad por: 1. Seq# é menor que ISN. 2. Se o tamanho da janela do receptor rcvd for 0 e: O segmento tem payload ou Segmento fora de ordem (seq# é maior que o receptor LASTACK. 3. Se o tamanho da janela do receptor rcvd for 0 e seq# cair além da janela. 4. Seq# é igual a ISN, mas não a um pacote SYN.
Opção de escala de janela inválida	A opção de escala de janela TCP inválida é causada pelo comprimento de byte da opção de escala de janela incorreta.
TCP fora da janela	O pacote é muito antigo - uma janela atrás do ACK do outro lado. Isso pode aconte nos estados ESTABLISHED, CLOSEWAIT e LASTACK.
payload extra de TCP após envio FIN	Carga recebida após o envio do FIN. Isso pode acontecer no estado CLOSEWAIT.

Sobrecarga da janela TCP	Isso ocorre quando o tamanho do segmento de entrada sobrecarrega a janela do receptor. No entanto, se o vTCP estiver habilitado, essa condição é permitida porqu firewall precisa armazenar em buffer o segmento para que o ALG seja consumido posteriormente.
Retran com sinalizadores inválidos	Um pacote retransmitido já foi confirmado pelo receptor.
Segmento fora de ordem TCP	O pacote fora de ordem está prestes a ser entregue para L7 para inspeção. Se L7 r permitir o segmento OO, esse pacote será descartado.
Inundação de SYN	Sob um ataque de inundação TCP SYN. Sob certas condições quando as conexões atuais com esse host excederem o valor de meia-abertura configurado, o firewall rejeitará quaisquer novas conexões com esse endereço IP por um período de temp Como resultado, os pacotes serão descartados.
Erro interno - falha na alocação de verificação de inundação de sincronização	Durante a verificação de inundação de sincronização, a alocação do hostdb falha. Ação recomendada: marque "show platform hardware qfp ative feature firewall mem (mostrar memória de firewall de recurso ativa do qfp de hardware da plataforma) pa verificar o status da memória.
Derivação de blecaute de inundação	Se as conexões semiabertas configuradas forem excedidas e o tempo de blecaute configurado, todas as novas conexões a esse endereço IP serão descartadas.
Limite de sessão de meia abertura excedido	Pacote descartado devido ao excesso de sessões de meia-abertura permitidas. Verifique também as configurações de "máximo incompleto alto/baixo" e "um minut alto/baixo" para verificar se o número de sessões semiabertas não está sendo restringido por essas configurações.
Excesso de pacotes por fluxo	O número máximo de pacotes inspecionáveis permitidos por fluxo é excedido. O nú máximo é 25.
Muitos pacotes de erro ICMP por fluxo	O número máximo de pacotes de erro ICMP permitidos por fluxo é excedido. O núm máximo é 3.
Carga TCP inesperada do Rsp para Inicializar	No estado SYNRCVD, o TCP recebe um pacote com payload do respondente para direção do iniciador.
Erro interno - Direção indefinida	Direção do pacote indefinida.
SYN dentro da janela atual	Um pacote SYN é visto na janela de uma conexão TCP já estabelecida.
RST dentro da janela atual	Um pacote RST é observado dentro da janela de uma conexão TCP já estabelecida
Segmento fora de uso	Um segmento TCP é recebido que não deve ter sido recebido através da máquina estado TCP, como um pacote TCP SYN sendo recebido no estado de escuta do respondente.
Erro interno ICMP - Informações de NAT ICMP ausentes	O pacote ICMP não é fornecido, mas as informações de NAT interno estão ausente Este é um erro interno.
Pacote ICMP em estado de fechamento de SCB	Recebido um pacote ICMP no estado FECHAMENTO SCB.
Cabeçalho IP perdido no pacote ICMP	Cabeçalho IP ausente no pacote ICMP.
Erro de ICMP sem IP ou ICMP	Pacote de erro ICMP sem IP ou ICMP no payload. Provavelmente causado por um pacote mal formado ou um ataque.

Pacote de erro de ICMP muito curto	O pacote de erro ICMP é muito curto.
Erro ICMP Excede Limite de Intermitência	O pacote de erro ICMP excede o limite de burst de 10.
Erro ICMP inalcançável	Pacote de erro ICMP inalcançável excede o limite. Somente o 1 st pacote inalcançá pode passar.
Erro de ICMP Seq# inválido	Seq# do pacote incorporado não corresponde ao seq# do pacote que originou o err ICMP.
Erro de ICMP na confirmação inválida	ACK inválido no pacote incorporado de erro ICMP.
queda de ação ICMP	A ação ICMP configurada é solta.
Zone-pair sem policy-map	Política não presente em par de zonas. isso pode ser devido ao ALG (Application L Gateway, Gateway de Camada de Aplicação) não estar configurado para abrir o pir para o canal de dados da aplicação, ou o ALG não abriu o pinhole corretamente, ou nenhum pinhole está aberto devido a problemas de escalabilidade.
Sessão perdida e política não presente	Falha na pesquisa da sessão e não há nenhuma política presente para inspecionar pacote.
Erro e política de ICMP não presentes	Erro de ICMP sem política configurada no par de zonas.
Falha na classificação	Falha de classificação em um determinado par de zonas quando o Firewall tenta determinar se o protocolo é inspecionável.
Queda de ação de classificação	A ação de classificação é descartada.
Configuração incorreta da política de segurança	Falha na classificação devido a uma configuração incorreta da política de segurança Isso também pode ser devido à ausência de pinpole para o canal de dados L7.
Enviar RST para o respondente	Enviar RST para o respondente no estado SYNSENT quando ACK# não é igual a I
Queda de política de firewall	A ação da política é cair.
Descarte de Fragmento	Descarte os fragmentos restantes quando o primeiro fragmento for descartado.
Queda de política de firewall ICMP	A ação de política do pacote ICMP incorporado é DROP.
A inspeção L7 retorna DROP	L7 (ALG) decide descartar o pacote. O motivo pode ser encontrado em diferentes estatísticas de ALG.
Pacote do segmento L7 não permitido	Pacote segmentado recebido quando o ALG não o honra.
Pacote de Fragmento L7 Não Permitido	Recebidos pacotes fragmentados (ou VFR) quando o ALG não o honra.
Tipo de prova L7 desconhecido	Tipo de protocolo não reconhecido.

Solucionar problemas de quedas de firewall

Quando o motivo da queda é identificado nos contadores globais ou de queda de recursos do firewall acima, talvez sejam necessárias etapas adicionais de solução de problemas se essas quedas forem inesperadas. Além da validação da configuração para garantir que a configuração

esteja correta para as funcionalidades de firewall habilitadas, geralmente é necessário fazer capturas de pacotes para o fluxo de tráfego em questão para ver se os pacotes estão malformados ou se há algum problema de implementação de protocolo ou aplicativo.

Registro

A funcionalidade de registro ASR gera syslogs para gravar pacotes descartados. Esses syslogs fornecem mais detalhes sobre por que o pacote foi descartado. Há dois tipos de sysloggings:

1. Syslogging armazenado em buffer local
2. Registro remoto de alta velocidade

Syslogging de buffer local

Para isolar a causa das quedas, você pode usar a solução de problemas genérica de ZBFW, como ativar quedas de log. Há duas maneiras de configurar o registro de queda de pacote.

Método 1: Use inspect-global parameter-map para registrar todos os pacotes descartados.

```
parameter-map type inspect-global     log dropped-packets
```

Método 2: Use o mapa de parâmetros de inspeção personalizada para registrar os pacotes descartados apenas para uma classe específica.

```
parameter-map type inspect LOG_PARAM
log dropped-packets
!
policy-map type inspect ZBFW_PMAP
class type inspect ZBFW_CMAP
inspect LOG_PARAM
```

Essas mensagens são enviadas para o log ou console, dependendo de como o ASR está configurado para registro. Aqui está um exemplo de uma mensagem de log de queda.

```
*Apr  8 13:20:39.075: %IOSXE-6-PLATFORM: F0: cpp_cp: QFP:0.0 Thread:103
TS:00000605668054540031 %FW-6-DROP_PKT: Dropping tcp pkt from GigabitEthernet0/0/2
14.38.112.250:41433 => 14.36.1.206:23(target:class)-(INSIDE_OUTSIDE_ZP:class-default)
due to Policy drop:classify result with ip ident 11579 tcp flag 0x2, seq 2014580963,
ack 0
```

Limitações de syslogging de buffer local

1. Esses registros têm uma taxa limitada de acordo com a ID de bug da Cisco CSCud09943.
2. Esses registros podem não ser impressos a menos que uma configuração específica seja aplicada. Por exemplo, os pacotes descartados por pacotes padrão de classe não serão registrados a menos que a palavra-chave **log** seja especificada:

```
policy-map type inspect ZBFW_PMAP
class class-default
drop log
```

Registro remoto de alta velocidade

O HSL (High Speed Login, registro de alta velocidade) gera syslogs diretamente do QFP e o envia ao coletor HSL do netflow configurado. Esta é a solução de registro recomendada para ZBFW em ASR.

Para HSL, use esta configuração:

```
parameter-map type inspect inspect-global
  log template timeout-rate 1
  log flow-export v9 udp destination 1.1.1.1 5555
```

Para usar essa configuração, é necessário um coletor netflow capaz do Netflow Versão 9. Isso é detalhado em

Guia de configuração: Firewall de política baseado em zona, Cisco IOS XE versão 3S (ASR 1000) Firewall de alta velocidade

Rastreamento de pacotes usando correspondência condicional

Ative as depurações condicionais para ativar o rastreamento de pacotes e depois habilitar o rastreamento de pacotes para esses recursos:

```
ip access-list extended CONDITIONAL_ACL
 permit ip host 10.1.1.1 host 192.168.1.1
 permit ip host 192.168.1.1 host 10.1.1.1
!
debug platform condition feature fw dataplane submode all level info
debug platform condition ipv4 access-list CONDITIONAL_ACL both
```

> **Note**: A condição de correspondência pode usar o endereço IP diretamente, pois uma ACL não é necessária. Isso corresponderá como origem ou destino, o que permite rastreamentos bidirecionais. Esse método pode ser usado se você não tiver permissão para alterar a configuração. Por exemplo: debug platform condition ipv4 address 192.168.1.1/32.

Ative o recurso de rastreamento de pacotes:

```
debug platform packet-trace copy packet both
debug platform packet-trace packet 16
debug platform packet-trace drop
debug platform packet-trace enable
```

Há duas maneiras de usar este recurso:

1. Insira o comando **debug platform packet-trace drop** para rastrear apenas os pacotes descartados.

2. A exclusão do comando **debug platform packet-trace drop** rastreará qualquer pacote que

corresponda à condição, incluindo aqueles que são inspecionados/passados pelo dispositivo.

Ativar depurações condicionais:

```
debug platform condition start
```

Execute o teste e, em seguida, desative as depurações:

```
debug platform condition stop
```

Agora as informações podem ser exibidas na tela. Neste exemplo, os pacotes ICMP foram descartados devido a uma política de firewall:

```
Router#show platform packet-trace statistics
Packets Summary
 Matched  2
 Traced   2
Packets Received
 Ingress  2
 Inject   0
Packets Processed
 Forward  0
 Punt     0
 Drop     2
   Count       Code  Cause
   2           183   FirewallPolicy
 Consume  0
```

```
Router#show platform packet-trace summary
Pkt   Input            Output           State  Reason
0     Gi0/0/2          Gi0/0/0          DROP   183 (FirewallPolicy)
1     Gi0/0/2          Gi0/0/0          DROP   183 (FirewallPolicy)
```

```
Router#show platform packet-trace packet 0
Packet: 0           CBUG ID: 2980
Summary
 Input     : GigabitEthernet0/0/2
 Output    : GigabitEthernet0/0/0
 State     : DROP 183 (FirewallPolicy)
 Timestamp
   Start   : 1207843476722162 ns (04/15/2014 12:37:01.103864 UTC)
   Stop    : 1207843477247782 ns (04/15/2014 12:37:01.104390 UTC)
Path Trace
 Feature: IPV4
   Source      : 10.1.1.1
   Destination : 192.168.1.1
   Protocol    : 1 (ICMP)
 Feature: ZBFW
   Action  : Drop
   Reason  : ICMP policy drop:classify result
   Zone-pair name  : INSIDE_OUTSIDE_ZP
   Class-map name  : class-default
Packet Copy In
 c89c1d51 5702000c 29f9d528 08004500 00540000 40004001 ac640e26 70fa0e24
 01010800 172a2741 00016459 4d5310e4 0c000809 0a0b0c0d 0e0f1011 12131415
```

```
Packet Copy Out
 c89c1d51 5702000c 29f9d528 08004500 00540000 40003f01 ad640e26 70fa0e24
 01010800 172a2741 00016459 4d5310e4 0c000809 0a0b0c0d 0e0f1011 12131415
```

O comando show platform packet-trace packet <num> decode decodifica as informações e o conteúdo do cabeçalho do pacote. Este recurso foi introduzido no XE3.11:

```
Router#show platform packet-trace packet all decode
Packet: 0           CBUG ID: 2980
Summary
 Input     : GigabitEthernet0/0/2
 Output    : GigabitEthernet0/0/0
 State     : DROP 183 (FirewallPolicy)
 Timestamp
   Start   : 1207843476722162 ns (04/15/2014 12:37:01.103864 UTC)
   Stop    : 1207843477247782 ns (04/15/2014 12:37:01.104390 UTC)
Path Trace
 Feature: IPV4
    Source      : 10.1.1.1
    Destination : 192.168.1.1
    Protocol    : 1 (ICMP)
  Feature: ZBFW
    Action  : Drop
    Reason  : ICMP policy drop:classify result
    Zone-pair name  : INSIDE_OUTSIDE_ZP
    Class-map name  : class-default
Packet Copy In
 c89c1d51 5702000c 29f9d528 08004500 00540000 40004001 ac640e26 70fa0e24
 01010800 172a2741 00016459 4d5310e4 0c000809 0a0b0c0d 0e0f1011 12131415
 ARPA
    Destination MAC     : c89c.1d51.5702
    Source MAC          : 000c.29f9.d528
   Type               : 0x0800 (IPV4)
 IPv4
   Version            : 4
   Header Length      : 5
   ToS                : 0x00
   Total Length       : 84
   Identifier         : 0x0000
   IP Flags           : 0x2 (Don't fragment)
   Frag Offset        : 0
   TTL                : 64
   Protocol           : 1 (ICMP)
   Header Checksum    : 0xac64
   Source Address     : 10.1.1.1
   Destination Address : 192.168.1.1
 ICMP
   Type               : 8 (Echo)
   Code               : 0 (No Code)
   Checksum           : 0x172a
   Identifier         : 0x2741
   Sequence           : 0x0001
Packet Copy Out
 c89c1d51 5702000c 29f9d528 08004500 00540000 40003f01 ad640e26 70fa0e24
 01010800 172a2741 00016459 4d5310e4 0c000809 0a0b0c0d 0e0f1011 12131415
 ARPA
   Destination MAC     : c89c.1d51.5702
   Source MAC          : 000c.29f9.d528
   Type               : 0x0800 (IPV4)
 IPv4
   Version            : 4
   Header Length      : 5
   ToS                : 0x00
```

```
   Total Length        : 84
   Identifier          : 0x0000
   IP Flags            : 0x2 (Don't fragment)
   Frag Offset         : 0
   TTL                 : 63
   Protocol            : 1 (ICMP)
   Header Checksum     : 0xad64
   Source Address      : 10.1.1.1
   Destination Address : 192.168.1.1
 ICMP
   Type                : 8 (Echo)
   Code                : 0 (No Code)
   Checksum            : 0x172a
   Identifier          : 0x2741
   Sequence            : 0x0001
```

Captura de pacote incorporado

O suporte à Captura de pacote incorporado foi adicionado no Cisco IOS-XE 3.7 (15.2(4)S). Para obter mais detalhes, consulte

Exemplo de configuração de Captura de pacote incorporado para Cisco IOS e IOS-XE.

Debugs

Depurações Condicionais

No XE3.10, depurações condicionais serão apresentadas. Instruções condicionais podem ser usadas para garantir que o recurso ZBFW registre apenas mensagens de depuração que sejam relevantes para a condição. As depurações condicionais usam ACLs para restringir logs que correspondem aos elementos da ACL. Além disso, antes do XE3.10, as mensagens de depuração eram mais difíceis de ler. A saída de depuração foi aprimorada no XE3.10 para torná-los mais fáceis de entender.

Para habilitar essas depurações, emita este comando:

```
debug platform condition feature fw dataplane submode [detail | policy | layer4 | drop]
debug platform condition ipv4 access-list <ACL_name> both
debug platform condition start
```

Observe que o comando condition deve ser definido através de uma ACL e direcionalidade. As depurações condicionais não serão implementadas até que sejam iniciadas com o comando **debug platform condition start**. Para desativar depurações condicionais, use o comando **debug platform condition stop**.

```
debug platform condition stop
```

Para desativar depurações condicionais, **NÃO** use o comando **undebug all**. Para desativar todas as depurações condicionais, use o comando:

```
ASR#clear platform condition all
```

Antes do XE3.14, as depurações **ha** e **event** não são condicionais. Como resultado, o comando **debug platform condition feature fw dataplane submode all** faz com que todos os registros sejam criados, independentemente da condição selecionada abaixo. Isso pode criar ruído adicional que dificulta a depuração.

Por padrão, o nível de registro condicional é **info**. Para aumentar/diminuir o nível de registro, use o comando:

```
debug platform condition feature fw dataplane submode all [verbose | warning]
```

Coletar e exibir depurações

Os arquivos de depuração não serão impressos no console ou no monitor. Todas as depurações são gravadas no disco rígido do ASR. As depurações são gravadas no disco rígido sob a pasta **tracelogs** com o nome **cpp_cp_F0-0.log.<date>**. Para visualizar o arquivo onde as depurações são gravadas, use a saída:

```
ASR# cd harddisk:
ASR# cd tracelogs
ASR# dir cpp_cp_F0*Directory of harddisk:/tracelogs/cpp_cp_F0*

Directory of harddisk:/tracelogs/

3751962 -rwx 1048795 Jun 15 2010 06:31:51 +00:00
cpp_cp_F0-0.log.5375.20100615063151
3751967 -rwx 1048887 Jun 15 2010 02:18:07 +00:00
cpp_cp_F0-0.log.5375.20100615021807
39313059840 bytes total (30680653824 bytes free)
```

Cada arquivo de depuração será armazenado como um arquivo **cpp_cp_F0-0.log.<date>**. Esses são arquivos de texto regulares que podem ser copiados do ASR com TFTP. O máximo do arquivo de log no ASR é de 1Mb. Após 1Mb, as depurações são gravadas em um novo arquivo de log. É por isso que cada arquivo de log tem uma marca de hora para indicar o início do arquivo.

Arquivos de log podem existir nestes locais:

```
harddisk:/tracelogs/
bootflash:/tracelogs/
```

Como os arquivos de log são exibidos somente depois que são girados, o arquivo de log pode ser girado manualmente com este comando:

```
ASR# test platform software trace slot f0 cpp-control-process rotate
```

Isso cria imediatamente um arquivo de log "cpp_cp" e inicia um novo no QFP. Por exemplo:

```
ASR#test platform software trace slot f0 cpp-control-process rotate
 Rotated file from: /tmp/fp/trace/stage/cpp_cp_F0-0.log.7311.20140408134406,
Bytes: 82407, Messages: 431

ASR#more tracelogs/cpp_cp_F0-0.log.7311.20140408134406
04/02 10:22:54.462 : btrace continued for process ID 7311 with 159 modules
04/07 16:52:41.164 [cpp-dp-fw]: (info): QFP:0.0 Thread:110 TS:00000531990811543397
```

```
:FW_DEBUG_FLG_HA:[]: HA[1]: Changing HA state to 9
04/07 16:55:23.503 [cpp-dp-fw]: (info): QFP:0.0 Thread:120 TS:00000532153153672298
:FW_DEBUG_FLG_HA:[]: HA[1]: Changing HA state to 10
04/07 16:55:23.617 [buginf]: (debug): [system] Svr HA bulk sync CPP(0) complex(0)
epoch(0) trans_id(26214421) rg_num(1)
```

Esse comando permite que os arquivos de depuração sejam mesclados em um único arquivo para facilitar o processamento. Ele mescla todos os arquivos no diretório e os entrelaça com base no tempo. Isso pode ajudar quando os logs são muito detalhados e são criados em vários arquivos:

```
ASR#request platform software trace slot rp active merge target bootflash:MERGED_OUTPUT.log
Creating the merged trace file: [bootflash:MERGED_OUTPUT.log]
 including all messages

Done with creation of the merged trace file: [bootflash:MERGED_OUTPUT.log]
```