Guide de dépannage de ZBFW pour IOS-XE

Contenu

Introduction

Ce document décrit comment dépanner au mieux la fonctionnalité ZBFW (Zone Based Firewall) sur le routeur ASR 1000, avec des commandes utilisées pour interroger les compteurs de pertes matérielles sur l'ASR. L'ASR1000 est une plate-forme de transfert matérielle. La configuration logicielle de Cisco IOS-XE® programme les ASIC matériels (QFP) afin d'exécuter des fonctionnalités de transfert de fonctionnalité. Cela permet un débit plus élevé et de meilleures performances. L'inconvénient est qu'il représente un plus grand défi à résoudre. Les commandes Cisco IOS traditionnelles utilisées pour interroger les sessions en cours et les compteurs de perte via le pare-feu basé sur une zone (ZBFW) ne sont plus valides car les pertes ne sont plus dans le logiciel.

Liens et documentation

Références des commandes

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

Étapes de dépannage du chemin de données

Afin de dépanner le chemin de données, vous devez identifier si le trafic est correctement transmis par le code ASR et Cisco IOS-XE. Spécifique aux fonctions de pare-feu, le dépannage de la couche de données suit les étapes suivantes :

1. **Verify Configuration** - Recueillez la configuration et examinez le résultat afin de vérifier la connexion.

2. **Vérifier l'état de la connexion** - Si le trafic passe correctement, Cisco IOS-XE ouvre une connexion sur la fonctionnalité ZBFW. Cette connexion suit le trafic et les informations d'état entre un client et un serveur.

3. **Vérifier les compteurs de perte** - Lorsque le trafic ne passe pas correctement, Cisco IOS-XE enregistre un compteur de perte pour tous les paquets abandonnés. Vérifiez ce résultat afin d'isoler la cause de la défaillance du trafic.

4. **Journalisation** - Recueillez des syslogs afin de fournir des informations plus précises sur les builds de connexion et les abandons de paquets.

5. **Packet Trace Dropping Packets** - Utilisez le suivi des paquets afin d'attraper les paquets abandonnés.

6. **Débogues** - Rassembler les débogages est l'option la plus explicite. Les débogages peuvent être obtenus sous condition afin de confirmer le chemin exact de transfert des paquets.

Vérifier la configuration

Le résultat de **show tech support firewall** est résumé 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> --------
```

Vérifier l'état de la connexion

Les informations de connexion peuvent être obtenues afin que toutes les connexions sur ZBFW soient répertoriées. Entrez 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]
```

Elle montre une connexion Telnet TCP de 14.38.112.250 à 14.36.1.206.

> **Note**: Sachez que si vous exécutez cette commande, il faudra beaucoup de temps s'il y a beaucoup de connexions sur le périphérique. Cisco vous recommande d'exécuter cette commande avec des filtres spécifiques comme indiqué ici.

La table de connexion peut être filtrée jusqu'à une adresse source ou de destination spécifique. Utilisez des filtres après le sous-mode **plateforme**. Les options à filtrer sont les suivantes :

```
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 filtrée de sorte que seules les connexions provenant 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 la table de connexion filtrée, les informations détaillées de connexion peuvent être obtenues pour une analyse plus complète. Pour afficher ce résultat, utilisez le mot clé **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
```

Vérifier les compteurs de perte de pare-feu

La sortie du compteur de dépôt a changé pendant XE 3.9. Avant XE 3.9, les raisons de perte du pare-feu étaient très génériques. Après XE 3.9, les raisons de perte de pare-feu ont été étendues pour devenir plus granulaires.

Afin de vérifier les compteurs de perte, effectuez deux étapes :

1. Confirmez les compteurs de perte globaux dans Cisco IOS-XE. Ces compteurs indiquent la fonction qui a abandonné le trafic. La qualité de service (QoS), la traduction d'adresses de réseau (NAT), le pare-feu, etc. sont des exemples de fonctionnalités.

2. Une fois la sous-fonction identifiée, recherchez les compteurs de perte granulaires proposés par la sous-fonction. Dans ce guide, la sous-fonctionnalité analysée est la fonction Pare-feu.

Compteurs de pertes globaux sur QFP

La commande de base sur laquelle s'appuyer fournit toutes les pertes sur le QFP :

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

Cette commande vous montre les abandons génériques globalement sur QFP. Ces pertes peuvent être associées à n'importe quelle fonction. Voici quelques exemples de fonctionnalités :

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

Pour afficher toutes les pertes, incluez les compteurs dont la valeur est égale à zéro, utilisez la commande :

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

Pour effacer les compteurs, utilisez cette commande. Il efface le résultat après l'avoir affiché à l'écran. Cette commande est désactivée en lecture, de sorte que la sortie est réinitialisée à zéro **après** qu'elle soit affichée à l'écran.

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

Vous trouverez ci-dessous une liste de compteurs de perte de pare-feu global QFP et une explication :

Motif de suppression globale du pare-feu	Explication
Pare-feuBackpression	Débit de paquets dû à la contre-pression par le mécanisme de journalisation.
ZoneNonPare-Feu	Aucune zone de sécurité configurée pour l'interface.
Pare-feu L4Inspecteur	Échec du contrôle de la stratégie de couche 4. Reportez-vous au tablea ci-dessous pour obtenir des raisons de suppression plus précises (raiso de suppression des fonctionnalités du pare-feu).
ZoneNonTransfertPare-feu	Le pare-feu n'est pas initialisé et aucun trafic n'est autorisé à passer.
FirewallNonsession	La création de session échoue. Cela peut être dû à une limite de sessio maximale atteinte ou à une défaillance d'allocation de mémoire.
StratégiePare-feu	La stratégie de pare-feu configurée est abandonnée.
Pare-feuL4	Échec de l'inspection de couche 4. Reportez-vous au tableau ci-dessou pour obtenir des raisons de suppression plus précises (raisons de suppression de la fonction de pare-feu).
Pare-feuL7	Paquet abandonné en raison de l'inspection L7. Reportez-vous à la liste ci-dessous pour obtenir une liste plus détaillée des raisons de suppress de la couche 7 (raisons de suppression de la fonctionnalité de pare-feu)
Pare-feuPasInitiateur	Pas un initiateur de session pour TCP, UDP ou ICMP. Aucune session n'est créée. Par exemple, pour ICMP, le premier paquet reçu n'est pas ECHO ou TIMESTAMP. Pour TCP, il ne s'agit pas d'un SYN.
Pare-feuAucuneNouvelleSession	Cela peut se produire dans le traitement normal des paquets ou dans u traitement de canal imprécis. La haute disponibilité du pare-feu n'autorise pas les nouvelles sessions
FirewallSyncookieMaxDst	Afin de fournir une protection de la propagation SYN basée sur l'hôte, il a un taux SYN par destination comme limite d'inondation SYN. Lorsque nombre d'entrées de destination atteint la limite, de nouveaux paquets SYN sont abandonnés.
FirewallSyncookie	La logique SYNCOOLIE est déclenchée. Cela indique que SYN/ACK av le cookie SYN a été envoyé et que le paquet SYN d'origine est abandonné.
FirewallARStandby	Le routage asymétrique n'est pas activé et le groupe de redondance n' pas actif.

Compteurs de suppression de fonctions de pare-feu sur QFP

La limitation avec le compteur de pertes global QFP est qu'il n'y a pas de granularité dans les raisons de pertes, et certaines des raisons de pertes telles que **FirewallL4** deviennent si surchargées au point qu'elles sont peu utiles pour le dépannage. Cela a depuis été amélioré dans Cisco IOS-XE 3.9 (15.3(2)S), où des compteurs de perte de fonctionnalité de pare-feu ont été ajoutés. Ceci donne un ensemble de raisons de chute beaucoup plus granulaires :

```
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
....
```

Vous trouverez ci-dessous une liste des raisons et des explications de suppression des fonctionnalités de pare-feu :

Motif de suppression des fonctionnalités du pare-feu	Explication
Longueur d'en-tête non valide	Le datagramme est si petit qu'il ne peut pas contenir l'en-tête TCP, UDP ou ICMP de couche 4. Elle peut être causée par : 1. Longueur d'en-tête TCP < 20 2. Longueur d'en-tête UDP/ICMP < 8
Longueur de données UDP non valide	La longueur du datagramme UDP ne correspond pas à la longueur spécifiée dans l'en UDP.
Numéro ACK non valide	Cette baisse peut être due à l'une des raisons suivantes : 1. ACK n'est pas égal au n° suivant_seq de l'homologue TCP. 2. ACK est supérieur au numéro SEQ le plus récent envoyé par l'homologue TCP.
Indicateur ACK non valide	Dans les états TCP SYNSENT et SYNRCVD, ACK# est censé être égal à ISN+1, mais Cette baisse peut être due à l'une des raisons suivantes : 1. Indicateur ACK attendu mais non défini dans un état TCP différent. 2. Outre l'indicateur ACK, un autre indicateur (comme RST) est également défini.
Initiateur TCP non valide	Cela se produit lorsque : 1. Le premier paquet d'un initiateur TCP n'est pas un SYN (le segment TCP non init reçu sans session valide). 2. L'indicateur ACK est défini pour le paquet SYN initial.
SYN avec données	Le paquet SYN contient la charge utile. Ceci n'est pas pris en charge.
Indicateurs TCP non valides	Les indicateurs TCP non valides peuvent être provoqués par : 1. Le paquet SYN initial TCP comporte des indicateurs autres que SYN. 2. Dans l'état d'écoute TCP, un homologue TCP reçoit une RST ou un ACK. 3. Le paquet d'un autre répondeur est reçu avant SYN/ACK. 4. SYN/ACK attendu n'est pas reçu du répondeur.
Segment non valide dans l'état SYNSENT	Un segment TCP non valide dans l'état SYNSENT est causé par : 1. SYN/ACK a une charge utile. 2. SYN/ACK a d'autres indicateurs (PSH, URG, FIN) définis. 3. Recevez un SYN de transit avec la charge utile. 4. Recevez un paquet non SYN de l'initiateur.
Segment non valide dans l'état SYNRCVD	Un segment TCP non valide dans l'état SYNRCVD peut être causé par : 1. Recevez un SYN de retransit avec la charge utile de l'initiateur. 2. Recevez un segment non valide qui n'est pas SYN/ACK, RST ou FIN du répondeu Cela se produit à l'état SYNRCVD lorsque des segments proviennent de l'initiateur. Ell causée par :
SEQ non valide	1. Seq# est inférieur à ISN. 2. Si la taille de la fenêtre du récepteur rcvd est 0 et : Le segment a une charge utile, ou Segment hors commande (le n° séq est supérieur au récepteur LASTACK. 3. Si la taille de la fenêtre du récepteur rcvd est 0 et seq# se situe au-delà de la fené

	4. Seq# est égal à ISN mais pas à un paquet SYN.
Option d'échelle de fenêtre non valide	L'option d'échelle de fenêtre TCP non valide est due à une longueur d'octet d'option d'échelle de fenêtre incorrecte.
TCP hors fenêtre	Le paquet est trop ancien - une fenêtre derrière l'ACK de l'autre côté. Cela pourrait se produire dans les états ESTABLISHED, CLOSEWAIT et LASTACK.
Charge utile supplémentaire TCP après envoi du FIN	Charge utile reçue après l'envoi de FIN. Cela pourrait se produire dans l'état CLOSEW
Débordement de fenêtre TCP	Cela se produit lorsque la taille du segment entrant dépasse la fenêtre du destinataire. Cependant, si vTCP est activé, cette condition est autorisée car le pare-feu doit mettre mémoire tampon le segment pour qu'ALG puisse le consommer ultérieurement.
Retourner avec indicateurs non valides	Un paquet retransmis a déjà été reconnu par le récepteur.
Segment TCP hors service	Le paquet hors commande est sur le point d'être livré à L7 pour inspection. Si L7 n'aut pas le segment OO, ce paquet sera abandonné.
Inondation SYN	Dans le cadre d'une attaque par inondation TCP SYN. Dans certaines conditions, lorsc les connexions actuelles à cet hôte dépassent la valeur semi-ouverte configurée, le pa rejette toute nouvelle connexion à cette adresse IP pendant un certain temps. Par conséquent, les paquets seront abandonnés.
Erreur interne - échec de la vérification de la synchronisation alloc	Lors du contrôle de synchronisation, l'allocation de hostdb échoue. Action recommandée : cochez « show platform hardware qfp active feature firewall me » pour vérifier l'état de la mémoire.
Abandon d'interruption de la synchronisation	Si les connexions semi-ouvertes configurées sont dépassées et que le temps d'arrêt es configuré, toute nouvelle connexion à cette adresse IP est abandonnée.
Limite de session semi-ouverte dépassée	Paquet abandonné en raison du dépassement des sessions semi-ouvertes autorisées. Vérifiez également les paramètres « max-incomplet high/low » et « one minute high/lov pour vous assurer que le nombre de sessions semi-ouvertes n'est pas limité par ces configurations.
Trop de Pkt par flux	Le nombre maximal de paquets inspectables autorisé par flux est dépassé. Le nombre maximal est 25.
Trop de paquets d'erreur ICMP par flux	Le nombre maximal de paquets d'erreur ICMP autorisé par flux est dépassé. Le nombr maximal est 3.
Charge utile TCP inattendue de Rsp à Init	Dans l'état SYNRCVD, TCP reçoit un paquet avec charge utile du répondeur vers l'initi
Erreur interne - Direction non définie	Direction de paquet non définie.
SYN dans la fenêtre active	Un paquet SYN apparaît dans la fenêtre d'une connexion TCP déjà établie.
RST dans la fenêtre actuelle	Un paquet RST est observé dans la fenêtre d'une connexion TCP déjà établie.
Segment d'arrêt	Un segment TCP qui n'aurait pas dû être reçu par l'intermédiaire de la machine d'état T tel qu'un paquet SYN TCP reçu à l'état d'écoute par le répondeur, est reçu.
Erreur interne	Le paquet ICMP n'est pas entré mais les informations NAT internes sont manquantes.

ICMP - Informations NAT	s'agit d'une erreur interne.
ICMP manquantes	
Paquet ICMP en état de fermeture SCB	Réception d'un paquet ICMP dans l'état SCB CLOSE.
En-tête IP manquant dans le paquet ICMP	En-tête IP manquant dans le paquet ICMP.
Erreur ICMP No IP ou ICMP	Paquet d'erreur ICMP sans IP ou ICMP dans la charge utile. Probablement causée par paquet mal formé ou une attaque.
Pkt d'erreur ICMP trop court	Le paquet d'erreur ICMP est trop court.
Err ICMP dépassant la limite de rafale	Le pkt d'erreur ICMP dépasse la limite de rafale de 10.
Erreur ICMP inaccessible	Le pkt d'erreur ICMP inaccessible dépasse la limite. Seul le 1 er paquet inaccessible est autorisé à passer.
Numéro de séquence d'erreur ICMP non valide	Le numéro de séquence du paquet incorporé ne correspond pas au numéro de séquen du paquet qui génère l'erreur ICMP.
Accusé de réception d'erreur ICMP non valide	ACK non valide dans le paquet incorporé Erreur ICMP.
Liste des actions ICMP	L'action ICMP configurée est abandonnée.
Zone-pair sans policy-map	Stratégie non présente sur la paire de zones. cela peut être dû au fait qu'ALG (Applicat Layer Gateway) n'a pas été configuré pour ouvrir le trou de broche pour le canal de données d'application, ou qu'ALG n'a pas ouvert correctement le trou de broche, ou qu'aucun trou de broche n'est ouvert en raison de problèmes d'évolutivité.
Session Manquée Et Stratégie Non Présente	La recherche de session a échoué et aucune stratégie n'est présente pour inspecter ce paquet.
Erreur ICMP et stratégie non présente	Erreur ICMP sans stratégie configurée sur la zone-pair.
Échec de la classification	Échec de classification dans une paire de zones donnée lorsque le pare-feu tente de déterminer si le protocole est inspectable.
Suppression de l'action de classification	L'action de classification est abandonnée.
Erreur de configuration de la stratégie de sécurité	Échec de la classification en raison d'une mauvaise configuration de la stratégie de séc Cela peut également être dû à l'absence de pinpole pour le canal de données L7.
Envoyer la TVD au répondeur	Envoyer la TVD au répondeur dans l'état SYNSENT lorsque ACK# n'est pas égal à ISN
Suppression de la stratégie de	L'action politique est à abandonner.

pare-feu	
Dépose de fragments	Déposez les fragments restants lorsque le premier fragment est supprimé.
Abandon de la stratégie de pare-feu ICMP	L'action de stratégie du paquet intégré ICMP est DROP.
Retours d'inspection L7 DROP	L7 (ALG) décide de supprimer le paquet. La raison en est tirée de différentes statistiqu ALG.
Pkt de segment L7 non autorisé	Paquet segmenté reçu lorsque ALG ne l'honore pas.
Paquet de fragments L7 non autorisé	Réception de paquets fragmentés (ou VFR) lorsque ALG ne l'honore pas.
Type de proto L7 inconnu	Type de protocole non reconnu.

Dépannage des abandons de pare-feu

Une fois que la raison de la perte est identifiée à partir des compteurs de perte de fonctionnalité globale ou de pare-feu ci-dessus, des étapes de dépannage supplémentaires peuvent être nécessaires si ces pertes sont inattendues. Outre la validation de configuration afin de s'assurer que la configuration est correcte pour les fonctionnalités de pare-feu activées, il est souvent nécessaire de prendre des captures de paquets pour le flux de trafic en question pour voir si les paquets sont mal formés ou s'il y a des problèmes de mise en oeuvre de protocole ou d'application.

Journalisation

La fonctionnalité de journalisation ASR génère des syslogs afin d'enregistrer les paquets abandonnés. Ces Syslogs fournissent plus de détails sur les raisons pour lesquelles le paquet a été abandonné. Il existe deux types de slogans :

1. Syslogging en mémoire tampon locale

2. Journalisation à grande vitesse à distance

Syslogging en mémoire tampon locale

Afin d'isoler la cause des pertes, vous pouvez utiliser le dépannage ZBFW générique, comme activer les pertes de journal. Il y a deux façons de configurer la journalisation des pertes de paquets.

Méthode 1 : Utilisez inspect-global paramètres-map afin de consigner tous les paquets abandonnés.

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

Méthode 2 : Utilisez custom inspect paramètre-map afin de consigner les paquets abandonnés

pour une classe spécifique uniquement.

```
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 journal ou à la console selon la configuration de l'ASR pour la journalisation. Voici un exemple de message de journal de suppression.

```
*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
```

Limitations de la journalisation système locale en mémoire tampon

1. Ces journaux sont limités selon l'ID de bogue Cisco CSCud09943.
2. Ces journaux ne peuvent pas être imprimés, sauf si une configuration spécifique est appliquée. Par exemple, les paquets abandonnés par les paquets de classe par défaut ne seront pas consignés, sauf si le mot clé **log** est spécifié :

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

Journalisation à grande vitesse à distance

La journalisation à haut débit (HSL) génère des syslogs directement à partir de QFP et les envoie au collecteur HSL de netflow configuré. Il s'agit de la solution de journalisation recommandée pour ZBFW sur ASR.

Pour HSL, utilisez cette configuration :

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

Pour utiliser cette configuration, un collecteur NetFlow compatible avec Netflow version 9 est requis. Ceci est détaillé dans

Guide de configuration : Pare-feu de stratégie basé sur les zones, journalisation haut débit du pare-feu Cisco IOS XE version 3S (ASR 1000)

Suivi des paquets à l'aide de correspondances conditionnelles

Activez les débogages conditionnels afin d'activer le suivi des paquets, puis activez le suivi des paquets pour ces fonctionnalités :

```
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**: La condition de correspondance peut utiliser l'adresse IP directement, car une liste de contrôle d'accès n'est pas nécessaire. Cela correspond à la source ou à la destination qui autorise les traces bidirectionnelles. Cette méthode peut être utilisée si vous n'êtes pas autorisé à modifier la configuration. Exemple : debug platform condition ipv4 address 192.168.1.1/32.

Activez la fonction de suivi des paquets :

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

Il existe deux façons d'utiliser cette fonction :

1. Entrez la commande **debug platform packet-trace drop** afin de tracer uniquement les paquets abandonnés.

2. L'exclusion de la commande **debug platform packet-trace drop** trace tout paquet qui correspond à la condition, qui inclut ceux qui sont inspectés/transmis par le périphérique.

Activer les débogages conditionnels :

```
debug platform condition start
```

Exécutez le test, puis désactivez les débogages :

```
debug platform condition stop
```

Maintenant, les informations peuvent être affichées à l'écran. Dans cet exemple, les paquets ICMP ont été abandonnés en raison d'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
```

La commande **show platform packet-trace packet <num> decode** décode les informations et le contenu de l'en-tête de paquet. Cette fonctionnalité 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 de paquets intégrée

La prise en charge de la capture de paquets intégrée a été ajoutée dans Cisco IOS-XE 3.7 (15.2(4)S). Pour plus d'informations, reportez-vous à la section

Exemple de configuration de la capture de paquets intégrée pour Cisco IOS et IOS-XE.

Déboguages

Débogues conditionnels

Dans XE3.10, les débogages conditionnels seront introduits. Des instructions conditionnelles peuvent être utilisées afin de s'assurer que la fonctionnalité ZBFW ne consigne que les messages de débogage qui sont pertinents à la condition. Les débogages conditionnels utilisent des listes de contrôle d'accès afin de restreindre les journaux qui correspondent aux éléments de la liste de contrôle d'accès. En outre, avant XE3.10, les messages de débogage étaient plus difficiles à lire. La sortie de débogage a été améliorée dans XE3.10 pour les rendre plus faciles à comprendre.

Afin d'activer ces débogages, émettez cette commande :

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

Notez que la commande condition doit être définie via une liste de contrôle d'accès et une directive. Les débogages conditionnels ne seront pas implémentés tant qu'ils ne seront pas démarrés avec la commande **debug platform condition start**. Afin de désactiver les débogages conditionnels, utilisez la commande **debug platform condition stop**.

```
debug platform condition stop
```

Afin de désactiver les débogages conditionnels, **NE PAS** utiliser la commande **undebug all**. Afin de désactiver tous les débogages conditionnels, utilisez la commande :

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

Avant XE3.14, les débogages **ha** et **event** ne sont pas conditionnels. Par conséquent, la commande **debug platform condition feature fw dataplane submode all** entraîne la création de tous les journaux, indépendamment de la condition sélectionnée ci-dessous. Cela peut créer un bruit supplémentaire qui rend le débogage difficile.

Par défaut, le niveau de journalisation conditionnelle est **info**. Pour augmenter/diminuer le niveau de journalisation, utilisez la commande :

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

Collecte et affichage des débogages

Les fichiers de débogage ne s'impriment pas sur la console ou le moniteur. Tous les débogages sont écrits sur le disque dur de l'ASR. Les débogages sont écrits sur le disque dur sous le dossier **tracelogs** portant le nom **cpp_cp_F0-0.log.<date>**. Pour afficher le fichier dans lequel les débogages sont écrits, utilisez la sortie :

```
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)
```

Chaque fichier de débogage sera stocké en tant que fichier **cpp_cp_F0-0.log.<date>**. Il s'agit de fichiers texte ordinaires qui peuvent être copiés à partir de l'ASR avec TFTP. Le nombre maximal de fichiers journaux sur l'ASR est de 1 Mo. Après 1 Mo, les débogages sont écrits dans un nouveau fichier journal. C'est pourquoi chaque fichier journal est horodaté afin d'indiquer le début du fichier.

Les fichiers journaux peuvent exister dans ces emplacements :

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

Étant donné que les fichiers journaux ne sont affichés qu'après leur rotation, le fichier journal peut être tourné manuellement à l'aide de la commande suivante :

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

Cela crée immédiatement un fichier journal « cpp_cp » et en lance un nouveau 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 de fusionner les fichiers de débogage en un seul fichier pour faciliter le traitement. Il fusionne tous les fichiers du répertoire et les entrelace en fonction du temps. Cela peut aider lorsque les journaux sont très détaillés et sont créés sur 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]
```