ZBFW pour la configuration IOS-XE dépannent le guide

Contenu

Introduction

Ce document décrit comment le meilleur dépannent la caractéristique du Pare-feu basée par zone (ZBFW) sur le routeur de services d'agrégation (ASR) 1000, avec les commandes qui sont utilisées pour voter les compteurs de baisse de matériel sur l'ASR. L'ASR1000 est une plate-forme réalisée par matériel d'expédition. La configuration du logiciel du ® de Cisco IOS XE programme le matériel ASIC (processeur d'écoulement de tranche de temps (QFP) afin d'exécuter des fonctionnalités d'expédition de caractéristique. Ceci tient compte du haut débit et de la meilleure représentation. L'inconvénient à ceci est qu'il présente un plus grand défi pour dépanner. Les commandes Cisco IOS traditionnelles utilisées pour voter des sessions en cours et des compteurs de baisse par l'intermédiaire du Pare-feu basé sur zone (ZBFW) ne sont plus tout valides que les baisses ne sont plus en logiciel.

Liens et documentation

Références de commandes

- Références de commandes de Routeurs à services d'agrégation de la gamme Cisco ASR 1000
- Références de commandes de Cisco IOS XE 3S

Datapath dépannent des étapes

Afin de dépanner le datapath, vous devez identifier si le trafic est correctement traversé le code ASR et de Cisco IOS XE. La particularité aux fonctionnalités de pare-feu, le dépannage de datapath suit ces étapes :

1. **Vérifiez la configuration** - Recueillez la configuration et examinez la sortie afin de vérifier la connexion.

2. **Vérifiez l'état de connexion** - Si le trafic passe correctement, le Cisco IOS XE ouvrent une connexion sur la caractéristique ZBFW. Cette connexion dépiste les informations du trafic et d'état entre un client et serveur.

3. **Vérifiez les compteurs de baisse** - Quand le trafic ne passe pas correctement, le Cisco IOS XE se connecte une baisse contre- pour tous les paquets relâchés. Vérifiez cette sortie afin d'isoler la cause de la panne du trafic.

4. **Se connecter** - Syslog de rassemblement afin de fournir des informations plus granulaires sur des constructions et des pertes de paquets de connexion.

5. **Paquets lâchés par tracé de paquets** - Suivi de paquet d'utilisation afin d'attraper les paquets relâchés.

6. **Debugs** - Le rassemblement met au point est l'option la plus bavarde. Des debugs peuvent être obtenus conditionnellement afin de confirmer le chemin de transfert précis pour les paquets.

Vérifiez la configuration

La sortie du **Pare-feu de support technique d'exposition** est récapitulée ici :

```
-------- 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> --------
```

Vérifiez l'état de connexion

Les informations de connexion peuvent être obtenues de sorte que toutes les connexions sur ZBFW soient répertoriées. Sélectionnez cette commande :

```
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]
```

Il affiche une connexion de telnet de TCP de 14.38.112.250 à 14.36.1.206.

> Remarque: Rendez-vous compte que si vous exécutez cette commande, cela prendra un longtemps s'il y a un bon nombre de connexions sur le périphérique. Cisco recommande que vous exécutiez cette commande avec les filtres spécifiques comme tracé les grandes lignes ici.

La table de connexion peut être filtrée vers le bas à une adresse source ou de destination spécifique. Filtres d'utilisation après sous-mode de **plate-forme**. Les options de filtrer sont :

```
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>
```

Cette table de connexion est ainsi seulement les connexions filtrées originaires de 14.38.112.250 sont affichées :

```
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]
```

Une fois que la table de connexion est filtrée, les informations de connexion détaillées peuvent être obtenues pour un anlaysis plus complet. Afin d'afficher cette sortie, utilisez le mot clé de **détail**.

```
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
```

Compteurs de baisse de Pare-feu de contrôle

La sortie de compteur de baisse changée pendant le XE 3.9. Avant XE 3.9, les raisons de baisse de Pare-feu étaient très génériques. Après XE 3.9, les raisons de baisse de Pare-feu ont été étendues de devenir plus granulaires.

Afin de vérifier des compteurs de baisse, exécutez deux étapes :

1. Confirmez les compteurs globaux de baisse dans le Cisco IOS XE. Ces compteurs affichent quelle caractéristique a relâché le trafic. Les exemples des caractéristiques incluent le Qualité de service (QoS), Traduction d'adresses de réseau (NAT), Pare-feu, et ainsi de suite.

2. Une fois que le subfeature a été identifié, questionnez les compteurs granulaires de baisse offerts par le subfeature. De ce guide, le subfeature étant analysé est la fonctionnalité de pare-feu.

Compteurs globaux de baisse sur QFP

La commande de base de compter en fonction fournit toutes les baisses à travers le QFP :

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

Cette commande montre vous les baisses génériques globalement à travers le QFP. Ces baisses peuvent être sur n'importe quelle caractéristique. Quelques caractéristiques d'exemple sont :

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

Afin de voir toutes les baisses, incluez les compteurs qui ont une valeur de zéro, utilisent la commande :

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

Afin d'effacer les compteurs, utilisez cette commande. Il efface la sortie après l'avoir affichée à l'écran. Cette commande est claire sur lu, ainsi la sortie est remise à zéro **après qu'**elle soit affichée à l'écran.

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

Est ci-dessous une liste de compteurs et d'explication globaux de baisse de Pare-feu QFP :

Raison globale de baisse de Pare-feu	Explication
FirewallBackpressure	Perte de paquets due à la contre-pression en se connectant le mécanisme.

FirewallInvalidZone	Aucune zone de Sécurité configurée pour l'interface.
FirewallL4Insp	Panne de contrôle de la stratégie L4. Voyez la table ci-dessous pour des raisons plus granulaires de baisse (la baisse de fonctionnalité de pare-feu raisonne).
FirewallNoForwardingZone	Le Pare-feu est uninitialized, et aucun trafic n'est permis pour passer.
FirewallNonsession	La création de session échoue. Il pourrait être dû à la limite maximum de session a atteint ou défaillance d'allocation de mémoire.
FirewallPolicy	La stratégie configurée de Pare-feu est baisse.
FirewallL4	Panne de l'inspection L4. Voyez la table ci-dessous pour des raisons plus granulaires de baisse (la baisse de fonctionnalité de pare-feu raisonne).
FirewallL7	Perte de paquets due à l'inspection L7. Voir ci-dessous pour une liste des raisons plus granulaires de la baisse L7 (la baisse de fonctionnalité de pare-fe raisonne).
FirewallNotInitiator	Pas un demandeur de session pour le TCP, l'UDP, ou l'ICMP. Aucune sessio n'est créée. Par exemple, parce que ICMP le premier paquet reçu n'est pas ÉCHO ou HORODATEUR. Pour le TCP, ce n'est pas une synchronisation. Ceci a pu se produire dans le traitement de paquets normal ou le traitement imprécis de canal.
FirewallNoNewSession	La Haute disponibilité de Pare-feu ne permet pas de nouvelles sessions.
FirewallSyncookieMaxDst	Afin d'assurer la protection contre l'inondation SYN gérée par le système central, il y a un débit de synchronisation de par-destination car limite d'inondation de synchronisation. Quand le nombre d'entrées de destination atteint la limite, de nouveaux paquets de synchronisation sont lâchés.
FirewallSyncookie	La logique SYNCOOLIE est déclenchée. Ceci indique que SYN/ACK avec le Témoin de synchronisation a été envoyé, et le paquet d'origine de synchronisation est lâché.
FirewallARStandby	Le routage asymétrique n'est pas activé et le redundancy group n'est pas da l'état active.

Compteurs de baisse de fonctionnalité de pare-feu sur QFP

La limite avec le compteur global de baisse QFP est qu'il n'y a aucune finesse dans les raisons de baisse, et certaines des raisons de baisse telles que **FirewallL4** obtiennent ainsi ont surchargé au point qu'elles sont peu utile pour le dépannage. Ceci a été depuis amélioré dans le Cisco IOS XE 3.9 (15.3(2)S), où des compteurs de baisse de fonctionnalité de pare-feu ont été ajoutés. Ceci donne un ensemble beaucoup plus granulaire de raisons de baisse :

```
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
....
```

Est ci-dessous une liste de raisons et d'explications de baisse de fonctionnalité de pare-feu :

Raison de baisse de fonctionnalité de pare-feu	Explication
Longueur d'en-tête non valide	Le datagramme est en-tête tellement petite qu'il ne pourrait pas contenir la couche 4TCP,UDP, ou d'ICMP. Il pourrait sont provoqué par par : 1. Longueur d'en-tête de TCP < 20

	2. Longueur d'en-tête UDP/ICMP < 8
Longueur des données non valide d'UDP	La longueur de datagramme UDP n'apparie pas la longueur spécifiée dans l'en-tête d'U
Nombre non valide ACK	Cette baisse pourrait sont provoqué par par une de ces raisons : 1. Les égaux ACK pas au next_seq# du TCP scrutent. 2. L'ACK est plus grand que le SEQ# le plus récent envoyé par le pair de TCP.
Indicateur ACK non valide	Dans l'état du TCP SYNSENT et SYNRCVD, c'est prévu l'ACK# est égal à ISN+1 mais n'est pas. Cette baisse pourrait sont provoqué par par une de ces raisons : 1. Attendant l'indicateur ACK mais non réglé dans l'état différent de TCP. 2. Autre que l'indicateur ACK, autre indicateur (comme RST) est également placé.
Demandeur non valide de TCP	Ceci se produit quand : 1. Le premier paquet d'un demandeur de TCP n'est pas une synchronisation (le segu de TCP de Non-initiale est reçu sans session valide). 2. Le paquet initial de synchronisation a l'indicateur ACK réglé.
synchronisation avec des données	Le paquet de synchronisation contient la charge utile. Ceci n'est pas pris en charge.
Indicateurs non valides de TCP	Les indicateurs non valides de TCP mettent en boîte sont provoqué par par : 1. Le TCP parafent le paquet de synchronisation a des indicateurs autres que la synchronisation. 2. Dans le TCP écoutent l'état, un pair de TCP reçoit un RST ou un ACK. 3. Le paquet de l'autre responder est reçu avant SYN/ACK. 4. SYN/ACK prévu n'est pas reçu du responder.
Segment non valide dans l'état SYNSENT	Un segment de TCP non valide dans l'état SYNSENT est provoqué par par : 1. SYN/ACK a la charge utile. 2. SYN/ACK a d'autres indicateurs (PSH, URG, FIN) réglés. 3. Recevez une synchronisation de transit avec la charge utile. 4. Recevez un paquet de non-synchronisation du demandeur.
Segment non valide dans l'état SYNRCVD	Un segment de TCP non valide dans l'état SYNRCVD pourrait sont provoqué par par : 1. Recevez une synchronisation de retransit avec la charge utile du demandeur. 2. Recevez un segment non valide qui n'est pas SYN/ACK, RST, ou FIN du respond
SEQ non valide	Ceci se produit dans l'état SYNRCVD quand les segments provient le demandeur. Il es provoqué par par : 1. Seq# est moins que l'ISN. 2. Si la taille de la fenêtre de rcvd de récepteur est 0 et : Le segment a la charge utile, ou Segment en panne (le seq# est plus grand que le récepteur LASTACK. 3. Si la taille de la fenêtre de rcvd de récepteur est 0 et le seq# tombe au delà de la fenêtre. 4. Égaux de Seq# à l'ISN mais pas à un paquet de synchronisation.
Option non valide d'échelle de fenêtre	L'option non valide d'échelle de fenêtre de TCP est provoqué par par la longueur incor d'octet d'option d'échelle de fenêtre.
TCP hors de fenêtre	Le paquet est trop vieux - une fenêtre derrière l'autre ACK de côté. Ceci a pu se produi dans l'état ÉTABLI, CLOSEWAIT et LASTACK.
Charge utile supplémentaire	Charge utile reçue après la FIN envoyée. Ceci a pu se produire dans l'état CLOSEWAI

de TCP après la FIN envoyée	
Dépassement de fenêtre de TCP	Ceci se produit quand la fenêtre de segment de taille du récepteur entrant de dépasser Cependant, si le vTCP est activé, on permet cette condition parce que le Pare-feu doit mettre en mémoire tampon le segment pour qu'ALG consomme plus tard.
Retran avec les indicateurs non valides	Un paquet retransmis a été déjà reconnu par le récepteur.
Segment en panne de TCP	Le paquet en panne est sur le point d'être livrée à L7 pour l'inspection. Si L7 ne permet le segment OOO, ce paquet sera lâché.
Inondation de synchronisation	Sous une attaque par inondation SYN de TCP. Dans certaines conditions quand les connexions en cours à cet hôte dépasse la valeur entrouverte configurée le Pare-feu rejettera toutes les nouvelles connexions à cette adresse IP pendant une période. En conséquence les paquets seront lâchés.
Interne errez - l'alloc de contrôle de synflood a manqué	Pendant le contrôle de synflood, l'allocation du hostdb échoue. Action recommandée : vérifiez « la mémoire active de Pare-feu de caractéristique de qf matériel de show platform » pour vérifier l'état de mémoire.
Baisse d'arrêt total de Synflood	Si des connexions semi-duplex configurées est dépassées et temps d'arrêt total est configuré, toute la nouvelle connexion à cette adresse IP sont abandonnées.
La limite entrouverte de session dépassent	En raison relâché par paquet des sessions entrouvertes permises dépassées. Vérifiez également les configurations « de haut-bas max-incomplete » et le « one-minut haut-bas » pour s'assurer # des sessions entrouvertes ne sont pas étranglés par ces configurations.
Trop de paquet par écoulement	Le nombre maximal de paquets inspectable permis par écoulement est dépassé. Le no maximum est 25.
Trop de paquets d'erreurs d'ICMP par écoulement	Le nombre maximal de paquets d'erreurs d'ICMP permis par écoulement est dépassé. nombre maximal est 3.
Charge utile de TCP d'Unexpect de Rsp à Init	Dans l'état SYNRCVD, le TCP reçoit un paquet avec la charge utile du responder à la direction de demandeur.
Erreur interne - Direction non définie	Direction de paquet éliminée.
synchronisation à l'intérieur de fenêtre en cours	Un paquet de synchronisation est vu dans la fenêtre d'une connexion TCP déjà établie.
RST à l'intérieur de fenêtre en cours	On observe un paquet RST dans la fenêtre d'une connexion TCP déjà établie.
Segment égaré	On reçoit un segment de TCP qui ne devrait pas avoir été reçu par l'ordinateur d'état de tel qu'un paquet de synchronisation de TCP étant reçu dans l'état d'écoute du responde
Erreur interne d'ICMP - ICMP manqué les informations NAT	Le paquet d'ICMP nat'ed mais les informations NAT internes manquent. C'est une erreu interne.
Le paquet d'ICMP dans SCB ferment l'état	A reçu un paquet d'ICMP dans l'état ÉTROIT SCB.
En-tête IP	En-tête IP manquante en paquet d'ICMP.

manquée en paquet d'ICMP	
Erreur d'ICMP aucun IP ou ICMP	Paquet d'erreurs d'ICMP sans IP ou ICMP en charge utile. Entraîné probablement par u paquet mal formé ou une attaque.
L'ICMP errent paquet trop court	Le paquet d'erreurs d'ICMP est trop court.
L'ICMP errent dépassent la limite de rafale	Le paquet d'erreur d'ICMP dépasse la limite de rafale de 10.
L'ICMP errent inaccessible	Le paquet d'erreur d'ICMP inaccessible dépassent la limite. Seulement on permet au le paquet inaccessible pour traverser.
L'ICMP errent Seq# non valide	Seq# de paquet encastré n'apparie pas le seq# du paquet qui lance l'erreur d'ICMP.
L'ICMP errent ACK non valide	L'ACK non valide dans l'erreur d'ICMP a encastré le paquet.
Baisse d'action d'ICMP	L'action configurée d'ICMP est baisse.
Zone-paire sans policy-map	Stratégie non actuelle sur le zone-paire. il pourrait être dû à ALG (passerelle de couche application) n'étant pas configuré pour ouvrir le trou d'épingle pour le canal de données applications, ou ALG n'a pas ouvert le trou d'épingle correctement, ou aucun trou d'épin n'est dû ouvert aux problèmes d'évolutivité.
Session manquée et stratégie non actuelle	La consultation de session a manqué et aucune stratégie n'est présente pour examiner paquet.
Erreur et stratégie d'ICMP non actuelles	Erreur d'ICMP sans la stratégie configurée sur le zone-paire.
La classification a manqué	Manque de classification dans une paire donnée de zone quand essais de Pare-feu de déterminer si le protocole est inspectable.
Baisse d'action de classification	L'action de classification est baisse.
Stratégie de sécurité Misconfig	Classification défectueuse due à la mauvaise configuration de stratégie de sécurité. Ce pu également être dû à aucun pinpole pour la voie de transmission de données L7.
Envoyez RST au responder	Envoyez RST au responder dans l'état SYNSENT quand ACK# n'est pas égal à ISN+1.
Baisse de stratégie de Pare-feu	L'action de stratégie est de relâcher.
Baisse de fragment	Relâchez les fragments demeurants quand le premier fragment est abandonné.
Baisse de stratégie de Firwall d'ICMP	L'action de stratégie du paquet encastré par ICMP est BAISSE.
L'inspection L7 renvoie la BAISSE	L7 (ALG) décide de relâcher le paquet. La raison a pu être trouvée des statistiques différentes ALG.
Paquet du segment L7 ne pas laisser	Paquet segmenté reçu quand ALG ne l'honore pas.

Paquet du fragment L7 ne pas laisser	(Ou VFR) paquets fragmentés reçus quand ALG ne l'honore pas.
Type L7 Proto inconnu	Type de protocole non reconnu.

Dépannez les baisses de Pare-feu

Une fois que la raison de baisse est identifiée des compteurs ci-dessus globaux ou de fonctionnalité de pare-feu de baisse, les étapes de dépannage supplémentaires pourraient être nécessaires si ces baisses sont inattendues. Indépendamment de la validation de configuration afin d'assurer la configuration est correct pour les fonctionnalités de Pare-feu activées, on l'exige souvent pour prendre des captures de paquet pour la circulation en question pour voir si les paquets sont mal formés ou s'il y a des questions d'implémentation de protocole ou d'application.

Se connecter

L'ASR se connectant la fonctionnalité génère des Syslog afin d'enregistrer les paquets tombés. Ces Syslog fournissent plus de détails sur pourquoi le paquet a été lâché. Il y a deux types de sysloggings :

1. Syslogging mis en mémoire tampon par gens du pays
2. Se connecter distant de grande vitesse

Syslogging mis en mémoire tampon par gens du pays

Afin d'isoler la cause des baisses, vous pouvez utiliser le dépannage générique ZBFW, tel qu'activer des baisses de log. Il y a deux manières de configurer se connecter de perte de paquets.

Méthode 1 : Employez le parameter-map examiner-global afin de se connecter tous les paquets relâchés.

```
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
....
```

Méthode 2 : La coutume d'utilisation examinent le parameter-map afin de se connecter les paquets abandonnés pour seulement la classe spécifique.

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

Ces messages sont envoyés au log ou à la console selon la façon dont l'ASR est configuré pour se connecter. Voici un exemple d'un message de log de baisse.

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

Limites de Syslogging mis en mémoire tampon par gens du pays

1. Ces logs sont débit limité selon l'ID de bogue Cisco CSCud09943.

2. Ces logs ne pourraient pas imprimer à moins que la configuration spécifique soit appliquée. Par exemple, les paquets lâchés par des paquets de classe-par défaut pas sont enregistré à moins que le **mot clé de journal** soit spécifié :

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

Se connecter distant de grande vitesse

La grande vitesse se connectant (HSL) génère des Syslog directement du QFP et les envoie au collecteur configuré du NetFlow HSL. C'est la solution se connectante recommandée pour ZBFW sur l'ASR.

Pour HSL, utilisez cette configuration :

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

Afin d'utiliser cette configuration, un collecteur de NetFlow capable de la version 9 de NetFlow est exigé. Ceci est détaillé dedans

Guide de configuration : Pare-feu basé sur zone de stratégie, se connecter ultra-rapide de Pare-feu de la release 3S (ASR 1000) de Cisco IOS XE

Suivi de paquet utilisant apparier conditionnel

Activez conditionnel met au point afin d'activer le suivi de paquet et puis activer le suivi de paquet pour ces caractéristiques :

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

> Remarque: L'état de correspondance peut utiliser l'adresse IP directement, car un ACL n'est pas nécessaire. Ceci s'assortira comme source ou destination qui tiennent compte des suivis bidirectionnels. Cette méthode peut être utilisée si on ne te permet pas pour modifier la configuration. Exemple : mettez au point l'ipv4 addres 192.168.1.1/32 d'état de plate-forme.

Activez la caractéristique de paquet-suivi :

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

Il y a deux manières d'utiliser cette caractéristique :

1. Sélectionnez la commande de **baisse de tracé de paquets de plate-forme de débogage** afin de tracer seulement les paquets relâchés.

2. L'exclusion de la commande **mettent au point la baisse de tracé de paquets de plate-forme** tracera n'importe quel paquet qui apparie la condition, qui inclut ceux qui sont examinés/passés par le périphérique.

Activez conditionnel met au point :

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

Exécutez le test, puis l'arrêtez met au point :

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

Maintenant les informations peuvent être affichées à l'écran. Dans cet exemple, les paquets d'ICMP étaient dus lâché à une stratégie de Pare-feu :

```
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
```

Le <num> de paquet de tracé de paquets de show platform décodent la commande décode les informations d'en-tête et le contenu de paquet. Cette caractéristique a été introduite dans 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
```

Capture incluse de paquet

Le support inclus de capture de paquet a été ajouté dans le Cisco IOS XE 3.7 (15.2(4)S). Pour plus de détails, voyez

Capture incluse de paquet pour l'exemple de Cisco IOS et de configuration IOS-XE.

Debugs

Debugs conditionnels

Dans XE3.10, conditionnel met au point sera introduit. Des déclarations conditionnelles peuvent être utilisées afin d'assurer les messages de débogage de logs de caractéristique ZBFW seulement qui sont appropriés à la condition. Conditionnel met au point l'utilisation ACLs afin de limiter les logs qui apparient les éléments d'ACL. En outre, avant XE3.10, il était plus difficile lire les messages de débogage. La sortie de débogage a été améliorée dans XE3.10 pour les faciliter pour comprendre.

Afin d'activer ces derniers met au point, émet cette commande :

```
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
```

Notez que la commande de condition doit être placée par l'intermédiaire d'un ACL et d'une directionnalité. Le conditionnel met au point ne sera pas mis en application avant elles est commencé par la commande **met au point le début d'état de plate-forme**. Afin d'arrêter

conditionnel met au point l'utilisation que la commande **mettent au point l'arrêt d'état de plate-forme**.

```
debug platform condition stop
```

Afin d'arrêter conditionnel met au point, n'utilise pas la commande **undebug all**. Afin d'arrêter tout le conditionnel met au point, utilise la commande :

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

Avant XE3.14, l'**ha** et l'**événement** met au point ne sont pas conditionnels. En conséquence, la commande **mettent au point le sous-mode de dataplane de la caractéristique FW d'état de plate-forme toutes les** causes tous les logs à créer, indépendant de l'état sélectionné ci-dessous. Ceci pourrait créer le bruit supplémentaire qui rend le débogage difficile.

Par défaut, le niveau se connectant conditionnel est les **informations**. Afin d'augmenter/diminuez le niveau de se connecter, utilisent la commande :

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

Debugs de rassemblement et de vue

Les fichiers de debug n'imprimeront pas à la console ou au moniteur. Tout met au point est écrit au disque dur de l'ASR. Des debugs sont écrits au disque dur sous les **tracelogs de** répertoire avec le nom **cpp_cp_F0-0.log.<date>**. Afin de visualiser le fichier où met au point sont écrits, utilisent la sortie :

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

Chacun met au point le fichier sera enregistré comme fichier **cpp_cp_F0-0.log.<date>**. Ce sont des fichiers texte réguliers qui peuvent être copiés outre de l'ASR avec le TFTP. Le maximum de fichier journal sur l'ASR est 1Mb. Après 1Mb, met au point sont écrits à un nouveau fichier journal. C'est pourquoi chaque fichier journal est horodaté afin d'indiquer le début du fichier.

Les fichiers journal pourraient exister dans ces emplacements :

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

Puisque des fichiers journal sont seulement affichés après qu'ils soient tournés, le fichier journal peut être manuellement tourné avec cette commande :

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

Ceci crée immédiatement un fichier journal de « cpp_cp » et commence un neuf sur le QFP. Exemple :

```
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)
```

Cette commande permet les fichiers de débogage à fusionner dans un fichier unique pour un traitement plus facile. Il fusionne tous les fichiers dans le répertoire et les entrelace a basé à

l'heure. Ceci peut aider quand les logs sont très bavards et sont créés à travers des plusieurs fichiers :

```
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]
```