ZBFW para a configuração IOS-XE pesquisam defeitos o guia

Índice

Introdução

Este documento descreve como o melhor pesquisa defeitos a característica baseada zona do Firewall (ZBFW) no roteador dos serviços da agregação (ASR) 1000, com comandos que são usados para votar os contadores de queda do hardware no ASR. O ASR1000 é uma plataforma com base em hardware da transmissão. A configuração de software do ® do Cisco IOS XE programa o asics de hardware (processador do fluxo do quantum (QFP) a fim executar funcionalidades da transmissão da característica. Isto permite o throughput elevado e o melhor desempenho. O inconveniente a este é que apresenta um desafio maior para pesquisar defeitos. Os comandos cisco ios tradicionais usados para votar sessões atual e contadores de queda através do Firewall Zona-baseado (ZBFW) são já não por mais válidas que as gotas sejam já não no software.

Links e documentação

Referências de comandos

- Referências de comandos do Roteadores de serviços de agregação Cisco ASR série 1000
- Referências de comandos do Cisco IOS XE 3S

Datapath pesquisa defeitos etapas

A fim pesquisar defeitos o datapath, você deve identificar se o tráfego está passado corretamente com o código ASR e de Cisco IOS XE. O específico aos recursos de firewall, o Troubleshooting do datapath segue estas etapas:

1. **Verifique a configuração** - Recolha a configuração e examine a saída a fim verificar a conexão.

2. **Verifique o estado de conexão** - Se o tráfego passa corretamente, o Cisco IOS XE abre uma conexão na característica ZBFW. Esta conexão segue o tráfego e a informação de estado entre um cliente e servidor.

3. **Verifique contadores de queda** - Quando o tráfego não passa corretamente, o Cisco IOS XE registra um contador de queda para todos os pacotes descartado. Verifique esta saída a fim isolar a causa da falha do tráfego.

4. **Registrar** - Syslog do recolhimento a fim fornecer a informação mais granulada em construções e em quedas de pacote de informação da conexão.

5. **Pacotes descartado do rastreamento de pacotes** - Use o pacote que segue a fim travar pacotes descartado.

6. **Debuga** - O recolhimento debuga é a maioria de opção eloquente. Debugs pode ser obtido condicionalmente a fim confirmar o trajeto de encaminhamento exato para os pacotes.

Verifique a configuração

A saída do **Firewall do suporte técnico da mostra** é 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> --------
```

Verifique o estado de conexão

A informação de conexão pode ser obtida de modo que todas as conexões em ZBFW estejam listadas. Incorpore 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]
```

Mostra uma conexão Telnet TCP de 14.38.112.250 a 14.36.1.206.

> **Note**: Esteja ciente que se você executa este comando, tomará um muito tempo se há uns lotes das conexões no dispositivo. Cisco recomenda que você executa este comando com filtros específicos como esboçado aqui.

A tabela de conexão pode ser filtrada para baixo a um endereço de origem ou de destino específico. Use filtros após o submode 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 tão somente conexões filtradas originado de 14.38.112.250 é indicada:

```
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]
```

Uma vez que a tabela de conexão é filtrada, a informação de conexão detalhada pode ser obtida para um anlaysis mais detalhado. A fim indicar esta saída, use a palavra-chave do **detalhe**.

```
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
```

Verifique contadores de queda do Firewall

A saída do contador de queda mudada durante XE 3.9. Antes de XE 3.9, as razões da gota do Firewall eram muito genéricas. Após XE 3.9, as razões da gota do Firewall foram estendidas tornar-se mais granuladas.

A fim verificar contadores de queda, execute duas etapas:

1. Confirme os contadores de queda globais no Cisco IOS XE. Estes contadores mostram que característica deixou cair o tráfego. Os exemplos das características incluem o Qualidade de Serviço (QoS), Network Address Translation (NAT), Firewall, e assim por diante.

2. Uma vez que o subfeature foi identificado, pergunte os contadores de queda granulados oferecidos pelo subfeature. Neste guia, o subfeature que está sendo analisado é os recursos de firewall.

Contadores de queda globais em QFP

O comando básico confiar sobre fornece todas as gotas através do QFP:

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

Este comando mostra-lhe as gotas genéricas globalmente através do QFP. Estas gotas podem estar em toda a característica. Algumas características do exemplo são:

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

A fim ver todas as gotas, inclua os contadores que têm um valor de zero, usam o comando:

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

A fim cancelar os contadores, use este comando. Cancela a saída após ter mostrado a à tela. Este comando é claro no lido, assim que a saída está restaurada a zero **depois que** é indicada à tela.

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

Está abaixo uma lista de contadores de queda e de explicação globais do Firewall QFP:

Razão global da gota do	Explicação

Firewall	
FirewallBackpressure	Queda de pacote de informação devido à pressão contrária registrando o mecanismo.
FirewallInvalidZone	Nenhuma zona de Segurança configurada para a relação.
FirewallL4Insp	Falha da verificação da política L4. Veja a tabela abaixo para umas razões m granuladas da gota (razões da gota dos recursos de firewall).
FirewallNoForwardingZone	O Firewall é uninitialized, e o sem tráfego é permitido passar.
FirewallNonsession	A criação de sessão falha. Poderia ser devido ao limite de sessão máximo alcançou ou falha de alocação de memória.
FirewallPolicy	A política de firewall configurada é gota.
FirewallL4	Falha da inspeção L4. Veja a tabela abaixo para umas razões mais granulada da gota (a gota dos recursos de firewall raciocina).
FirewallL7	Queda de pacote de informação devido à inspeção L7. Veja abaixo para uma lista de umas razões mais granuladas da gota L7 (a gota dos recursos de fire raciocina).
FirewallNotInitiator	Não um iniciador da sessão para o TCP, o UDP, ou o ICMP. Nenhuma sessã criada. Por exemplo, porque ICMP o primeiro pacote recebido não é ECO ou TIMESTAMP. Para o TCP, não é um SYN. Isto podia acontecer no pacote normal que processa ou que processa imprec do canal.
FirewallNoNewSession	A Alta disponibilidade do Firewall não permite sessões novas.
FirewallSyncookieMaxDst	A fim fornecer host-baseou a proteção de inundação de SYN, há uma taxa do destino per. SYN como o limite da inundação de SYN. Quando o número de entradas de destino alcança o limite, os pacotes SYN novos estão deixados c
FirewallSyncookie	A lógica SYNCOOLIE é provocada. Isto indica que o SYN/ACK com Cookie S esteve enviado, e o pacote SYN original está deixado cair.
FirewallARStandby	O roteamento assimétrico não é permitido e o grupo de redundância não est no estado ativo.

Contadores de queda dos recursos de firewall em QFP

A limitação com o contador de queda global QFP é que não há nenhuma granularidade nas razões da gota, e algumas das razões da gota tais como **FirewallL4** obtêm sobrecarregadas assim ao ponto que são de pouco uso para pesquisar defeitos. Isto tem sido aumentado desde no Cisco IOS XE 3.9 (15.3(2)S), onde os contadores de queda dos recursos de firewall foram adicionados. Isto dá um grupo muito mais granulado de razões da gota:

```
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
....
```

Está abaixo uma lista de razões e de explicações da gota dos recursos de firewall:

Razão da gota dos recursos de firewall	Explicação
Comprimento de cabeçalho	A datagrama é tão pequena que não poderia conter a camada 4TCP,UDP, ou cabeçalho ICMP. Poderia ser causada por:

inválido	1. Comprimento de cabeçalho de TCP < 20 2. Comprimento de cabeçalho UDP/ICMP < 8
Comprimento de dados inválido UDP	O comprimento da datagrama de UDP não combina o comprimento especificado no cabeçalho de UDP.
Número inválido ACK	Esta gota podia ser causada por uma destas razões: 1. Os iguais ACK não ao next_seq# do TCP espreitam. 2. O ACK é maior do que o SEQ# o mais recente enviado pelo par TCP.
Bandeira inválida ACK	No estado TCP SYNSENT e SYNRCVD, espera-se que o ACK# é igual a ISN+1 mas nã Esta gota podia ser causada por uma destas razões: 1. Esperando a bandeira ACK mas não ajustado no estado diferente TCP. 2. A não ser a bandeira ACK, a outra bandeira (como o RST) é ajustada igualmente.
Iniciador inválido TCP	Isto acontece quando: 1. O primeiro pacote de um iniciador TCP não é um SYN (o segmento NON-inicial TC recebido sem uma sessão válida). 2. O pacote SYN inicial tem a bandeira ACK ajustada.
SYN com dados	O pacote SYN contém o payload. Isto não é apoiado.
Bandeiras inválidas TCP	As bandeiras inválidas TCP podem ser causadas por: 1. O pacote SYN da inicial TCP tem bandeiras diferentes do SYN. 2. No TCP escuta o estado, um par TCP recebe um RST ou um ACK. 3. O pacote do outro que responde é recebido antes do SYN/ACK. 4. O SYN/ACK previsto não é recebido do que responde.
Segmento inválido no estado SYNSENT	Um segmento inválido TCP no estado SYNSENT é causado por: 1. O SYN/ACK tem o payload. 2. O SYN/ACK tem outras bandeiras (PSH, URG, FIN) ajustadas. 3. Receba um trânsito SYN com payload. 4. Receba um pacote NON-SYN do iniciador.
Segmento inválido no estado SYNRCVD	Um segmento inválido TCP no estado SYNRCVD podia ser causado por: 1. Receba um retransit SYN com o payload do iniciador. 2. Receba um segmento inválido que não seja SYN/ACK, RST, ou FIN do que respon
SEGS. inválido	Isto ocorre no estado SYNRCVD quando os segmentos vêm do iniciador. É causado por 1. Seq# é menos do que o ISN. 2. Se o tamanho de janela do rcvd do receptor é 0 e: O segmento tem o payload, ou Segmento fora de serviço (o seq# é maior do que o receptor LASTACK. 3. Se o tamanho de janela do rcvd do receptor é 0 e o seq# cai além do indicador. 4. Iguais de Seq# ao ISN mas não a um pacote SYN.
Opção inválida da escala do indicador	A opção inválida da escala da janela TCP é causada pelo comprimento incorreto do byte opção da escala do indicador.
TCP fora do indicador	O pacote é demasiado velho - um indicador atrás do outro ACK de lado. Isto podia acont no estado ESTABELECIDO, CLOSEWAIT e LASTACK.
Payload extra TCP após o FIN enviado	Payload recebido após o FIN enviado. Isto podia acontecer no estado CLOSEWAIT.
Excesso da janela TCP	Isto ocorrer quando o indicador do receptor entrante dos excessos do tamanho do segme Contudo, se o vTCP é permitido, esta circunstância é permitida porque o Firewall precisa

	proteger o segmento para que ALG consuma mais tarde.
Retran com bandeiras inválidas	Um pacote retransmitido foi reconhecido já pelo receptor.
Segmento fora de serviço TCP	O pacote estragado está a ponto de ser entregado ao L7 para a inspeção. Se o L7 não permite o segmento OOO, este pacote estará deixado cair.
Inundação de SYN	Sob um ataque de inundação de SYN TCP. Sob certas condições quando as conexões a este host excedem o valor entreaberto configurado o Firewall rejeitará todas as novas conexões a este endereço IP de Um ou Mais Servidores Cisco ICM NT por um período d tempo. Em consequência os pacotes serão deixados cair.
Interno erra - o alloc da verificação do synflood falhado	Durante a verificação do synflood, a atribuição do hostdb falha. Ação recomendada: verifique da “a memória ativa do Firewall da característica do qfp do hardware da plataforma mostra” para verificar o estado da memória.
Gota do escurecimento de Synflood	Se as conexões meio aberta configuradas são excedidas e tempo do escurecimento está configurado, toda a nova conexão a este endereço IP de Um ou Mais Servidores Cisco IC NT está deixada cair.
O limite de sessão entreaberto excede	O pacote deixou cair devido aos sessão semi-aberta permitidos excedidos. Igualmente verifique os ajustes “da elevação máxima incompleta - ponto baixo” e do “elev minuto - ponto baixo” para certificar-se do # dos sessão semi-aberta não estão sendo estrangulados por estas configurações.
Pacote demais pelo fluxo	O número máximo de pacotes inspectable permitidos pelo fluxo é excedido. O número máximo é 25.
Pacotes demais do erro ICMP pelo fluxo	O número máximo de pacotes do erro ICMP permitidos pelo fluxo é excedido. O número máximo é 3.
Payload de TCP de Unexpect de Rsp a Init	No estado SYNRCVD, o TCP recebe um pacote com o payload do que responde ao sent do iniciador.
Erro interno - Sentido indeterminado	Sentido do pacote undefined.
SYN dentro da janela atual	Um pacote SYN é visto dentro do indicador de uma conexão de TCP já estabelecida.
RST dentro da janela atual	Um pacote de RST é observado dentro do indicador de uma conexão de TCP já estabele
Segmento disperso	Um segmento TCP é recebido que não deva ter sido recebido através da máquina de est TCP tal como um pacote SYN de TCP que está sendo recebido no estado da escuta do c responde.
Erro interno ICMP - Informação NAT faltada ICMP	O pacote ICMP nat'ed mas a informação NAT interna falta. Este é um erro interno.
O pacote ICMP em SCB fecha o estado	Recebeu um pacote ICMP no estado PRÓXIMO SCB.
Cabeçalho IP faltado no pacote ICMP	Cabeçalho IP faltante no pacote ICMP.

Erro ICMP nenhum IP ou ICMP	Pacote do erro ICMP sem IP ou ICMP no payload. Causado provavelmente por um paco malformado ou por um ataque.
O ICMP erra Pacote demasiado curto	O pacote do erro ICMP é demasiado curto.
O ICMP erra excede o limite da explosão	O pkt do erro ICMP excede o limite da explosão de 10.
O ICMP erra inacessível	O pkt do erro ICMP inacessível excede o limite. Somente o ø pacote inacessível é permit passar completamente.
O ICMP erra Seq# inválido	Seq# do pacote encaixado não combina o seq# do pacote que origina o erro ICMP.
O ICMP erra Ack inválido	ACK inválido no pacote encaixado erro ICMP.
Gota da ação ICMP	A ação configurada ICMP é gota.
Zona-pares sem mapa de política	Política não atual em zona-pares. poderia ser devido a ALG (gateway de camada de aplicativo) que não está sendo configurado para abrir o furo de pino para o canal de dado aplicativo, ou ALG não abriu o furo de pino corretamente, ou nenhum furo de pino é aber devido às questões de escalabilidade.
Sessão faltada e política não atual	A consulta da sessão falhou e nenhuma política esta presente para inspecionar este pac
Erro ICMP e política não atuais	Erro ICMP sem a política configurada em zona-pares.
Classificação falhada	Falha da classificação em um par dado da zona quando o Firewall tentar determinar se o protocolo é inspectable.
Gota da ação da classificação	A ação da classificação é gota.
Política de segurança Misconfig	Classificação falhada devido ao misconfiguration da política de segurança. Isto podia igualmente ser devido a nenhum pinpole para o canal de dados L7.
Envie o RST ao que responde	Envie o RST ao que responde no estado SYNSENT quando ACK# não é igual a ISN+1.
Gota da política de firewall	A ação de política é deixar cair.
Gota do fragmento	Deixe cair fragmentos restantes quando o primeiro fragmento é deixado cair.
Gota da política ICMP	A ação de política do pacote encaixado ICMP é GOTA.
Firwall A inspeção L7 retorna a GOTA	O L7 (ALG) decide deixar cair o pacote. A razão podia ser encontrada das estatísticas diferentes ALG.
L7 segmento Pacote para	Pacote segmentado recebido quando ALG não o honrar.

não reservar L7 fragmento Pacote para não reservar	(Ou VFR) pacotes fragmentados recebidos quando ALG não o honrar.
Tipo L7 Proto desconhecido	Tipo de protocolo não reconhecido.

Pesquise defeitos gotas do Firewall

Uma vez que a razão da gota é identificada dos contadores de queda acima globais ou dos recursos de firewall, as etapas do Troubleshooting adicional puderam ser precisadas se estas gotas são inesperadas. Independentemente da validação da configuração a fim assegurar a configuração está correto para as funcionalidades de firewall permitidas, exige-se frequentemente para tomar capturas de pacote de informação para o fluxo de tráfego na pergunta para ver se os pacotes são deformados ou se há alguma edição da aplicação do protocolo ou do aplicativo.

Registro

A funcionalidade de registro ASR gerencie Syslog a fim gravar pacotes descartado. Estes Syslog fornecem mais detalhes em porque o pacote foi deixado cair. Há dois tipos de informações de syslog:

1. Informações de syslog protegida Local

2. Registro remoto da alta velocidade

Informações de syslog protegida Local

A fim isolar a causa das gotas, você pode usar o Troubleshooting genérico ZBFW, tal como a possibilidade de gotas do log. Há duas maneiras de configurar o registro da queda de pacote de informação.

Método 1: Use o parâmetro-mapa inspecionar-global a fim registrar todos os pacotes descartado.

```
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
....
```

Método 2: O costume do uso inspeciona o parâmetro-mapa a fim registrar pacotes descartado para somente a 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
```

Estas mensagens são enviadas ao log ou ao console segundo como o ASR é configurado registrando. Está aqui um exemplo de um mensagem de registro da gota.

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

Limitações da informações de syslog protegida Local

1. Estes logs são taxa limitada conforme a identificação de bug Cisco CSCud09943.

2. Estes logs não puderam imprimir a menos que a configuração específica fosse aplicada. Por exemplo, os pacotes deixados cair por pacotes do class-default não serão registrados a menos que a palavra-chave do **log** for especificada:

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

Registro remoto da alta velocidade

A alta velocidade que registra (HSL) gerencie Syslog diretamente do QFP e envia-os ao coletor configurado do Netflow HSL. Esta é a solução de registro recomendada para ZBFW no ASR.

Para o HSL, use esta configuração:

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

A fim usar esta configuração, um coletor de Netflow capaz da versão 9 do Netflow é exigido. Isto é detalhado dentro

Manual de configuração: Firewall Zona-baseado da política, registro de alta velocidade do Firewall da liberação 3S do Cisco IOS XE (ASR 1000)

Pacote que segue usando a harmonização condicional

Gire sobre condicional debuga a fim permitir o traçado do pacote e permitir então o pacote que segue para estas características:

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

Note: A condição do fósforo pode usar o endereço IP de Um ou Mais Servidores Cisco ICM NT diretamente, porque um ACL não é necessário. Isto combinará como a fonte ou o destino que permitem traços bidirecionais. Este método pode ser usado se não é permitido você alterar a configuração. Por exemplo: debugar o endereço 192.168.1.1/32 do IPv4 da condição da plataforma.

Gire sobre a característica deseguimento:

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

Há duas maneiras de usar esta característica:

1. Incorpore o comando da **gota do rastreamento de pacotes da plataforma debugar** a fim seguir somente os pacotes descartado.

2. A exclusão da **gota do rastreamento de pacotes da plataforma do** comando debug seguirá todo o pacote que combinar a circunstância, que inclui que são inspecionadas/passadas pelo dispositivo.

Gire sobre condicional debuga:

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

Execute o teste, a seguir gire-o debuga fora:

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

Agora a informação pode ser indicada à tela. Neste exemplo, os pacotes ICMP eram deixado cair 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 <num> do pacote do rastreamento de pacotes da plataforma da mostra descodifica o comando descodifica a informação e os índices de cabeçalho de pacote de informação. Esta característica foi introduzida em 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 de informação encaixada

O apoio encaixado da captura de pacote de informação foi adicionado no Cisco IOS XE 3.7 (15.2(4)S). Para mais detalhes, veja

Captura de pacote de informação encaixada para o Cisco IOS e o exemplo de configuração IOS-XE.

Debugs

Condicional debuga

Em XE3.10, condicional debuga será introduzido. As indicações condicionais podem ser usadas a

fim assegurar-se de que os logs da característica ZBFW somente debuguem as mensagens que são relevantes à circunstância. Condicional debuga o uso ACL a fim restringir os logs que combinam os elementos ACL. Também, antes de XE3.10, as mensagens debugar eram mais difíceis de ler. O resultado do debug foi melhorado em XE3.10 para facilitá-lo compreender.

A fim permitir estes debuga, emitem este comando:

```
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
```

Observe que o comando condition deve ser ajustado através de um ACL e de um directionality. O condicional debuga não será executado até ele é começado com o **começo da condição da plataforma do** comando debug. A fim desligar condicional debuga o uso a **parada da condição da plataforma do** comando debug.

```
debug platform condition stop
```

A fim desligar condicional debuga, não usam o comando undebug all. A fim desligar todo o condicional debuga, usam o comando:

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

Antes de XE3.14, o **ha** e o **evento** debugam não são condicionais. Em consequência, **todo do** comando debug da **plataforma da condição da característica fw do dataplane o submode** faz com que todos os logs sejam criados, independente da condição selecionada abaixo. Isto poderia criar o ruído adicional que faz debugar difícil.

Àrevelia, o nível de registro condicional é **informação**. A fim aumentar/diminua o nível do registro, usam o comando:

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

Recolha e a vista debuga

Debugar arquivos não imprimirá ao console ou ao monitor. Tudo debuga é escrito ao disco rígido do ASR. Debugs é escrito ao disco rígido sob os **tracelogs do** dobrador com o nome **cpp_cp_F0-0.log.<date>**. A fim ver o arquivo onde debuga são escritos, usam a saída:

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

Cada um debuga o arquivo será armazenado como um arquivo **cpp_cp_F0-0.log.<date>**. Estes são os arquivos de texto regulares que podem ser copiados fora do ASR com TFTP. O máximo do arquivo de registro no ASR é 1Mb. Após 1Mb, debuga são escritos a um arquivo de registro novo. É por isso cada arquivo de registro é timestamped a fim indicar o começo do arquivo.

Os arquivos de registro puderam existir nestes lugar:

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

Desde que os arquivos de registro são indicados somente depois que são girados, o arquivo de registro pode manualmente ser girado com este comando:

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

Isto cria imediatamente um arquivo de registro do “cpp_cp” e começa 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)
```

Este comando permite que os arquivos debugar sejam fundidos em um arquivo único para um processamento mais fácil. Funde todos os arquivos no diretório e entrelaça-se os baseou no tempo. Isto pode ajudar quando os logs são muito verbosos e são criados através dos arquivos múltiplos:

```
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]
```