

Dépannage du chemin de données Firepower

Phase 8 : Stratégie d'analyse réseau

Contenu

[Introduction](#)

[Conditions préalables](#)

[Dépannage de la fonction de stratégie d'analyse du réseau](#)

[Utilisation de l'outil « trace » pour rechercher les pertes de préprocesseur \(FTD uniquement\)](#)

[Vérifier la configuration NAP](#)

[Afficher les paramètres NAP](#)

[Paramètres NAP pouvant entraîner des pertes silencieuses](#)

[Vérification de la configuration du serveur principal](#)

[Création d'un NAP ciblé](#)

[Analyse fausse positive](#)

[Étapes d'atténuation](#)

[Données à fournir au TAC](#)

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 Vue d'ensemble](#) 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 huitième étape du dépannage du chemin de données Firepower, la fonction Stratégie d'analyse du réseau.



Conditions préalables

- Cet article s'applique à toutes les plates-formes Firepower
La fonctionnalité **trace** n'est disponible que dans les versions 6.2.0 et ultérieures du logiciel 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 fonction de stratégie d'analyse du réseau

La politique d'analyse du réseau (NAP) contient des paramètres de préprocesseur de snort qui

effectuent des inspections sur le trafic, en fonction de l'application identifiée. Les préprocesseurs peuvent supprimer le trafic en fonction de la configuration. Cet article explique comment vérifier la configuration NAP et rechercher les pertes de préprocesseur.

Note: Les règles de préprocesseur ont un ID de générateur (GID) autre que '1' ou '3' (c'est-à-dire 129, 119, 124). Vous trouverez plus d'informations sur les mappages GID/préprocesseur dans les [Guides de configuration](#) FMC.

Utilisation de l'outil « trace » pour rechercher les pertes de préprocesseur (FTD uniquement)

L'outil **de suivi du support système** peut être utilisé pour détecter les pertes effectuées au niveau du préprocesseur.

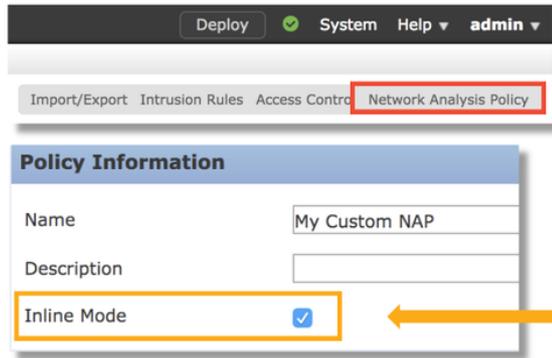
Dans l'exemple ci-dessous, le préprocesseur de normalisation TCP a détecté une anomalie. En conséquence, le trafic est abandonné par la règle **129:14**, qui recherche les horodatages manquants dans un flux TCP.

```
> system support trace
[omitted for brevity...]
172.16.111.226-51174 - 50.19.123.95-443 6 Packet: TCP, ACK, seq 3849839667, ack 1666843207
172.16.111.226-51174 - 50.19.123.95-443 6 Stream: TCP normalization error in timestamp, window, seq, ack, fin, flags, or unexpected data, drop
172.16.111.226-51174 - 50.19.123.95-443 6 AppID: service unknown (0), application unknown (0)
172.16.111.226-51174 > 50.19.123.95-443 6 AS 4 | 0 Starting with minimum 3, 'block urls', and SrcZone first with zones -1 -> -1, 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
172.16.111.226-51174 > 50.19.123.95-443 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997, icmpType 0, icmpCode 0
172.16.111.226-51174 > 50.19.123.95-443 6 AS 4 | 0 pending rule order 3, 'block urls', URL
172.16.111.226-51174 > 50.19.123.95-443 6 Firewall: pending rule-matching, 'block urls', pending URL
172.16.111.226-51174 > 50.19.123.95-443 6 Snort: processed decoder alerts or actions queue, drop
172.16.111.226-51174 > 50.19.123.95-443 6 IPS Event: gid 129, sid 14, drop
172.16.111.226-51174 > 50.19.123.95-443 6 NAP id 1, IPS id 0, Verdict BLOCK
172.16.111.226-51174 > 50.19.123.95-443 6 ==> Blocked by Stream
```

Note: Bien que le préprocesseur **TCP Stream Configuration** abandonne le trafic, il peut le faire car le préprocesseur **de normalisation en ligne** est également activé. Pour plus d'informations sur la normalisation en ligne, vous pouvez lire cet [article](#).

Vérifier la configuration NAP

Dans l'interface FMC (Firepower Management Center), le NAP peut être affiché sous **Politiques > Contrôle d'accès > Intrusion**. Ensuite, cliquez sur l'option **Stratégie d'analyse réseau** en haut à droite, après quoi vous pouvez afficher les NAP, en créer de nouveaux et en modifier des existants.



Edit or create a Network Analysis Policy

Uncheck this box to disable Inline Mode

Inline Result	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Message
<input type="checkbox"/>	172.16.111.226	50.19.123.95	51177 / tcp	443 (https) / tcp	STREAM5_NO_TIMESTAMP (129:14:2)
<input checked="" type="checkbox"/>	172.16.111.226	50.19.123.95	51174 / tcp	443 (https) / tcp	STREAM5_NO_TIMESTAMP (129:14:2)

Inline Mode disabled = No Inline Result

Inline Mode enabled = "Dropped" Inline Result

Comme l'illustre l'illustration ci-dessus, les NAP contiennent une fonction « Inline Mode », qui équivaut à l'option « Drop When Inline » dans la stratégie d'intrusion. Une étape de réduction rapide pour empêcher le NAP de supprimer le trafic serait de désactiver le **mode en ligne**. Les événements d'intrusion générés par le NAP n'affichent rien dans l'onglet **Résultat en ligne** avec le **mode en ligne** désactivé.

Afficher les paramètres NAP

Dans le NAP, vous pouvez afficher les paramètres actuels. Cela inclut le nombre total de préprocesseurs activés, suivi de

préprocesseurs activés avec des paramètres autres que ceux par défaut (ceux qui ont été ajustés manuellement) et ceux qui sont activés avec des paramètres par défaut, comme le montre l'illustration ci-dessous.

Edit Policy: My Custom NAP

View preprocessors →

Currently Enabled

Enabled with non-default settings

Enabled with default settings

Paramètres NAP pouvant entraîner des pertes silencieuses

Dans l'exemple mentionné dans la section trace, la règle Configuration du flux TCP 129:14 abandonne le trafic. Ceci est déterminé en examinant la sortie de suivi du support système. Cependant, si cette règle n'est pas activée dans la stratégie d'intrusion correspondante, aucun événement d'intrusion n'est envoyé au FMC.

La raison pour laquelle cela se produit est due à un paramètre du préprocesseur de normalisation en ligne appelé **Bloquer les anomalies d'en-tête TCP non résolubles**. Cette option permet essentiellement à Snort d'effectuer une action de blocage lorsque certaines règles GID 129 détectent des anomalies dans le flux TCP.

Si **Bloquer les anomalies d'en-tête TCP non résolubles** est activé, il est recommandé d'activer les règles GID 129 conformément à l'illustration ci-dessous.

The screenshot displays the 'Intrusion Policy' configuration page for rule GID: "129". The interface shows a list of 19 rules, with 12 selected. A context menu is open over rule 129, showing options: 'Generate Events', 'Drop and Generate Events', and 'Disable'. The 'Drop and Generate Events' option is selected. The 'Policy Information' panel on the right shows the 'Settings' section, with 'Inline Normalization' selected. The 'Block Unresolvable TCP Header Anomalies' option is checked and highlighted with a red box.

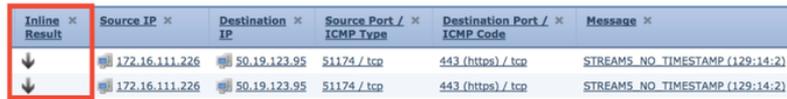
Rule ID	Action	Rule Name
129 4	<input checked="" type="checkbox"/>	STREAM5_BAD_TIMESTAMP
129 5	<input type="checkbox"/>	STREAM5_BAD_SEGMENT
129 6	<input checked="" type="checkbox"/>	STREAM5_WINDOW_TOO_LARGE
129 7	<input type="checkbox"/>	STREAM5_EXCESSIVE_TCP_OVERLAPS
129 8	<input checked="" type="checkbox"/>	STREAM5_DATA_AFTER_RESET
129 9	<input type="checkbox"/>	STREAM5_SESSION_HIJACKED_CLIENT
129 10	<input type="checkbox"/>	STREAM5_SESSION_HIJACKED_SERVER
129 11	<input checked="" type="checkbox"/>	STREAM5_DATA_WITHOUT_FLAGS
129 12	<input type="checkbox"/>	STREAM5_SMALL_SEGMENT
129 13	<input type="checkbox"/>	STREAM5_4WAY_HANDSHAKE
129 14	<input checked="" type="checkbox"/>	STREAM5_NO_TIMESTAMP
129 15	<input checked="" type="checkbox"/>	STREAM5_BAD_RST
129 16	<input checked="" type="checkbox"/>	STREAM5_BAD_FIN
129 17	<input checked="" type="checkbox"/>	STREAM5_BAD_ACK
129 18	<input checked="" type="checkbox"/>	STREAM5_DATA_AFTER_RST_RCVD
129 19	<input checked="" type="checkbox"/>	STREAM5_WINDOW_SLAM

Setting	Value
Back Orifice Detection	<input type="checkbox"/>
DCE/RPC Configuration	<input type="checkbox"/>
DNS Configuration	<input type="checkbox"/>
FTP and Telnet Configuration	<input type="checkbox"/>
GTP Command Channel Configuration	<input type="checkbox"/>
HTTP Configuration	<input type="checkbox"/>
Inline Normalization	<input checked="" type="checkbox"/>
IP Defragmentation	<input type="checkbox"/>
Packet Decoding	<input type="checkbox"/>
SIP Configuration	<input type="checkbox"/>
SMTP Configuration	<input type="checkbox"/>
SSH Configuration	<input type="checkbox"/>
SSL Configuration	<input type="checkbox"/>
Sun RPC Configuration	<input type="checkbox"/>
TCP Stream Configuration	<input checked="" type="checkbox"/>
UDP Stream Configuration	<input type="checkbox"/>

Setting	Value
Normalize IPv4	<input type="checkbox"/>
Normalize Don't Fragment Bit	<input type="checkbox"/>
Normalize Reserved Bit	<input type="checkbox"/>
Normalize TOS Bit	<input type="checkbox"/>
Normalize Excess Payload	<input type="checkbox"/>
Normalize IPv6	<input type="checkbox"/>
Normalize ICMPv4	<input type="checkbox"/>
Normalize ICMPv6	<input type="checkbox"/>
Normalize/Clear Reserved Bits	<input checked="" type="checkbox"/>
Normalize/Clear Option Padding Bytes	<input checked="" type="checkbox"/>
Clear Urgent Pointer if URG=0	<input checked="" type="checkbox"/>
Clear Urgent Pointer/URG on Empty Payload	<input checked="" type="checkbox"/>
Clear URG if Urgent Pointer Is Not Set	<input checked="" type="checkbox"/>
Normalize Urgent Pointer	<input type="checkbox"/>
Normalize TCP Payload	<input checked="" type="checkbox"/>
Remove Data on SYN	<input type="checkbox"/>
Remove Data on RST	<input type="checkbox"/>
Trim Data to Window	<input type="checkbox"/>
Trim Data to MSS	<input type="checkbox"/>
Block Unresolvable TCP Header Anomalies	<input checked="" type="checkbox"/>

L'activation des règles GID 129 entraîne l'envoi d'événements d'intrusion au FMC lorsqu'ils agissent sur le trafic. Cependant, tant que les **Anomalies d'en-tête TCP bloquables** sont activées, elles peuvent toujours supprimer le trafic même si l'état de la règle dans la stratégie d'intrusion est défini sur **Générer** uniquement **des événements**. Ce comportement est expliqué dans les Guides de configuration FMC.

Still drops after setting to generate



Inline Result	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Message
↓	172.16.111.226	50.19.123.95	51174 / tcp	443 (https) / tcp	STREAMS_NO_TIMESTAMP (129:14:2)
↓	172.16.111.226	50.19.123.95	51174 / tcp	443 (https) / tcp	STREAMS_NO_TIMESTAMP (129:14:2)

Check configuration guide for relative protocols/preprocessors:

Block Unresolvable TCP Header Anomalies

When you enable this option, the system blocks anomalous TCP packets that, if normalized, would be invalid and likely would be blocked by the receiving host. For example, the system blocks any SYN packet transmitted subsequent to an established session.

The system also drops any packet that matches any of the following TCP stream preprocessor rules, regardless of whether the rules are enabled:

- 129:1
- 129:3
- 129:4
- 129:6
- 129:8
- 129:11
- 129:14 through 129:19

The Total Blocked Packets performance graph tracks the number of packets blocked in inline deployments and, in passive deployments and inline deployments in tap mode, the number that would have been blocked in an inline deployment.

La documentation ci-dessus se trouve dans cet [article](#) (pour la version 6.4, qui est la version la plus récente au moment de la publication de cet article).

Vérification de la configuration du serveur principal

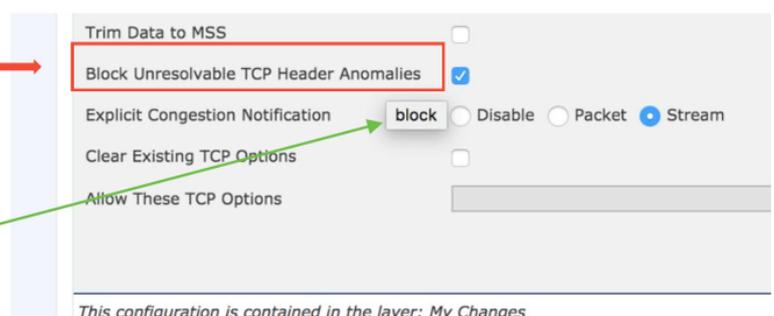
Une autre couche de complexité est ajoutée au comportement du préprocesseur en ce sens que certains paramètres peuvent être activés sur le serveur principal, sans être répercutés dans le FMC. Voilà quelques raisons possibles.

- D'autres fonctionnalités activées peuvent forcer les paramètres d'activation du préprocesseur (la principale étant la stratégie de fichier)
- Certaines règles de stratégie d'intrusion nécessitent certaines options de préprocesseur afin d'effectuer la détection
- Un défaut peut provoquer le comportement Nous en avons vu un exemple : [CSCuz50295](#) - « La politique de fichiers avec le bloc Malware permet la normalisation TCP avec l'indicateur de blocage »

Avant d'examiner la configuration du serveur principal, notez que les mots clés Snort, qui sont utilisés dans les fichiers de configuration Snort du serveur principal, peuvent être vus en survolant un paramètre spécifique dans le NAP. Reportez-vous à l'illustration ci-dessous.

Hover over option to see backend snort configuration keyword

Snort config keyword is "block"



Trim Data to MSS

Block Unresolvable TCP Header Anomalies

Explicit Congestion Notification **block** Disable Packet Stream

Clear Existing TCP Options

Allow These TCP Options

This configuration is contained in the layer: My Changes

L'option **Bloquer les anomalies d'en-tête TCP non résolubles** dans l'onglet NAP se traduit par le mot clé **block** sur le serveur principal. En gardant ces informations à l'esprit, la configuration du serveur principal peut être vérifiée à partir de l'interpréteur de commandes expert.

```
root@ciscoasa:~# de_info.pl
-----
DE Name      : Primary Detection Engine (c9ef19d6-e187-11e6-ba76-99617d53da68)
DE Type      : ids
DE Description : Primary detection engine for device c9ef19d6-e187-11e6-ba76-99617d53da68
DE Resources  : 1
DE UUID      : 0d82120c-e188-11e6-8606-a4827d53da68
-----

root@ciscoasa:~# cd /var/sf/detection_engines/0d82120c-e188-11e6-8606-a4827d53da68/network_analysis/
root@ciscoasa: network_analysis# ls
b50f27b0-e31a-11e6-b866-dd9e65c01d56 object_b50f27b0-e31a-11e6-b866-dd9e65c01d56 snort.conf.b50f27b0-e31a-11e6-b866-
dd9e65c01d56 snort.conf.b50f27b0-e31a-11e6-b866-dd9e65c01d56.default
root@ciscoasa: network_analysis# cat b50f27b0-e31a-11e6-b866-dd9e65c01d56/normalize.conf
#
# generated from My Changes
#
preprocessor normalize_tcp: ips, rsv, pad, req_urg, req_pay, req_urp, block
```

“block” option is enabled in normalize.conf

Création d'un NAP ciblé

Si certains hôtes déclenchent des événements de préprocesseur, un NAP personnalisé peut être utilisé pour inspecter le trafic en provenance ou à destination de ces hôtes. Dans le NAP personnalisé, les paramètres qui causent des problèmes peuvent être désactivés.

Il s'agit des étapes de mise en oeuvre d'un PAN ciblé.

1. Créez le NAP conformément aux instructions mentionnées dans la section Vérifier la configuration du NAP de cet article.
2. Dans l'onglet **Avancé** de la stratégie de contrôle d'accès, accédez à la section **Analyse du réseau et stratégies d'intrusion**. Cliquez sur **Ajouter une règle** et créez une règle à l'aide des hôtes cibles et choisissez le NAP nouvellement créé dans la section **Stratégie d'analyse du réseau**.

The screenshot shows the 'Network Analysis and Intrusion Policies' configuration window. On the left, a smaller window shows the 'Default Network Analysis Policy' set to 'Security Over Connectivity'. In the main window, the 'Network Analysis Rules' section shows a table with one rule:

#	Source Zo...	Dest Zones	Source Networ...	Dest Networks	VLAN T...	Network Analysis ...
1	Any	Any	62_network	Any	Any	My Custom NAP

Annotations include:

- A red arrow pointing to the '1 Custom Rule' button with the text: "Click to expand NA Rules".
- A red arrow pointing to the '62_network' and 'My Custom NAP' cells in the table with the text: "Add rule(s) to target traffic with certain NAP".

Analyse fausse positive

La recherche de faux positifs dans Intrusion Events pour les règles de préprocesseur est très différente de celle des règles Snort utilisées pour l'évaluation des règles (qui contiennent un GID de 1 et 3).

Pour effectuer une analyse fausse positive des événements de règle de préprocesseur, une capture de session complète est nécessaire pour rechercher des anomalies dans le flux TCP.

Dans l'exemple ci-dessous, une analyse fausse positive est effectuée sur la règle **129:14**, qui est montrée comme abandonnant le trafic dans les exemples ci-dessus. Puisque **129:14** recherche des flux TCP dans lesquels des horodatages sont manquants, vous pouvez clairement voir pourquoi la règle a été déclenchée par l'analyse de capture de paquets illustrée ci-dessous.

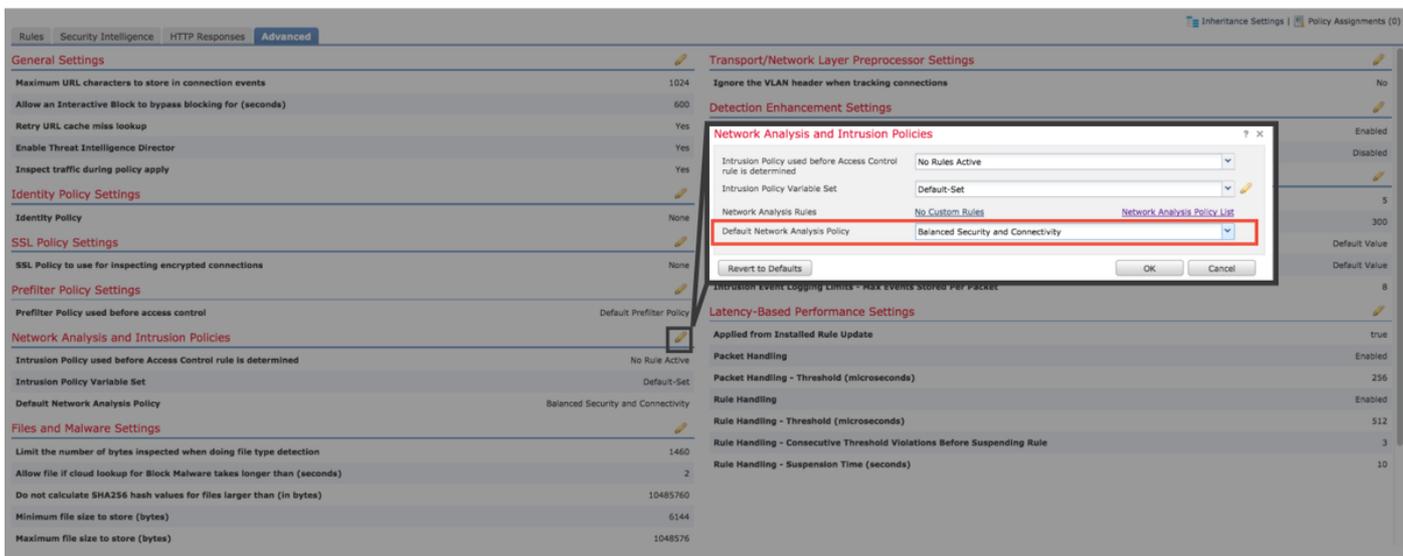
Full session pcap

The image displays two network packet captures side-by-side. The left capture, titled 'Full session pcap', shows a SYN packet with the following details: Source Port: 51174, Destination Port: 443, Sequence number: 3849839666, and Flags: 0x002 (SYN). A red box highlights the 'Flags: 0x002 (SYN)' field, and a callout box points to it with the text 'SYN packet has TCP Timestamps'. The 'Options' field is expanded to show 'Timestamps: TSval 2054852, TSecr 0'. The right capture, titled 'Packet that triggered event', shows an ACK packet with the following details: Source Port: 51174, Destination Port: 443, Acknowledgment number: 1666843207, and Flags: 0x010 (ACK). A red box highlights the 'Flags: 0x010 (ACK)' field, and a callout box points to it with the text 'No TCP Timestamps in event packet (violates RFC)'. The 'Options' field is expanded to show 'Timestamps: TSval 2054852, TSecr 0'.

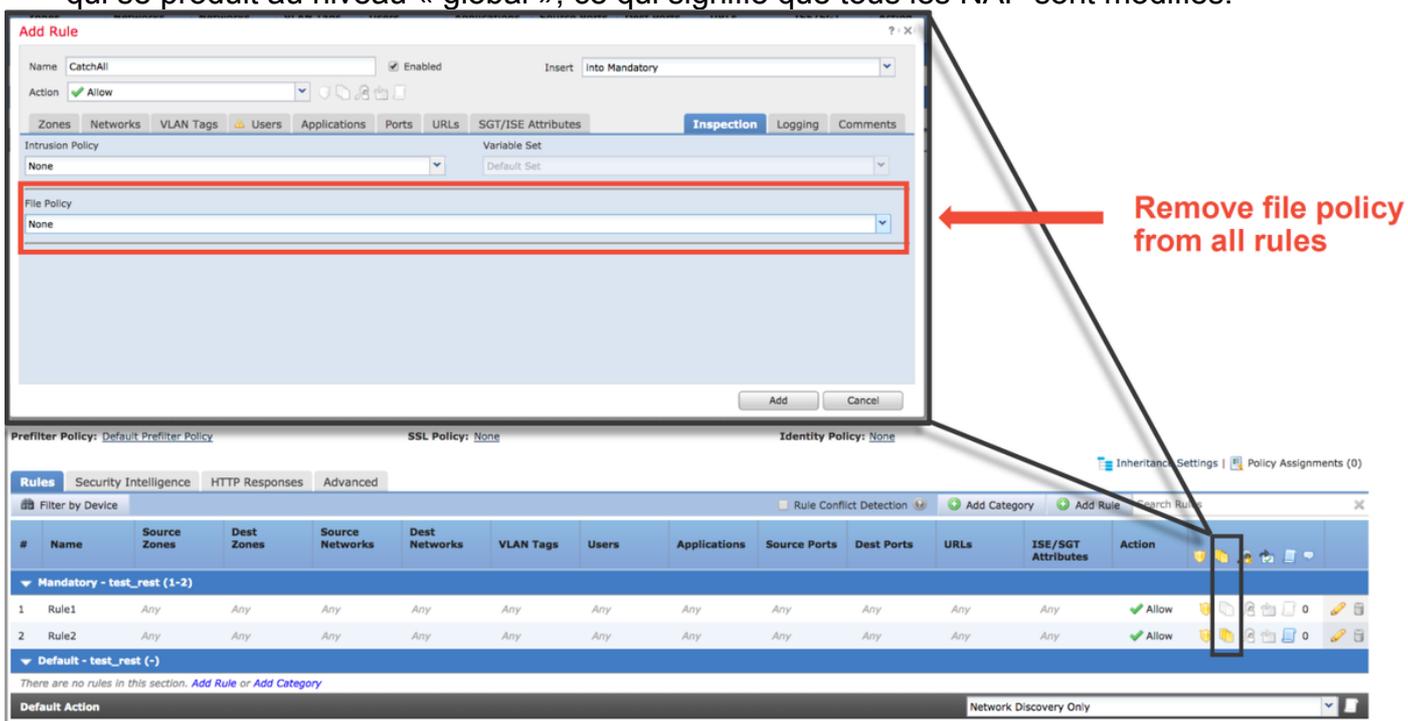
Étapes d'atténuation

Pour atténuer rapidement les problèmes éventuels liés au PAN, les étapes suivantes peuvent être effectuées.

- Si un NAP personnalisé est utilisé et que vous ne savez pas si un paramètre NAP est en train de supprimer le trafic mais que vous pensez qu'il le sera, vous pouvez essayer de le remplacer par une stratégie de sécurité et de connectivité équilibrées ou de connectivité sur la sécurité.



- Si des « règles personnalisées » sont utilisées, veillez à définir le NAP sur l'une des valeurs par défaut mentionnées ci-dessus
- Si des règles de contrôle d'accès utilisent une stratégie de fichier, vous devrez peut-être essayer de la supprimer temporairement car une stratégie de fichier peut activer les paramètres de préprocesseur sur le serveur principal qui ne sont pas reflétés dans le FMC, ce qui se produit au niveau « global », ce qui signifie que tous les NAP sont modifiés.



Chaque protocole possède un préprocesseur différent et le dépannage de ces derniers peut être très spécifique au préprocesseur. Cet article ne couvre pas tous les paramètres du préprocesseur et les méthodes de dépannage pour chacun d'eux.

Vous pouvez consulter la documentation de chaque préprocesseur pour avoir une meilleure idée de ce que fait chaque option, ce qui est utile lors du dépannage d'un préprocesseur spécifique.

Données à fournir au TAC

Données Instructions

Dépannage
du fichier à
partir du
périphérique
Firepower
Capture de
paquet de
session
complète à
partir du
périphérique
Firepower

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

<http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepower-8000-series-applian>