

Dépannage du chemin de données Firepower

Phase 4 : Stratégie de contrôle d'accès

Contenu

[Introduction](#)

[Dépannage de la phase ACP \(Access Control Policy\)](#)

[Vérifier les événements de connexion](#)

[Étapes d'atténuation rapide](#)

[Débogage de l'ACP](#)

[Exemple 1 : Le trafic correspond à une règle d'approbation](#)

[Exemple 2 : Le trafic correspondant à une règle d'approbation est bloqué](#)

[Scénario 3 : Trafic bloqué par la balise d'application](#)

[Données à fournir au TAC](#)

[Étape suivante : Dépannage de la couche de stratégie SSL](#)

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 quatrième étape du dépannage du chemin de données Firepower, la politique de contrôle d'accès (ACP). Ces informations s'appliquent à toutes les plates-formes et versions de Firepower actuellement prises en charge.



Dépannage de la phase ACP (Access Control Policy)

En règle générale, déterminer quelle règle ACP un flux correspond devrait être assez simple. Les événements de connexion peuvent être examinés pour voir quelle règle/action est appliquée. Si cela ne montre pas clairement ce que le PVA fait avec le trafic, le débogage peut être effectué sur l'interface de ligne de commande de Firepower (CLI).

Vérifier les événements de connexion

Après avoir obtenu une idée de l'interface d'entrée et de sortie, le trafic doit correspondre ainsi que les informations de flux, la première étape pour identifier si Firepower bloque le flux serait de vérifier les événements de connexion pour le trafic en question. Vous pouvez les afficher dans Firepower Management Center sous **Analysis > Connections > Events**.

Note: Avant de vérifier les événements de connexion, assurez-vous que la journalisation est activée dans vos règles ACP. La journalisation est configurée dans l'onglet « Journalisation » de chaque règle de stratégie de contrôle d'accès ainsi que dans l'onglet Security Intelligence. Assurez-vous que les règles suspectes sont configurées pour envoyer les journaux à l'« Observateur d'événements ». Cela s'applique également à l'action par défaut.

The screenshot displays the Palo Alto Networks Security Intelligence Center (SIC) interface. The top navigation bar includes Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. The main content area shows a table of Connection Events with columns for First Packet, Last Packet, Action, Reason, Initiator IP, Initiator Country, Responder IP, Responder Country, Ingress Security Zone, Egress Security Zone, Source Port / ICMP Type, Destination Port / ICMP Code, Application Protocol, Client, and Web Application. A detailed view of a selected event is shown on the right, including fields for Initiator IP, Responder IP, Original Client IP, Device, Application, URL, Ingress Security Zone, Egress Security Zone, Ingress / Egress Security Zone, Source Port / ICMP Type, Destination Port / ICMP Code, Protocol, DNS Query, DNS Response, DNS Record Type, DNS TTL, DNS Record Name, HTTP Response Code, VLAN ID, and Destination IP.

En cliquant sur « Edit Search » et filtré par une adresse IP source unique (Initiator), vous pouvez voir les flux qui ont été détectés par Firepower. La colonne Action indique « Autoriser » pour le trafic de cet hôte.

Si Firepower bloque intentionnellement le trafic, l'action contiendra le mot « Bloquer ». Cliquer sur « Affichage table des événements de connexion » fournit plus de données. Les champs suivants des événements de connexion peuvent être examinés si l'action est Bloquer :

- Motif
- Règle de contrôle d'accès

Étapes d'atténuation rapide

Afin d'atténuer rapidement un problème qui est supposé être causé par les règles ACP, il est possible d'effectuer les opérations suivantes :

- Créez une règle avec l'action « Trust » ou « Allow » pour le trafic en question et placez-la en haut du ACP, ou surtout des règles de blocage.
- Désactivez temporairement toutes les règles avec une action contenant le mot « Bloquer »
- Si l'action par défaut est définie sur Bloquer tout le trafic, passez temporairement à Découverte réseau uniquement

Note: Ces mesures d'atténuation rapides nécessitent des changements de politiques qui peuvent ne pas être possibles dans tous les environnements. Il est recommandé d'essayer d'abord d'utiliser le suivi de la prise en charge du système pour déterminer quelle règle le trafic correspond avant d'apporter des modifications à la stratégie.

Débogage de l'ACP

Un dépannage supplémentaire peut être effectué pour les opérations ACP via l'utilitaire CLI > de support du système firewall-engine-debug.

Note: Sur les plates-formes Firepower 9300 et 4100, le shell en question est accessible via les commandes suivantes :

```
# connexion du module 1 console
Firepower-module1> connect ftd
>
```

Pour les instances multiples, l'interface de ligne de commande du périphérique logique est accessible à l'aide des commandes suivantes.

```
# connect module 1 telnet
Firepower-module1> connect ftd ftd1
Connexion à la console du conteneur ftd(ftd1)... Entrez « exit » pour revenir à l'interface de
ligne de commande de démarrage.
>
```

L'utilitaire de débogage du moteur de pare-feu de prise en charge du système comporte une entrée pour chaque paquet évalué par le PVA. Il indique le processus d'évaluation des règles en cours, ainsi que les raisons pour lesquelles une règle est mise en correspondance ou non.

Note: Dans les versions 6.2 et ultérieures, l'outil de suivi du support système peut être exécuté. Il utilise les mêmes paramètres mais inclut plus de détails. Assurez-vous d'entrer « y » lorsque vous y êtes invité avec "Enable firewall-engine-debug ? ».

Exemple 1 : Le trafic correspond à une règle d'approbation

Dans l'exemple ci-dessous, l'établissement d'une session SSH est évalué à l'aide de la prise en charge du système firewall-engine-debug.

Il s'agit de l'ACP exécuté sur le périphérique Firepower.

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN ...	Users	Applic...	Sourc...	Dest P...	URLs	ISE/S... Attrib...	Acti...	
▼ Mandatory - JG AC (all) (1-6)														
1	Trust ssh for host	Any	Any	192.168.0.7	Any	Any	Any	Any	Any	SSH	Any	Any	Trust	
2	inspect	Any	Any	10.0.0.0/8	Any	Any	Any	Any	Any	Any	Any	Any	Allow	
3	trust server backup	Any	Any	192.168.62.3	10.123.175.22	Any	Any	Any	Any	Any	Any	Any	Trust	

Le PVA a trois règles.

1. La première règle consiste à faire confiance à tout trafic provenant de 192.168.0.7 avec les ports de destination utilisés par SSH.
2. La deuxième règle inspecte tout le trafic provenant de 10.0.0.0/8 dans lequel les critères réseau correspondent en fonction des données d'en-tête XFF (comme indiqué par l'icône en regard de l'objet réseau).

3. La troisième règle fait confiance à tout le trafic de 192.168.62.3 à 10.123.175.22

Dans le scénario de dépannage, une connexion SSH de 192.168.62.3 à 10.123.175.22 est analysée.

On s'attend à ce que la session corresponde à la règle AC 3 « trust server backup ». La question est : combien de paquets faut-il pour que cette session corresponde à cette règle ? Toutes les informations nécessaires dans le premier paquet pour déterminer la règle CA ou plusieurs paquets sont-elles requises, et si c'est le cas, combien ?

Dans l'interface de ligne de commande Firepower, les éléments suivants sont entrés pour voir quel est le processus d'évaluation des règles ACP.

```
>system support firewall-engine-debug

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.3
Please specify a client port:
Please specify a server IP address: 10.123.175.22
Please specify a server port: 22
Monitoring firewall engine debug messages
```

Astuce : Il est préférable de remplir autant de paramètres que possible lors de l'exécution de `firewall-engine-debug`, de sorte que seuls les messages de débogage intéressants sont imprimés à l'écran.

Dans la sortie de débogage ci-dessous, vous voyez les quatre premiers paquets de la session en cours d'évaluation.

SYN

SYN,ACK

ACK

Premier paquet SSH (client à serveur)

```
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 | 0 New session
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 | 0 Starting with minimum 4, 'inspect', and IPPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 | 0 pending rule order 4, 'inspect', XFF wait for Appld

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 | 0 Starting with minimum 4, 'inspect', and IPPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 | 0 pending rule order 4, 'inspect', XFF wait for Appld

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 | 0 Starting with minimum 4, 'inspect', and IPPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 | 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 | 0 match rule order 5, 'trust server backup', action Trust
```

Voici un graphique illustrant la logique de débogage.

1. SYN 192.168.62.3 → 10.123.175.22
2. SYN,ACK 10.123.175.22 → 192.168.62.3
3. ACK 192.168.62.3 → 10.123.175.22
4. SSH 192.168.62.3 → 10.123.175.22

Starts evaluation at 'inspect' rule



Service identified as SSH

No match 'inspect' rule (non-http)

Match 'trust server backup' rule and Trust flow

Pour ce flux, il faut 4 paquets pour que le périphérique corresponde à la règle.

Ceci est une explication détaillée de la sortie de débogage.

- Le processus d'évaluation ACP commence à la règle « inspecter » parce que la règle « faire confiance à ssh pour l'hôte » n'a pas été mise en correspondance car l'adresse IP ne correspondait pas à la condition requise. Il s'agit d'une correspondance rapide car toutes les informations nécessaires pour déterminer si cette règle doit correspondre sont présentes dans le premier paquet (adresses IP et ports)
- Il est impossible de déterminer si le trafic correspond à la règle « inspect » tant que l'application n'est pas identifiée, puisque les informations X-Forwarded-For (XFF) sont trouvées dans le trafic d'application HTTP, l'application n'est pas encore connue, ce qui place la session dans un état en attente pour la règle 2, les données d'application en attente.
- Une fois l'application identifiée dans le quatrième paquet, la règle « inspect » entraîne une non-correspondance, car l'application est SSH, plutôt que HTTP
- La règle de sauvegarde du serveur d'approbation est ensuite mise en correspondance, en fonction des adresses IP.

En résumé, la connexion prend 4 paquets pour correspondre à la session, car elle doit attendre que le pare-feu identifie l'application car la règle 2 contient une contrainte d'application.

Si la règle 2 n'avait que des réseaux sources et qu'il ne s'agissait pas de XFF, il aurait fallu 1 paquet pour que la session corresponde.

Vous devez toujours placer les règles des couches 1 à 4 au-dessus de toutes les autres règles de la stratégie lorsque cela est possible, car ces règles nécessitent généralement un paquet pour prendre une décision. Cependant, vous remarquerez peut-être que même avec les seules règles des couches 1 à 4, il peut y avoir plus d'un paquet correspondant à une règle CA, et la raison en est l'intelligence de sécurité URL/DNS. Si l'une ou l'autre de ces options est activée, le pare-feu doit déterminer l'application pour toutes les sessions évaluées par la stratégie AC, car il doit déterminer si elles sont HTTP ou DNS. Ensuite, il doit déterminer s'il doit autoriser la session en fonction des listes noires.

Ci-dessous se trouve une sortie tronquée de la commande **firewall-engine-debug**, dont les champs pertinents sont surlignés en rouge. Notez la commande utilisée pour obtenir le nom de l'application identifiée.

```

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 | 0 New session
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 | 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 | 0 pending rule order 4, 'inspect', XFF wait for Appld

[...omitted for brevity]

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 | 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 846, payload -1, client 2000000846, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 | 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 | 0 match rule order 5, 'trust server backup', action Trust

[! How to map service/application ID to name]
> expert
$ grep "^846[^\0-9]" /var/sf/appid/odp/appMapping.data
846 SSH 32 0 0 ssh

```

Exemple 2 : Le trafic correspondant à une règle d'approbation est bloqué

Dans certains scénarios, le trafic peut être bloqué malgré la correspondance d'une règle d'approbation dans le ACP. L'exemple ci-dessous évalue le trafic avec la même politique de contrôle d'accès et les mêmes hôtes.

```

192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 | 0 New session
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 | 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 | 0 pending rule order 4, 'inspect', XFF wait for Appld
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 | 0 Deleting session

[!Session was deleted because we hit a drop IPS rule and blacklisted the flow.
This happened before AC rule was matched (Intrusion policy before AC rule match dropped).
Firewall engine will re-evaluate from top of AC policy to find a rule for logging decision]

192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 | 0 Starting with minimum 0, id 0 and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline
sgt tag: 0, ISE sgt id: 0, svc -1, payload -1, client -1, misc -1, user 9999997, icmpType 102, icmpCode 22
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 | 0 no match rule order 3, 'Trust ssh for host', src network and GEO
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 | 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 | 0 match rule order 5, 'trust server backup', action Trust

```

Action ×	Reason ×	Initiator IP ×	Responder IP ×	Source Port / ICMP Type ×	Destination Port / ICMP Code ×	Application Protocol ×	Client ×	Intrusion Events ×	Access Control Policy ×	Access Control Rule ×
Block	Intrusion Block	192.168.62.3	10.123.175.22	55654 / tcp	22 (ssh) / tcp				JG AC (all)	trust server backup

Comme indiqué ci-dessus, la sortie `firewall-engine-debug` montre que le trafic correspond à un « Trust », alors que les événements de connexion montrent l'action de **Block** en raison d'une règle de stratégie d'intrusion (déterminée parce que la colonne Reason affiche **Intrusion Block**).

La raison pour laquelle cela peut se produire est due à la **stratégie d'intrusion utilisée avant que la règle de contrôle d'accès ne soit déterminée** Paramètre dans l'onglet **Avancé** du ACP. Avant que le trafic puisse être approuvé par l'action de règle, la stratégie d'intrusion en question identifie une correspondance de modèle et abandonne le trafic. Cependant, l'évaluation de la règle ACP aboutit à une correspondance de la règle Trust, puisque les adresses IP correspondaient aux critères de la règle « trust server backup ».

Pour que le trafic ne soit pas soumis à l'inspection de la politique d'intrusion, la règle de confiance peut être placée au-dessus de la règle d'« inspection », ce qui serait une pratique recommandée dans les deux cas. Étant donné que l'identification de l'application est nécessaire pour une correspondance et une non-correspondance de la règle « inspect », la **stratégie d'intrusion utilisée avant que la règle de contrôle d'accès ne soit déterminée** est utilisée pour le trafic qui est évalué par la même règle. En plaçant la règle de sauvegarde du serveur d'approbation au-dessus de la règle d'inspection, le trafic correspond à la règle lorsque le premier paquet est vu, car la règle est basée sur l'adresse IP, qui peut être déterminée dans le premier paquet. Par conséquent, la

stratégie d'intrusion utilisée avant que la règle de contrôle d'accès ne soit déterminée n'a pas besoin d'être utilisée.

Scénario 3 : Trafic bloqué par la balise d'application

Dans ce scénario, les utilisateurs signalent que cnn.com est bloqué. Cependant, il n'y a pas de règle spécifique qui bloque CNN. Les événements de connexion, associés à la sortie **firewall-engine-debug**, indiquent la raison du blocage.

Tout d'abord, Connection Events dispose d'une zone d'informations à côté des champs d'application qui affiche des informations sur l'application ainsi que la manière dont Firepower classe ladite application.

First Packet	Last Packet	Action	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Web Application	Application Risk	Business Relevance	URL
2017-05-19 16:02:29		Block	192.168.62.63	151.101.65.67	54308 / tcp	80 (http) / tcp	HTTP	CNN.com	Medium	Medium	http://cnn.com/

CNN.com

Turner Broadcasting System's news website.

Type Web Application
Risk Very Low
Business Relevance High
Categories multimedia (TV/video), news
Tags displays ads

Context Explorer | Wikipedia | Google | Yahoo! | Bing

Avec ces informations en tête, **firewall-engine-debug** est exécuté. Dans la sortie de débogage, le trafic est bloqué en fonction de la balise d'application.

```
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 | 0 New session
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 | 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0 -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 | 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 | 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0 -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 | 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 | 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0 -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 | 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 | 0 URL SI: ShmDBLookupURL("http://cnn.com/") returned 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 | 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0(0) -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 676, payload 1190, client 638, misc 0, user 9999997, url http://cnn.com/, xff
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 | 0 match rule order 4, 'block by tag', action Block
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 | 0 sending block response of 605 bytes
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 | 0 Deleting session
```

Même s'il n'existe pas de règle qui bloque explicitement <http://cnn.com>, l'affichage des annonces balisées est bloqué dans l'onglet **Applications** d'une règle ACP.

The screenshot shows the 'Editing Rule' configuration page in Cisco Firepower Management Center. The rule name is 'block by tag' and it is enabled. The action is 'Block with reset'. The 'Applications' tab is active, displaying a list of available applications. 'CNN.com' is selected and highlighted with a red box. The 'Selected Applications and Filters' pane shows a filter for 'Tags: displays ads'. Buttons for 'Save' and 'Cancel' are visible at the bottom right.

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/1176>

Firepower inspectant

le trafic

prise en charge du

systeme firewall-

engine-debug et

system-support-trace

output

Reportez-vous à cet article pour obtenir des instructions.

Exportation de la

stratégie de contrôle d'accès Accédez à **System > Tools > Import / Export**, sélectionnez Access Control Policy et

d'accès

Attention : Si l'ACP contient une stratégie SSL, supprimez la stratégie SSL de l'ACP avant d'exporter pour éviter de divulguer des informations PKI sensibles

Étape suivante : Dépannage de la couche de stratégie SSL

Si une stratégie SSL est en cours d'utilisation et que le dépannage de la stratégie de contrôle d'accès n'a pas révélé le problème, l'étape suivante consiste à dépanner la stratégie SSL.