

# Dépannage du chemin de données Firepower

## Phase 7 : Politique d'intrusion

### Contenu

[Introduction](#)

[Conditions préalables](#)

[Dépannage de la phase de stratégie d'intrusion](#)

[Utilisation de l'outil « trace » pour détecter les pertes de stratégie d'intrusion \(FTD uniquement\)](#)

[Rechercher les suppressions dans les stratégies d'intrusion](#)

[Créer une stratégie d'intrusion ciblée](#)

[Dépannage faux positif](#)

[Exemple positif réel](#)

[Données à fournir au TAC](#)

[Étapes suivantes](#)

### Introduction

Cet article fait partie d'une série d'articles qui expliquent comment dépanner systématiquement le chemin de données sur les systèmes Firepower pour déterminer si les composants de Firepower peuvent affecter le trafic. Reportez-vous à l'[article Présentation](#) pour obtenir des informations sur l'architecture des plates-formes Firepower et des liens vers les autres articles de dépannage du chemin de données.

Cet article couvre la septième phase du dépannage du chemin de données Firepower, la fonction de stratégie d'intrusion.

### Conditions préalables

- Cet article s'applique à toutes les plates-formes Firepower exécutant une stratégie d'intrusion. La fonctionnalité **trace** n'est disponible que dans les versions 6.2 et ultérieures pour la plate-forme Firepower Threat Defense (FTD).
- Connaissance de l'open source Snort utile, mais pas nécessaire. Pour plus d'informations sur Snort open source, rendez-vous sur <https://www.snort.org/>

### Dépannage de la phase de stratégie d'intrusion

#### Utilisation de l'outil « trace » pour détecter les pertes de stratégie d'intrusion (FTD uniquement)

L'outil de suivi de la prise en charge du système peut être exécuté à partir de l'interface de ligne de commande (CLI) FTD. Ceci est similaire à l'outil **firewall-engine-debug** mentionné dans l'[article](#) de la phase de la stratégie de contrôle d'accès, sauf qu'il creuse plus profondément dans le fonctionnement interne de Snort. Cela peut être utile pour voir si des règles de stratégie d'intrusion

se déclenchent sur le trafic intéressant.

Dans l'exemple ci-dessous, le trafic de l'hôte avec l'adresse IP 192.168.62.6 est bloqué par une règle de stratégie d'intrusion (dans ce cas, 1:23111)

```
> system support trace

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.69
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages

[... output omitted for brevity]

173.37.145.84-80 - 192.168.62.69-38488 6 Packet: TCP, ACK, seq 3594105349, ack 3856774965
173.37.145.84-80 - 192.168.62.69-38488 6 ApplID: service HTTP (676), application Cisco (2655)
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 | 0 URL SI: ShmDBLookupURL("http://www.cisco.com/<?php") returned 0
...
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 | 0 match rule order 5, 'inspect it all', action Allow
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 | 0 allow action
192.168.62.69-38488 > 173.37.145.84-80 6 Firewall: allow rule, 'inspect it all', allow
192.168.62.69-38488 > 173.37.145.84-80 6 IPS Event: gid 1, sid 23111, drop
192.168.62.69-38488 > 173.37.145.84-80 6 Snort detect_drop: gid 1, sid 23111, drop
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 | 0 Deleting session
192.168.62.69-38488 > 173.37.145.84-80 6 NAP id 1, IPS id 0, Verdict BLACKLIST
192.168.62.69-38488 > 173.37.145.84-80 6 ==>> Blocked by IPS
Verdict reason is sent to DAQ's PDTs
```

Notez que l'action appliquée par snort a été **abandonnée**. Lorsqu'une goutte est détectée par snort, cette session particulière est alors mise sur liste noire afin que tous les paquets supplémentaires soient également abandonnés.

La raison pour laquelle snort est capable d'exécuter l'action **drop** est que l'option « Drop when Inline » est activée dans la stratégie d'intrusion. Ceci peut être vérifié dans la page de renvoi initiale de la politique d'intrusion. Dans Firepower Management Center (FMC), accédez à **Politiques > Contrôle d'accès > Intrusion** et cliquez sur l'icône de modification en regard de la stratégie en question.

The screenshot shows the 'Policy Information' page for 'My Intrusion Policy'. The 'Drop when Inline' checkbox is checked. An orange arrow points to it with the text 'Uncheck this box to disable Drop when Inline'. Below is a table of intrusion events:

Inline Result	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Message
↓	192.168.62.69	173.37.145.84	38494 / tcp	80 (http) / tcp	POLICY-OTHER PHP uri taq injection attempt (1:23111:10)
↓	192.168.62.69	173.37.145.84	38488 / tcp	80 (http) / tcp	POLICY-OTHER PHP uri taq injection attempt (1:23111:10)

Annotations for the table:

- Drop when Inline disabled = "Would have dropped" Inline Result (points to the first row)
- Drop when Inline enabled = "Dropped" Inline Result (points to the second row)

Si « Drop When Inline » est désactivé, snort n'abandonne plus les paquets offensants, mais il alerte toujours avec un **résultat Inline** de « Aurait abandonné » dans les événements Intrusion.

Lorsque la commande « Drop When Inline » est désactivée, le résultat de la commande trace indique une action **drop** pour la session de trafic en question.

```
> system support trace

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.69
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages

[... output omitted for brevity]

173.37.145.84-80 - 192.168.62.69-38494 6 Packet: TCP, ACK, seq 2900935719, ack 691924600
173.37.145.84-80 - 192.168.62.69-38494 6 AppID: service HTTP (676), application Cisco (2655)
...
192.168.62.69-38494 > 173.37.145.84-80 6 AS 1 | 0 match rule order 5, 'inspect it all', action Allow
192.168.62.69-38494 > 173.37.145.84-80 6 AS 1 | 0 allow action
192.168.62.69-38494 > 173.37.145.84-80 6 Firewall: allow rule, 'inspect it all', allow
192.168.62.69-38494 > 173.37.145.84-80 6 IPS Event: gid 1, sid 23111, would drop
192.168.62.69-38494 > 173.37.145.84-80 6 Snort detect_drop: gid 1, sid 23111, would drop
192.168.62.69-38494 > 173.37.145.84-80 6 NAP id 1, IPS id 0, Verdict PASS
192.168.62.69-38494 > 173.37.145.84-80 6 ====> Blocked by IPS
Verdict reason is sent to DAQ's PDTS
```

## Rechercher les suppressions dans les stratégies d'intrusion

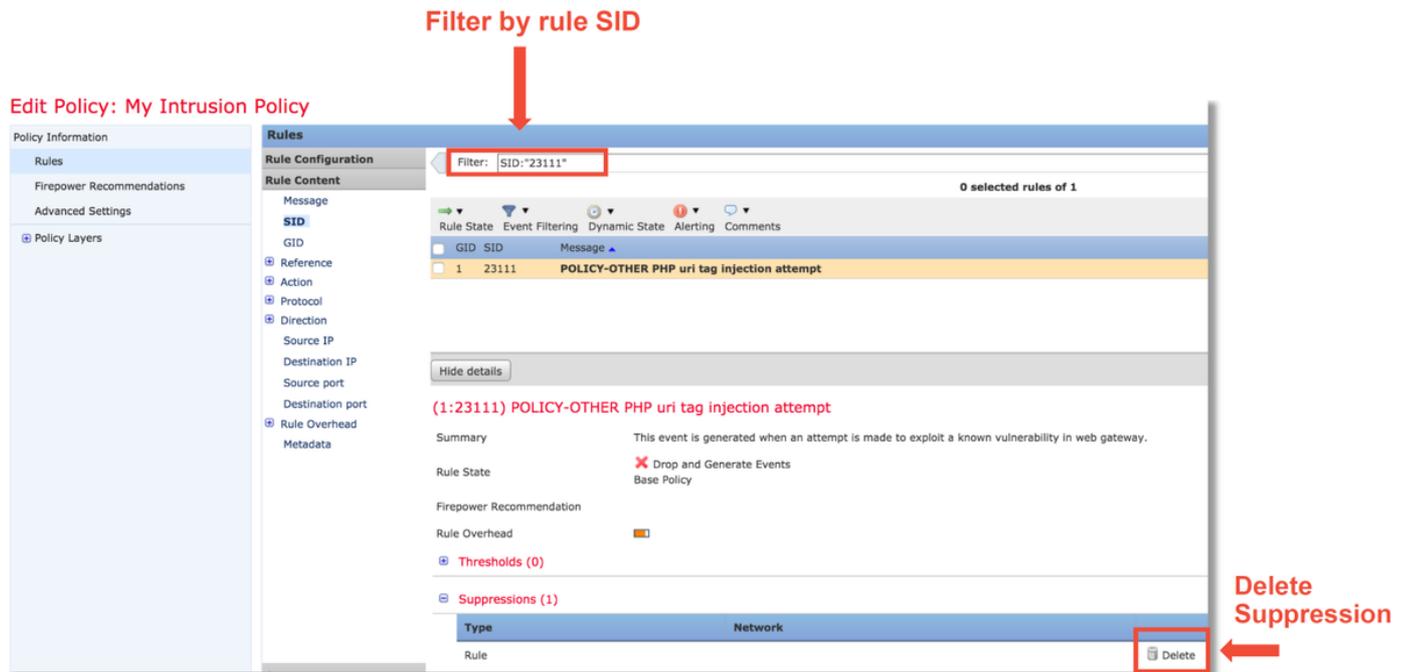
Il est possible de supprimer le trafic sans envoyer d'événements d'intrusion au FMC (abandon silencieux). Pour ce faire, vous devez configurer **les suppressions**. Afin de vérifier si une suppression a été configurée dans une stratégie d'intrusion, l'interpréteur de commandes expert peut être vérifié sur le serveur principal, comme illustré ci-dessous.

```
[ Look for suppressions ]
> expert
$ cd /var/sf/detection_engines/*
$ grep -H '^suppress' intrusion/*snort_suppression.conf
intrusion/68acdfa2-e31a-11e6-b866-dd9e65c01d56/snort_suppression.conf:suppress gen_id 1, sig_id 23111

[ Get the policy name ]
$ grep Name intrusion/snort.conf.68acdfa2-e31a-11e6-b866-dd9e65c01d56
# Name      : My Intrusion Policy
```

Notez que la stratégie d'intrusion appelée « Ma stratégie d'intrusion » contient une suppression pour la règle 1:2311. Par conséquent, le trafic peut être abandonné en raison de cette règle, sans aucun événement. C'est une autre raison pour laquelle l'utilitaire de suivi peut être utile, car il montre toujours les pertes qui se produisent.

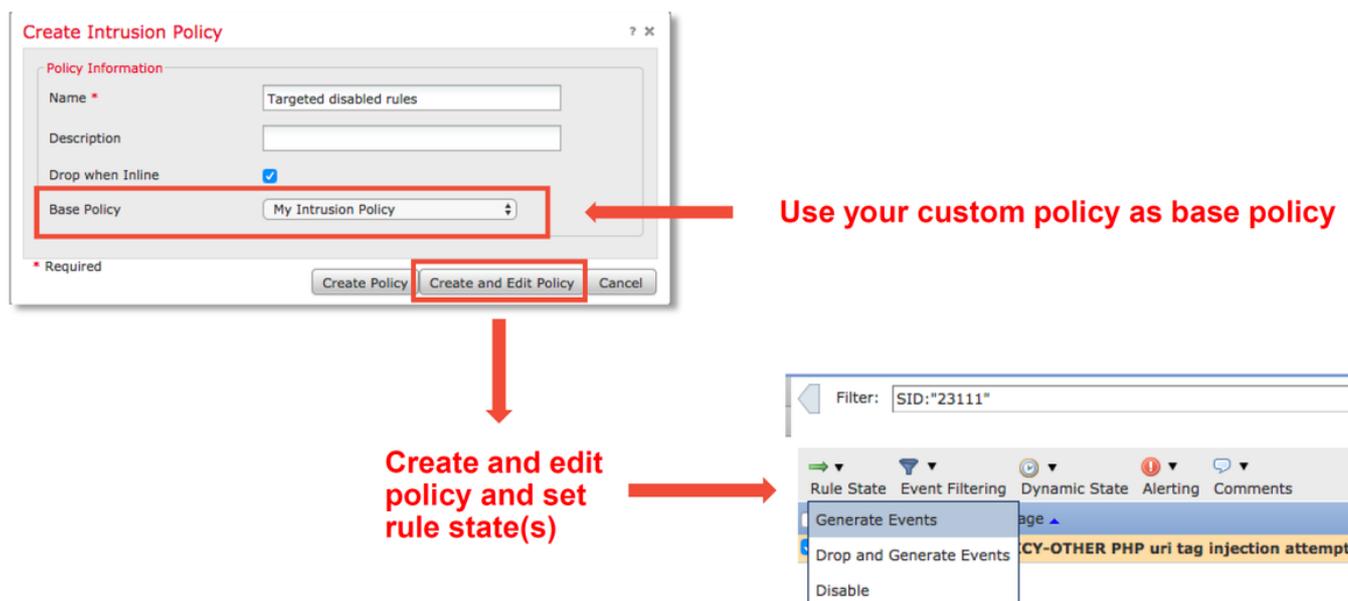
Afin de supprimer la suppression, la règle en question peut être filtrée dans la vue **Règles** de stratégie d'intrusion. Ceci ouvre une option pour supprimer la suppression, comme indiqué ci-dessous.



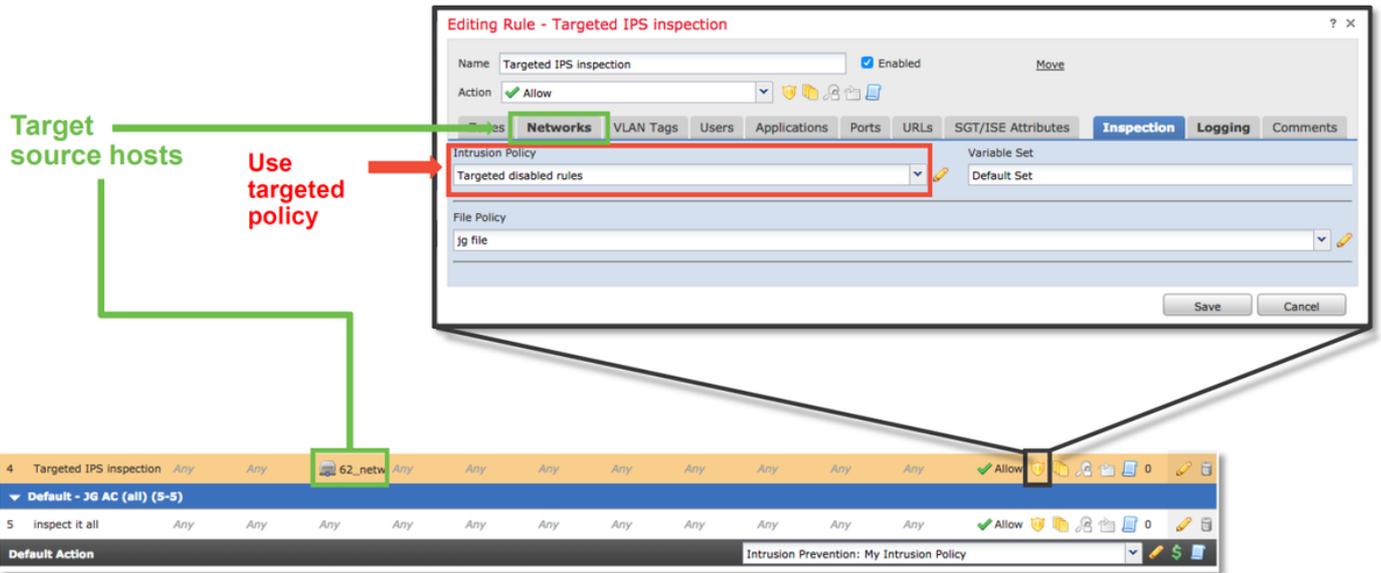
## Créer une stratégie d'intrusion ciblée

Si le trafic est abandonné par une règle de stratégie d'intrusion particulière, vous pouvez ne pas vouloir supprimer le trafic en question, mais vous pouvez également ne pas vouloir désactiver la règle. La solution consiste à créer une nouvelle stratégie d'intrusion avec la ou les règles incriminées désactivées, puis à lui demander d'évaluer le trafic provenant des hôtes cibles.

Voici une illustration de la création de la nouvelle stratégie d'intrusion (sous **Politiques > Contrôle d'accès > Intrusion**).



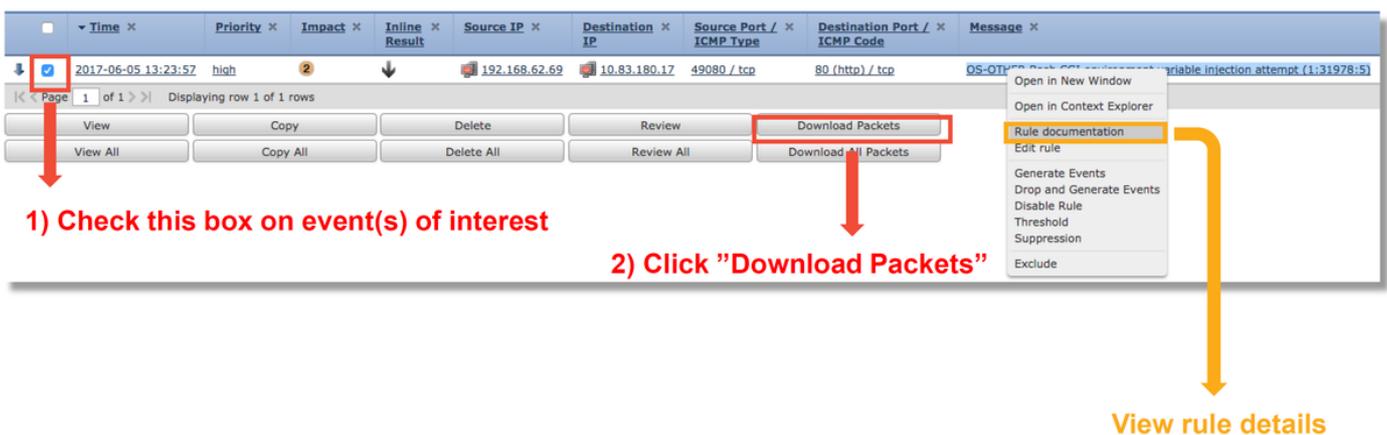
Après avoir créé la nouvelle stratégie d'intrusion, elle peut ensuite être utilisée dans une nouvelle règle de stratégie de contrôle d'accès, qui cible les hôtes en question, dont le trafic était précédemment abandonné par la stratégie d'intrusion d'origine.



## Dépannage faux positif

Un scénario courant est une analyse fausse positive pour les événements d'intrusion. Il y a plusieurs choses qui peuvent être vérifiées avant d'ouvrir un cas faux positif.

1. Dans la page **Vue tableau des événements d'intrusion**, cochez la case de l'événement en question
2. Cliquez sur **Download Packets** pour obtenir les paquets capturés par Snort lors du déclenchement de l'événement d'intrusion.
3. Cliquez avec le bouton droit sur le nom de la règle dans la colonne **Message**, puis **Documentation de la règle**, pour afficher la syntaxe de la règle et d'autres informations pertinentes.



Voici la syntaxe de la règle qui a déclenché l'événement dans l'exemple ci-dessus. Les parties de la règle qui peuvent être vérifiées par rapport à un fichier de capture de paquets (PCAP) téléchargé à partir du FMC pour cette règle sont en gras.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS \
(msg : « tentative d'injection de variable d'environnement OS-AUTRE Bash CGI »; \
flow:to_server, établi ; \
```

```

contenu : »() {« ; fast_pattern : uniquement ; http_header ; \
métadonnées : policy balance-ipsdrop, policy max-detect-ipsdrop, policy security-ipsdrop, policy
set community, service http ; \
référence : cve,2014-6271 ; référence : cve,2014-6277 ; référence : cve,2014-6278 ; référence :
cve,2014-7169 ; \
classtype:tentadmin; \
sid : 31978 ; rev : 5 ; )

```

Ces étapes initiales peuvent ensuite être suivies pour effectuer le processus d'analyse, pour voir si le trafic doit correspondre à la règle qui a déclenché.

1. Vérifiez la règle de contrôle d'accès correspondant au trafic. Ces informations font partie des colonnes de l'onglet Intrusion Events.
2. Recherchez le jeu de variables utilisé dans cette règle de contrôle d'accès. L'ensemble de variables peut ensuite être examiné sous **Objets > Gestion des objets > Jeux de variables**
3. Assurez-vous que les adresses IP du fichier PCAP correspondent aux variables (dans ce cas, un hôte inclus dans \$EXTERNAL\_NET se connectant à un hôte inclus dans la configuration de variable \$HOME\_NET)
4. Pour le **flux**, il peut être nécessaire de capturer une session/connexion complète. Snort ne capturera pas le flux complet pour des raisons de performances. Cependant, dans la plupart des cas, il est possible de supposer que si une règle avec flow : établi a été déclenchée, la session a été établie au moment où la règle a été déclenchée, de sorte qu'un fichier PCAP complet n'est pas nécessaire pour vérifier cette option dans une règle de snort. Mais il peut être utile de mieux comprendre la raison pour laquelle il a été déclenché.
5. Pour le **service http**, consultez le fichier PCAP dans Wireshark pour voir s'il ressemble au trafic HTTP. Si la détection de réseau est activée pour l'hôte et qu'elle a déjà vu l'application « HTTP », elle peut faire correspondre le service sur une session.

Avec ces informations en tête, les paquets téléchargés à partir du FMC peuvent être examinés plus en détail dans Wireshark. Le fichier PCAP peut être évalué pour déterminer si l'événement déclenché est faux positif.

Dans l'illustration ci-dessus, le contenu pour lequel la règle détecte était présent dans le fichier PCAP - "»() {"

Cependant, la règle spécifie que le contenu doit être détecté dans l'en-tête HTTP du paquet - **http\_header**

Dans ce cas, le contenu a été trouvé dans le corps HTTP. C'est donc un faux positif. Cependant, ce n'est pas un faux positif dans le sens où la règle est écrite de manière incorrecte. La règle est correcte et ne peut pas être améliorée dans ce cas. Cet exemple est susceptible de rencontrer un bogue Snort qui provoque une confusion dans la mémoire tampon de snort. Cela signifie que Snort a identifié les en-têtes http de manière incorrecte.

Dans ce cas, vous pouvez rechercher les bogues existants pour le moteur snort/IPS dans la version que votre périphérique exécute. S'il n'y en a pas, un dossier auprès du centre d'assistance technique Cisco (TAC) peut être ouvert. Les captures de session complètes sont nécessaires pour étudier un problème tel que l'équipe Cisco doit examiner comment Snort est entré dans cet état, ce qui ne peut pas être fait avec un seul paquet.

## Exemple positif réel

L'illustration ci-dessous montre l'analyse de paquets pour le même événement d'intrusion. Cette fois, l'événement est un vrai positif, car le contenu n'apparaît pas dans l'en-tête HTTP.

`content:"() {"; fast_pattern:only; http_header;`

content match is present  
in the http\_header

```
GET / HTTP/1.1
Host: 10.83.180.17
User-Agent: curl/7.47.0
Accept: */*
test: () {
```

## Données à fournir au TAC

### Données Instructions

Dépannage  
du fichier à  
partir du

périphérique <http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-tech>

Firepower  
inspectant le  
trafic

Captures de  
paquets

téléchargées Reportez-vous à cet article pour obtenir des instructions.

à partir du  
FMC

Toute sortie  
CLI

pertinente  
recueillie,  
telle que la  
sortie **trace**

Reportez-vous à cet article pour obtenir des instructions.

## Étapes suivantes

S'il a été déterminé que le composant Stratégie d'intrusion n'est pas la cause du problème, l'étape suivante consiste à dépanner la fonctionnalité Stratégie d'analyse du réseau.

Cliquez [ici](#) pour passer au dernier article.