

Dépannage du chemin de données Firepower : Aperçu

Contenu

[Introduction](#)

[Conditions préalables](#)

[Présentation de l'architecture du chemin de données](#)

[Plate-forme ASA avec fonctionnalités FirePOWER \(module SFR\)](#)

[Firepower Threat Defense sur ASA500-X et la plate-forme virtuelle FTD](#)

[FTD sur les plates-formes SSP](#)

[Appareils Firepower 9300 et 4100](#)

[Appareils Firepower 2100](#)

[Processus recommandé pour le dépannage du chemin de données Firepower](#)

[Chemin réel du paquet via FTD](#)

[Snort Packet Path](#)

[Paquet entrant et sortant](#)

[Couche DAQ Firepower](#)

[Intelligence de sécurité](#)

[Stratégie de contrôle d'accès](#)

[Stratégie SSL](#)

[Authentification active](#)

[Politique d'intrusion](#)

[Stratégie d'analyse réseau](#)

[Informations connexes](#)

Introduction

L'objectif de ce guide est d'aider à identifier rapidement si un périphérique Firepower Threat Defense (FTD) ou un appareil de sécurité adaptatif (ASA) avec les fonctionnalités FirePOWER est à l'origine d'un problème de trafic réseau. Il permet également de déterminer quels composants Firepower doivent faire l'objet d'une enquête et quelles données doivent être collectées avant d'engager le centre d'assistance technique Cisco (TAC).

Liste de tous les articles de la série de dépannages Firepower Data Path.

Dépannage du chemin de données Firepower Phase 1 : Paquet entrant

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214574-firepower-data-path-troubleshooting-phas.html>

Dépannage du chemin de données Firepower Phase 2 : Couche DAQ

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214575-firepower-data-path-troubleshooting-phas.html>

Dépannage du chemin de données Firepower Phase 3 : Intelligence de sécurité

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214576-firepower-data-path-troubleshooting-phas.html>

Dépannage du chemin de données Firepower Phase 4 : Stratégie de contrôle d'accès

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214577-firepower-data-path-troubleshooting-phas.html>

Dépannage du chemin de données Firepower Phase 5 : Stratégie SSL

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214581-firepower-data-path-troubleshooting-phas.html>

Dépannage du chemin de données Firepower Phase 6 : Authentification active

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/214608-firepower-data-path-troubleshooting-phas.html>

Dépannage du chemin de données Firepower Phase 7 : Politique d'intrusion

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214609-firepower-data-path-troubleshooting-phas.html>

Dépannage du chemin de données Firepower Phase 8 : Stratégie d'analyse réseau

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214610-firepower-data-path-troubleshooting-phas.html>

Conditions préalables

- Cet article suppose qu'on a une compréhension de base des plates-formes FTD et ASA.
- La connaissance de l'open source snort est recommandée, mais pas nécessaire.

Pour obtenir la liste complète de la documentation de Firepower, y compris les guides d'installation et de configuration, consultez la page [feuille de route de la documentation](#).

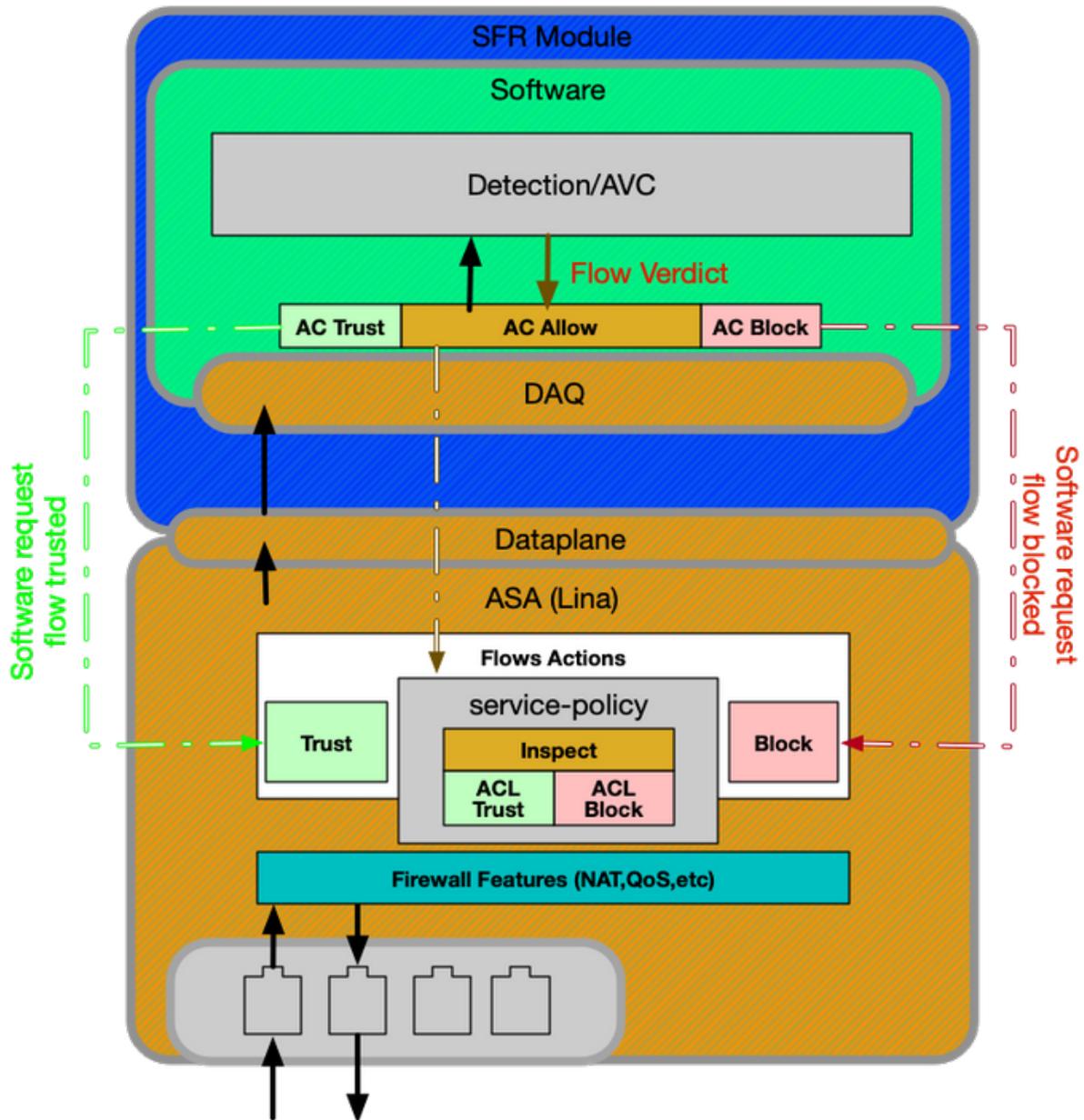
Présentation de l'architecture du chemin de données

La section suivante examine le chemin de données architecturaux pour différentes plates-formes Firepower. Avec l'architecture en tête, nous passerons ensuite à la façon de déterminer rapidement si le périphérique Firepower bloque ou non le flux de trafic.

Note: Cet article ne couvre pas les anciens périphériques des gammes Firepower 7000 et 8000, ni la plate-forme virtuelle NGIPS (non-FTD). Pour plus d'informations sur le dépannage de ces plates-formes, consultez notre page [TechNotes](#) .

Plate-forme ASA avec fonctionnalités FirePOWER (module SFR)

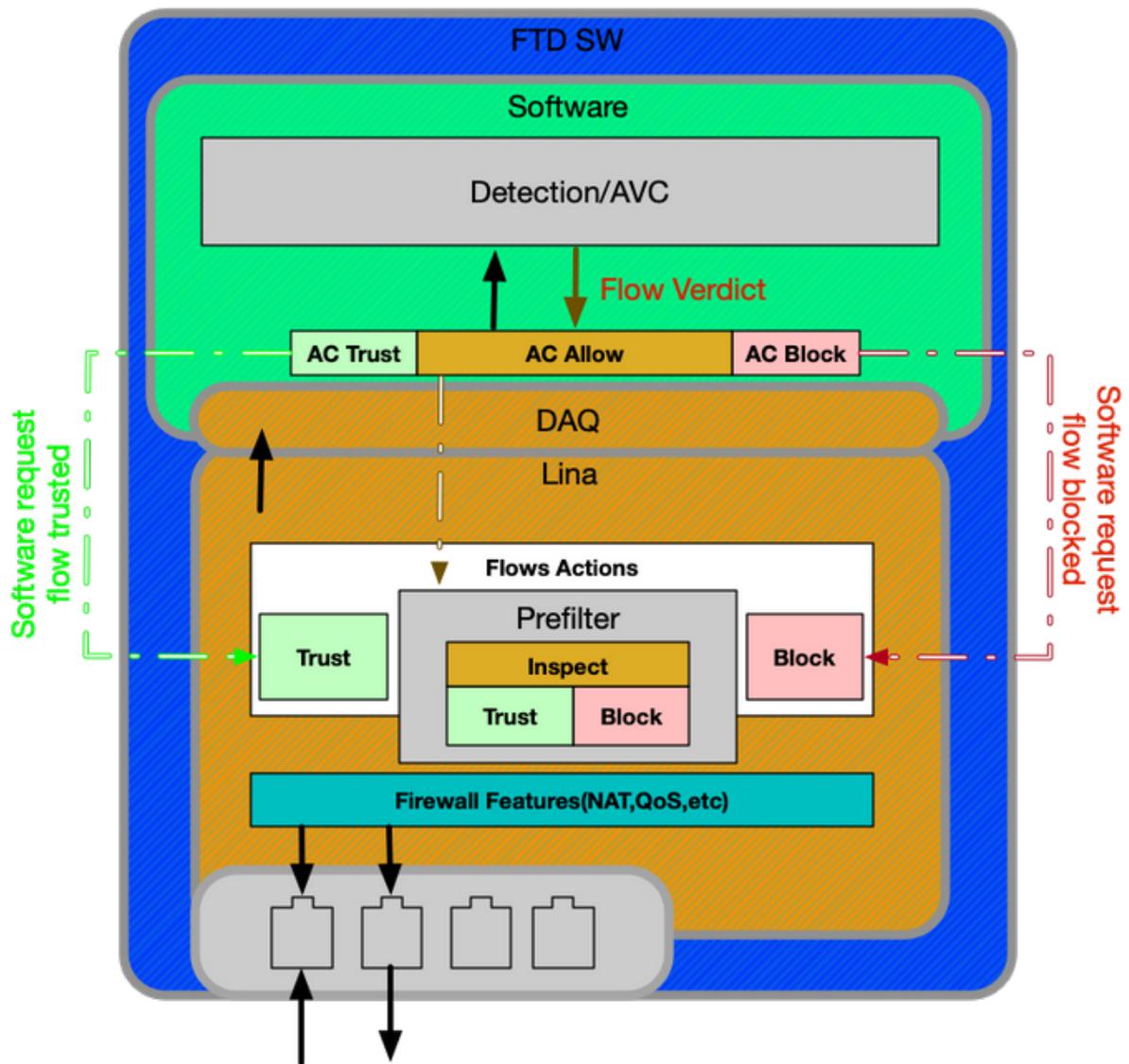
La plate-forme FirePOWER Services est également appelée module SFR. Il s'agit essentiellement d'une machine virtuelle qui fonctionne sur des plates-formes ASA 5500-X.



La stratégie de service sur l'ASA détermine le trafic envoyé au module SFR. Il y a une couche de plan de données qui est utilisée pour communiquer avec le moteur d'acquisition de données Firepower (DAQ), qui est utilisé pour traduire les paquets d'une manière que snort peut comprendre.

Firepower Threat Defense sur ASA500-X et la plate-forme virtuelle FTD

La plate-forme FTD se compose d'une seule image contenant à la fois le code Lina (ASA) et le code Firepower. Une différence majeure entre cette plate-forme et la plate-forme de module ASA avec SFR est qu'il existe des communications plus efficaces entre Lina et Snort.

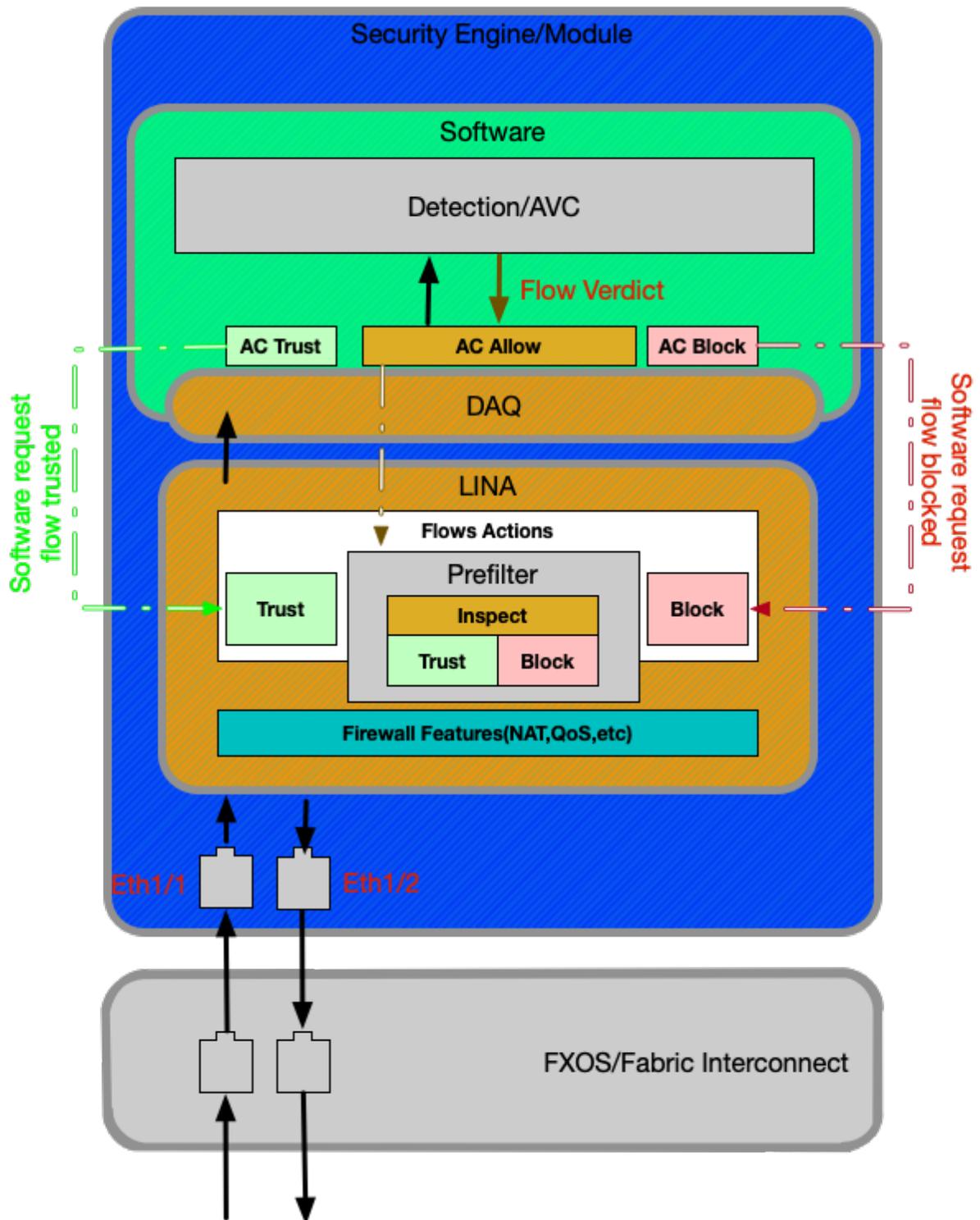


FTD sur les plates-formes SSP

Sur les modèles SSP (Security Service Platforms), le logiciel FTD s'exécute sur la plate-forme FXOS (Firepower eXtensible Operative System), qui est un système d'exploitation sous-jacent utilisé pour gérer le matériel du châssis et héberger diverses applications appelées périphériques logiques.

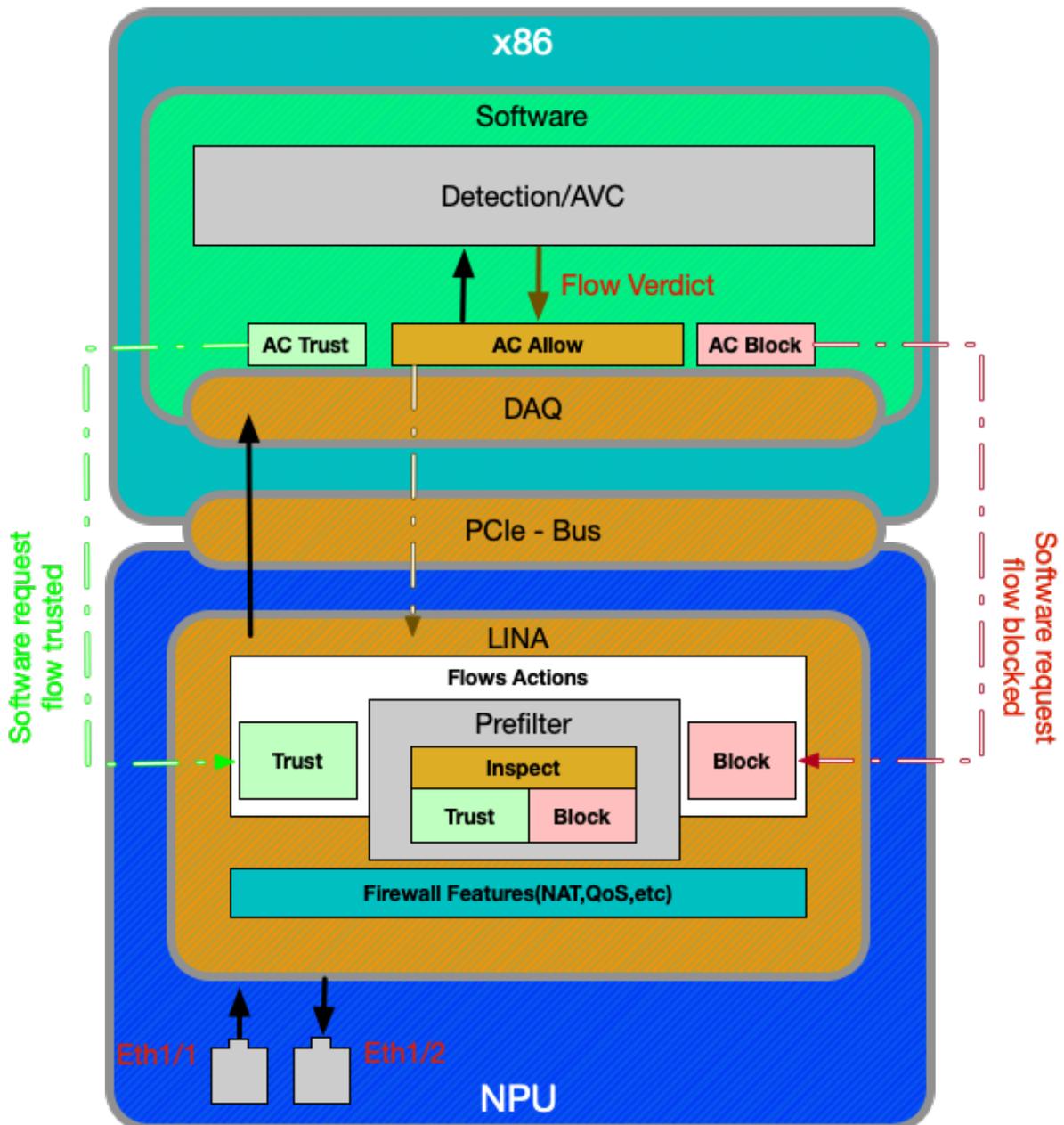
Au sein de la plate-forme SSP, il existe certaines différences entre les modèles, comme le montrent les diagrammes et les descriptions ci-dessous.

Appareils Firepower 9300 et 4100



Sur les plates-formes Firepower 9300 et 4100, les paquets d'entrée et de sortie sont gérés par un commutateur alimenté par le microprogramme FXOS (Fabric Interconnect). Les paquets sont ensuite envoyés aux interfaces affectées au périphérique logique (dans ce cas, FTD). Après cela, le traitement des paquets est identique à celui des plates-formes FTD non SSP.

Appareils Firepower 2100



Le périphérique Firepower 2100 fonctionne comme les plates-formes FTD non SSP. Il ne contient pas la couche d'interconnexion de fabric qui est présente sur les modèles 9300 et 4100. Cependant, il existe une différence majeure dans les périphériques de la gamme 2100 par rapport aux autres périphériques, à savoir la présence du circuit intégré spécifique à l'application (ASIC). Toutes les fonctionnalités ASA traditionnelles (Lina) s'exécutent sur l'ASIC, et toutes les fonctionnalités du pare-feu de nouvelle génération (NGFW) (snort, filtrage des URL, etc.) s'exécutent sur l'architecture x86 traditionnelle. La manière dont Lina et Snort communiquent sur cette plate-forme passe par une connexion PCIe (Peripheral Component Interconnect Express) via une file d'attente de paquets, contrairement aux autres plates-formes qui utilisent l'accès direct à la mémoire (DMA) pour mettre les paquets en file d'attente vers le snort.

Note: Les mêmes méthodes de dépannage des plates-formes FTD non SSP seront suivies sur la plate-forme FPR-2100.

Processus recommandé pour le dépannage du chemin de données Firepower

Maintenant que nous avons étudié comment identifier le trafic unique ainsi que l'architecture de base du chemin de données dans les plates-formes Firepower, nous examinons les endroits spécifiques où les paquets peuvent être abandonnés. Huit composants de base sont traités dans les articles Data Path, qui peuvent systématiquement dépanner pour déterminer les pertes de paquets possibles. Ceux-ci incluent :

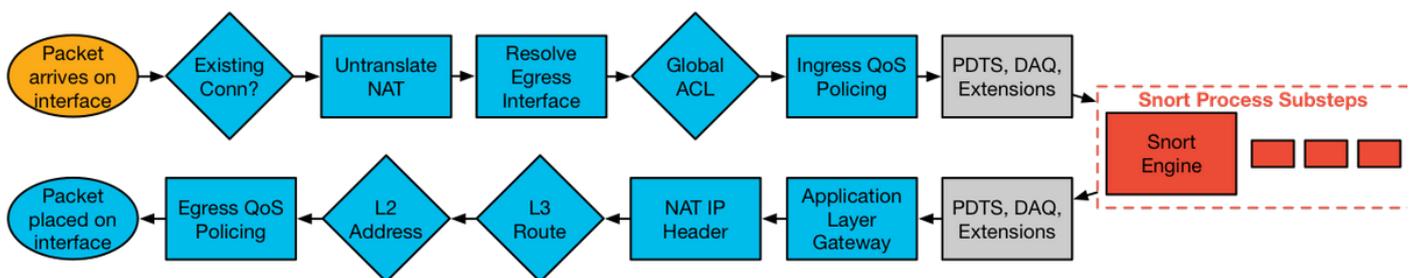
1. Paquet entrant
2. Couche DAQ Firepower
3. Intelligence de sécurité
4. Stratégie de contrôle d'accès
5. Stratégie SSL
6. Fonctionnalités d'authentification actives
7. Stratégie d'intrusion (règles IPS)
8. Stratégie d'analyse du réseau (paramètres de préprocesseur Snort)



Note: Ces composants ne sont pas répertoriés dans l'ordre exact des opérations dans le traitement de Firepower, mais sont commandés conformément à notre workflow de dépannage recommandé. Reportez-vous à l'illustration ci-dessous pour connaître le chemin réel du schéma de paquets.

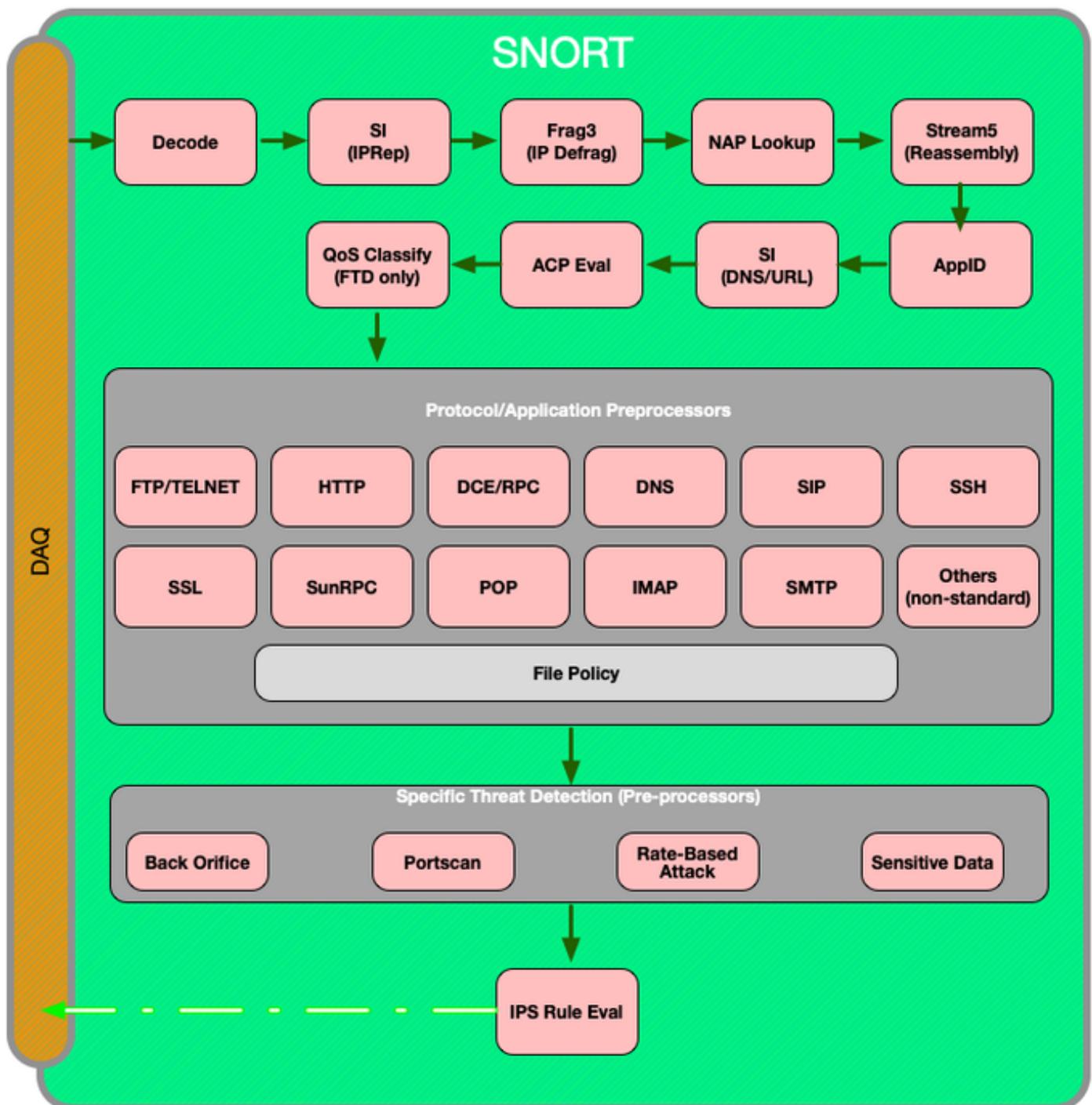
Chemin réel du paquet via FTD

L'illustration ci-dessous montre le chemin réel du paquet lorsqu'il traverse FTD.



Snort Packet Path

L'illustration ci-dessous montre le chemin du paquet via le moteur Snort.



Paquet entrant et sortant

La première étape du dépannage du chemin de données consiste à s'assurer qu'aucune perte ne se produit au stade d'entrée ou de sortie du traitement des paquets. Si un paquet est en train d'entrer mais pas de sortir, vous pouvez être sûr que le paquet est abandonné par le périphérique à un endroit quelconque du chemin de données.

Cet [article](#) explique comment dépanner l'entrée et la sortie de paquets sur les systèmes Firepower.

Couche DAQ Firepower

S'il a été déterminé que le paquet est en train d'entrer mais non en sortie, l'étape suivante du dépannage du chemin de données doit se trouver au niveau de la couche DAQ (acquisition de données) Firepower pour s'assurer que le trafic en question est envoyé à Firepower pour inspection et, dans l'affirmative, s'il est abandonné ou modifié.

Cet [article](#) explique comment dépanner le traitement initial du trafic par Firepower ainsi que le chemin qu'il emprunte sur l'ensemble de l'appareil.

Il explique également comment le périphérique Firepower peut être complètement contourné pour déterminer si un composant Firepower est responsable du problème de trafic.

Intelligence de sécurité

Security Intelligence est le premier composant de Firepower à inspecter le trafic. Les blocs de ce niveau sont très faciles à déterminer tant que la journalisation est activée. Cela peut être déterminé sur l'interface graphique de FMC en naviguant vers **Politiques > Contrôle d'accès > Politique de contrôle d'accès**. Après avoir cliqué sur l'icône de modification en regard de la stratégie en question, accédez à l'onglet **Security Intelligence**.

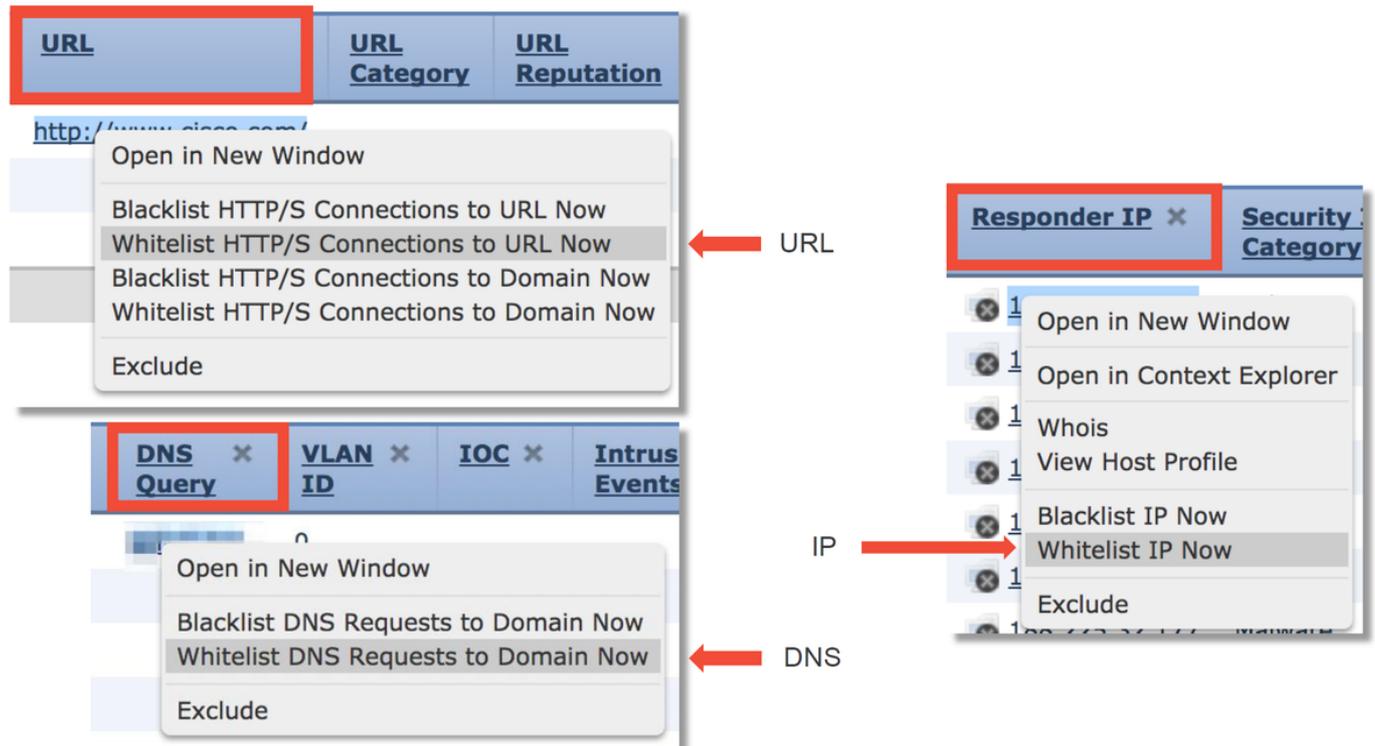
The screenshot shows the 'Security Intelligence' tab in the FMC configuration interface. It displays a list of rules under the 'Blacklist (30)' section. The 'Networks' tab is selected, showing a list of rules with their logging status. A red arrow points to the 'Logging enabled' status for the 'Networks' tab, and another red arrow points to the 'Logging disabled' status for the 'URLs' tab. A third red arrow points to the 'Edit' icon in the top right corner of the configuration area.

Rule Name	Logging Status
Attackers (Any Zone)	Logging enabled
Bogon (Any Zone)	Logging disabled
Bots (Any Zone)	Logging disabled
CnC (Any Zone)	Logging disabled
Dga (Any Zone)	Logging disabled
Exploitkit (Any Zone)	Logging disabled
Malware (Any Zone)	Logging disabled
Open_proxy (Any Zone)	Logging disabled
Phishing (Any Zone)	Logging disabled
Response (Any Zone)	Logging disabled
Spam (Any Zone)	Logging disabled
Suspicious (Any Zone)	Logging disabled
Tor_exit_node (Any Zone)	Logging disabled
Global Blacklist (Any Zone)	Logging disabled
my_custom_url (Any Zone)	Logging disabled
Global Blacklist for URL (Any Zone)	Logging disabled
URL Attackers (Any Zone)	Logging disabled
URL Bogon (Any Zone)	Logging disabled
URL Bots (Any Zone)	Logging disabled
URL CnC (Any Zone)	Logging disabled
URL Dga (Any Zone)	Logging disabled
URL Exploitkit (Any Zone)	Logging disabled
URL Malware (Any Zone)	Logging disabled
URL Open_proxy (Any Zone)	Logging disabled
URL Open_relay (Any Zone)	Logging disabled
URL Phishing (Any Zone)	Logging disabled
URL Response (Any Zone)	Logging disabled
URL Spam (Any Zone)	Logging disabled
URL Suspicious (Any Zone)	Logging disabled
URL Tor_exit_node (Any Zone)	Logging disabled

Une fois la journalisation activée, vous pouvez afficher les événements Security Intelligence sous **Analysis > Connections > Security Intelligence Events**. Il doit être clair sur la raison pour laquelle le trafic est bloqué.

First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Security Intelligence Category
2017-05-16 17:00:16		Domain Not Found	DNS Block	192.168.1.95		DNS Response
2017-05-16 16:57:50	2017-05-16 16:57:50	Block	URL Block	192.168.1.95	10.83.48.40	my_custom_url
2017-05-16 16:50:05		Block	IP Block	192.168.1.95		Malware

En guise d'étape de réduction rapide, vous pouvez cliquer avec le bouton droit sur la requête IP, URL ou DNS bloquée par la fonction Security Intelligence et choisir une option de liste blanche.



Si vous soupçonnez que quelque chose n'a pas été correctement mis sur la liste noire ou si vous souhaitez demander un changement de réputation, vous pouvez ouvrir un ticket directement auprès de Cisco Talos à l'adresse suivante :

https://www.talosintelligence.com/reputation_center/support

Vous pouvez également fournir les données au TAC pour signaler ce qui est bloqué et peut-être faire supprimer une entrée d'une liste noire.

Pour un dépannage approfondi du composant Security Intelligence, consultez l'[article](#) de dépannage du chemin de données approprié.

Stratégie de contrôle d'accès

S'il a été déterminé que la fonction Security Intelligence ne bloque pas le trafic, l'étape suivante recommandée consiste à dépanner les règles de stratégie de contrôle d'accès pour voir si une règle avec une action 'Block' abandonne le trafic.

Il est recommandé de commencer à utiliser la commande « firewall-engine-debug » ou de capturer avec trace. Généralement, ces outils peuvent vous donner la réponse immédiatement et vous dire quelle règle le trafic touche et pour quelles raisons.

- Exécutez le débogage sur l'interface de ligne de commande Firepower pour voir quelle règle bloque le trafic (assurez-vous d'entrer autant de paramètres que possible) via la commande suivante : > **prise en charge du système firewall-engine-debug**
- Le résultat du débogage peut être fourni au TAC pour analyse

Vous trouverez ci-dessous un exemple de résultat, illustrant l'évaluation des règles pour le trafic correspondant à une règle de contrôle d'accès avec l'action 'Autoriser' :

```
SHLL
> system support firewall-engine-debug

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.51
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages

192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 New session
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 Starting with minimum 3, 'block urls', 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
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 pending rule order 3, 'block urls', URL
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 Starting with minimum 3, 'block urls', and SrcZone
first with zones 1 -> 2, geo 0(0) -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 676,
payload 2655, client 638, misc 0, user 9999997, url http://www.cisco.com/, xff
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0: DataMessaging.GetURLData: Returning URL_BCTYPE
for www.cisco.com
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 rule order 3, 'block urls', URL Lookup Success:
http://www.cisco.com/ waited: 0ms
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 no match rule order 3, 'block urls',
url=(http://www.cisco.com/) c=4 r=96
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 match rule order 4, 'inspect it all', action Allow
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 allow action
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 File policy verdict is Type, Malware, and Capture
```

Si vous ne parvenez pas à déterminer quelle règle de contrôle d'accès (AC) correspond ou si vous ne parvenez pas à déterminer si la stratégie AC est le problème à l'aide des outils ci-dessus, voici quelques étapes de base pour dépanner la stratégie de contrôle d'accès (ces options ne sont pas la première option car elles nécessitent des modifications/déploiements de stratégie) :

- Activer la journalisation pour toutes les règles avec une action Bloquer
- Si vous ne voyez toujours pas d'événements de connexion pour le trafic et qu'il est bloqué, créez ensuite une règle d'approbation pour le trafic en question comme étape de réduction
- Si la règle d'approbation pour le trafic ne résout toujours pas le problème mais que vous soupçonnez toujours que la stratégie AC est en panne, créez ensuite une nouvelle stratégie de contrôle d'accès vierge si possible, en utilisant une action par défaut autre que 'Bloquer tout le trafic'

Check logging for block rules

#	Name	Sou... Zon...	Dest Zon...	Sou... Net...	Dest Net...	VLA...	Use...	App...	Sou...	Des...	URLs	ISE... Attr...	Acti...						
▼ Mandatory - My AC Policy (1-2)																			
1	block with logging	any	any	any	any	any	any	<input type="checkbox"/> YouT <input type="checkbox"/> YouTi	any	any	any	any	✗ Blocl						
2	block no logging	any	any	any	any	any	any		any	any	any	GamI any	✗ Blocl						



Add trust rule

1	Trust traffic	any	any	192.	any	any	any		any	any	any	any	→ Trus						
2	block with logging	any	any	any	any	any	any	<input type="checkbox"/> YouT <input type="checkbox"/> YouTi	any	any	any	any	✗ Bloc						
3	block no logging	any	any	any	any	any	any		any	any	any	Gam any	✗ Bloc						



Create blank AC policy

#	Name	Sour... Zones	Dest Zones	Sour... Netw...	Dest Netw...	VLAN...	Users	Appli...	Sour...	Dest ...	URLs	ISE/... Attri...	Action						
▼ Mandatory - Test - No rules (-)																			
There are no rules in this section. Add Rule or Add Category																			
▼ Default - Test - No rules (-)																			
There are no rules in this section. Add Rule or Add Category																			
Default Action												Intrusion Prevention: Balanced Security and Connectivity							

Pour un dépannage approfondi de la politique de contrôle d'accès, consultez l'[article](#) de dépannage du chemin de données approprié.

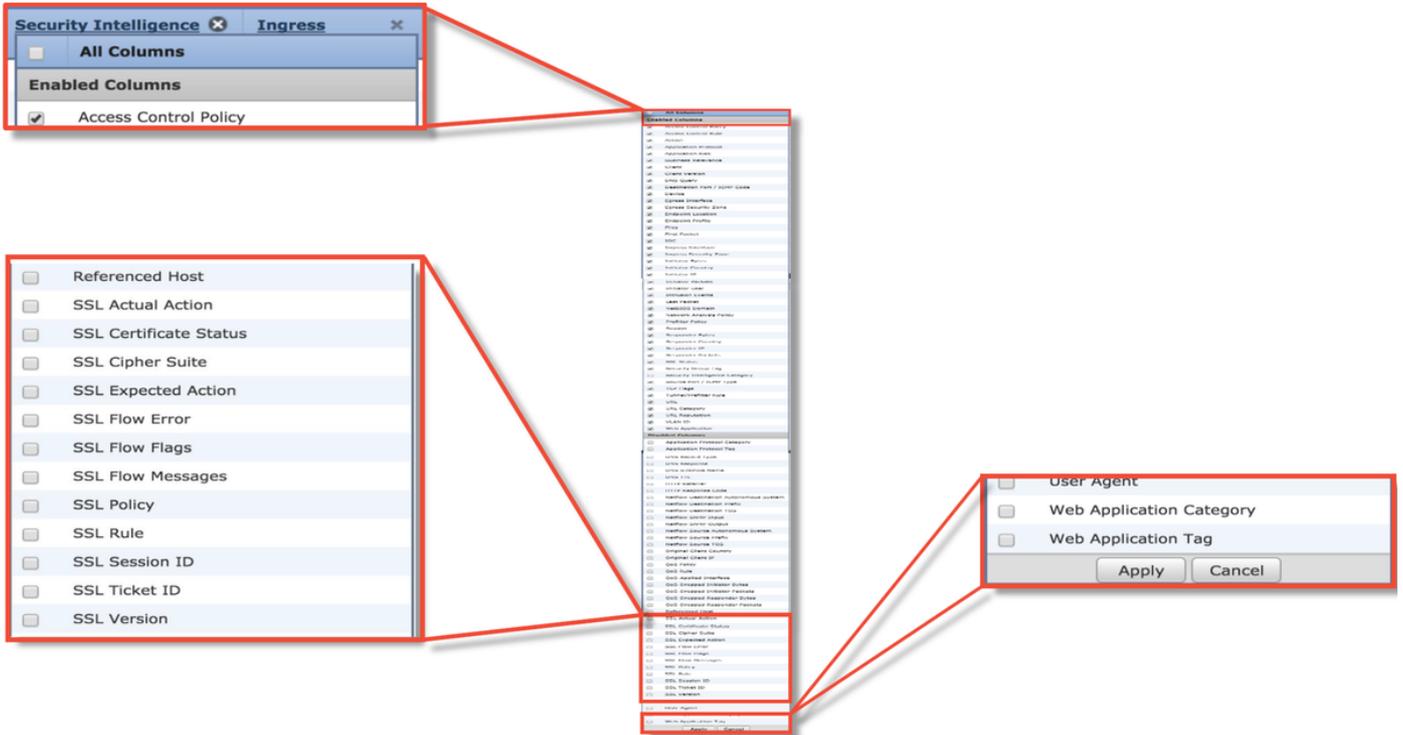
Stratégie SSL

Si la stratégie SSL est utilisée, il est possible qu'elle bloque le trafic. Voici quelques étapes de base pour dépanner la stratégie SSL :

- Activer la journalisation pour toutes les règles, y compris 'Action par défaut'

The screenshot shows the 'Editing Rule - DnD banking' dialog box in the Cisco ISE GUI. The 'Logging' tab is selected, and the 'Log at End of Connection' checkbox is checked. A red arrow points to this checkbox with the text 'Enable Logging'. The background shows a table of rules with columns for Name, Source, Destination, Action, and SSL. The 'DnD banking' rule is highlighted, and its 'Do not decrypt' action is visible.

- Cochez l'onglet Actions non décryptables pour voir si une option est définie pour bloquer le trafic
- Dans la section Événements de connexion, vérifiez tous les champs avec 'SSL' dans le nom. La plupart sont désactivées par défaut et doivent être activées dans la visionneuse Événements de connexion en cliquant sur la croix en regard de n'importe quel nom de colonne



Connection Events (switch workflow)
 Connections with Application Details > **Table View of Connection Events**
 Search Constraints (Edit Search Save Search)

SSL Blocking flow

First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country
2017-05-30 13:09:23	2017-05-30 13:09:24	Block	SSL Block	192.168.1.200		216.58.217.138	USA
2017-05-30 13:08:53	2017-05-30 13:08:54	Block	SSL Block	192.168.1.200		216.58.217.138	USA
2017-05-30 13:08:23	2017-05-30 13:08:24	Block	SSL Block	192.168.1.200		216.58.217.138	USA
2017-05-30 13:08:19	2017-05-30 13:08:20	Block	SSL Block	192.168.1.200		216.58.217.138	USA
2017-05-30 13:07:53	2017-05-30 13:07:54	Block	SSL Block	192.168.1.200		216.58.217.138	USA
2017-05-30 13:07:23	2017-05-30 13:07:24	Block	SSL Block	192.168.1.200		216.58.217.138	USA

Cause of the SSL failure

SSL Status	SSL Flow Error	SSL Actual Action	SSL Expected Action	SSL Certificate Status	SSL Version
Decrypt (Resign)	PUB_CRYPTOPENSSL_RSA_OP_FAILURE (0xb7000a20)	Decrypt (Resign)	Decrypt (Resign)	Valid	TLSv1.2
Decrypt (Resign)	PUB_CRYPTOPENSSL_RSA_OP_FAILURE (0xb7000a20)	Decrypt (Resign)	Decrypt (Resign)	Valid	TLSv1.2
Decrypt (Resign)	PUB_CRYPTOPENSSL_RSA_OP_FAILURE (0xb7000a20)	Decrypt (Resign)	Decrypt (Resign)	Valid	TLSv1.2
Decrypt (Resign)	PUB_CRYPTOPENSSL_RSA_OP_FAILURE (0xb7000a20)	Decrypt (Resign)	Decrypt (Resign)	Valid	TLSv1.2
Decrypt (Resign)	PUB_CRYPTOPENSSL_RSA_OP_FAILURE (0xb7000a20)	Decrypt (Resign)	Decrypt (Resign)	Valid	TLSv1.2
Decrypt (Resign)	PUB_CRYPTOPENSSL_RSA_OP_FAILURE (0xb7000a20)	Decrypt (Resign)	Decrypt (Resign)	Valid	TLSv1.2

SSL flow flags for what happened with flow

SSL Rule	SSL Session ID	SSL Ticket ID	SSL Flow Flags	SSL Flow Messages
MITM	0x0	0x0	VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SESSTKT, SERVER_HELLO_SESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ...	CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE
MITM	0x0	0x0	VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SESSTKT, SERVER_HELLO_SESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ...	CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE
MITM	0x0	0x0	VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SESSTKT, SERVER_HELLO_SESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ...	CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE
MITM	0x0	0x0	VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SESSTKT, SERVER_HELLO_SESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ...	CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE
MITM	0x0	0x0	VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SESSTKT, SERVER_HELLO_SESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ...	CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE
MITM	0x0	0x0	VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SESSTKT, SERVER_HELLO_SESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ...	CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE

- Créer une stratégie SSL vierge avec Ne pas déchiffrer comme action par défaut en tant qu'étape d'atténuation
- Supprimer la stratégie SSL de la stratégie de contrôle d'accès en tant qu'étape de réduction
 Cette option est définie dans l'onglet Avancé

Il est suspecté d'abandonner le trafic, les événements de connexion ainsi que la configuration de la stratégie peuvent être envoyés au TAC.

Pour un dépannage plus approfondi de la stratégie SSL, consultez [l'article](#) de dépannage du chemin de données approprié.

Authentication active

Lorsqu'elle est utilisée dans une stratégie d'identité, l'authentification active peut supprimer le trafic qui doit être autorisé en cas de problème. La fonctionnalité d'authentification active elle-même peut avoir un impact direct sur tout le trafic HTTP/HTTPS, car s'il est déterminé que nous devons authentifier un utilisateur, tout cela se produit uniquement sur le protocole HTTP. Cela signifie que l'authentification active ne doit pas avoir d'impact sur d'autres services réseau (tels que DNS, ICMP, etc.), sauf si vous avez des règles de contrôle d'accès spécifiques qui bloquent en fonction de l'utilisateur et que les utilisateurs ne peuvent pas s'authentifier via les services d'authentification actifs sur le FTD. Cependant, cela ne serait pas un problème direct de la fonctionnalité d'authentification active, mais le résultat est que les utilisateurs ne peuvent pas s'authentifier et ont une politique qui bloque les utilisateurs non authentifiés.

Une étape de réduction rapide consisterait à désactiver toute règle dans la stratégie d'identité avec l'action 'Authentification active'.

Assurez-vous également que l'option Utiliser l'authentification active si l'authentification passive ne permet pas d'identifier l'utilisateur n'est pas activée pour toutes les règles avec l'action 'Authentification passive'.

Editing Rule - Passive

Name: Passive Enabled Move

Action: Passive Authentication Realm: my-realm Authentication Type: HTTP Basic

Zones Networks VLAN Tags Ports Realm & Settings

Realm * my-realm Use active authentication if passive authentication cannot identify user

* Required Field

Make sure passive auth rules don't fall back to active auth

Remove or disable active auth rules

Or remove identity from Advanced tab of ACP

Action	Auth Type	
Active Authentication	NTLM	<input type="checkbox"/> <input type="checkbox"/>
Active Authentication	Kerberos	<input type="checkbox"/> <input type="checkbox"/>
Active Authentication	HTTP Negotiate	<input type="checkbox"/> <input type="checkbox"/>
Active Authentication	HTTP Response Pa	<input type="checkbox"/> <input type="checkbox"/>
Active Authentication	HTTP Basic	<input type="checkbox"/> <input type="checkbox"/>
Passive Authenticatio	none	<input type="checkbox"/> <input type="checkbox"/>

Identity Policy Settings

Identity Policy	
None	<input type="checkbox"/>

Dépannage plus approfondi de l'authentification active, consultez l'[article](#) de dépannage du chemin de données approprié.

Politique d'intrusion

Une stratégie d'intrusion peut entraîner une diminution du trafic ou une latence du réseau. Une stratégie d'intrusion peut être utilisée à l'un des trois endroits suivants de la stratégie de contrôle d'accès :

- Dans une règle de contrôle d'accès, dans l'onglet Inspection
- Dans l'action par défaut
- Dans l'onglet Avancé, dans la section **Stratégies d'analyse et d'intrusion de réseau > Stratégie d'intrusion utilisée avant que la règle de contrôle d'accès ne soit déterminée**

Pour savoir si une règle de stratégie d'intrusion bloque le trafic, accédez à la page **Analyse > Intrusions > Événements** du FMC. La vue **Table des événements d'intrusion** fournit des informations sur les hôtes impliqués dans ces événements. Reportez-vous à l'article de dépannage du chemin de données correspondant sur les informations relatives à l'analyse des événements.

La première étape recommandée pour déterminer si une signature de stratégie d'intrusion (IPS) bloque le trafic consiste à utiliser la fonctionnalité de **> trace de prise en charge du système** à partir de l'interface de ligne de commande du FTD. Cette commande debug fonctionne de la même manière que `firewall-engine-debug`, et elle vous donne également la possibilité d'activer `firewall-engine-debug` parallèlement à la trace.

L'illustration ci-dessous montre un exemple d'utilisation de l'outil de suivi de la prise en charge du système dans lequel le résultat a montré qu'un paquet a été bloqué en raison d'une règle d'intrusion. Vous obtenez ainsi tous les détails tels que l'ID de groupe (GID), SID (Signature Identifier), NAP (Network Analysis Policy) et l'ID IPS pour voir exactement quelle stratégie/règle bloque ce trafic.

```
SHELL
> 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 AppID: service HTTP (676), application Cisco (2655)
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 URL SI: ShmDBLookupURL("http://www.cisco.com/<?php")
returned 0

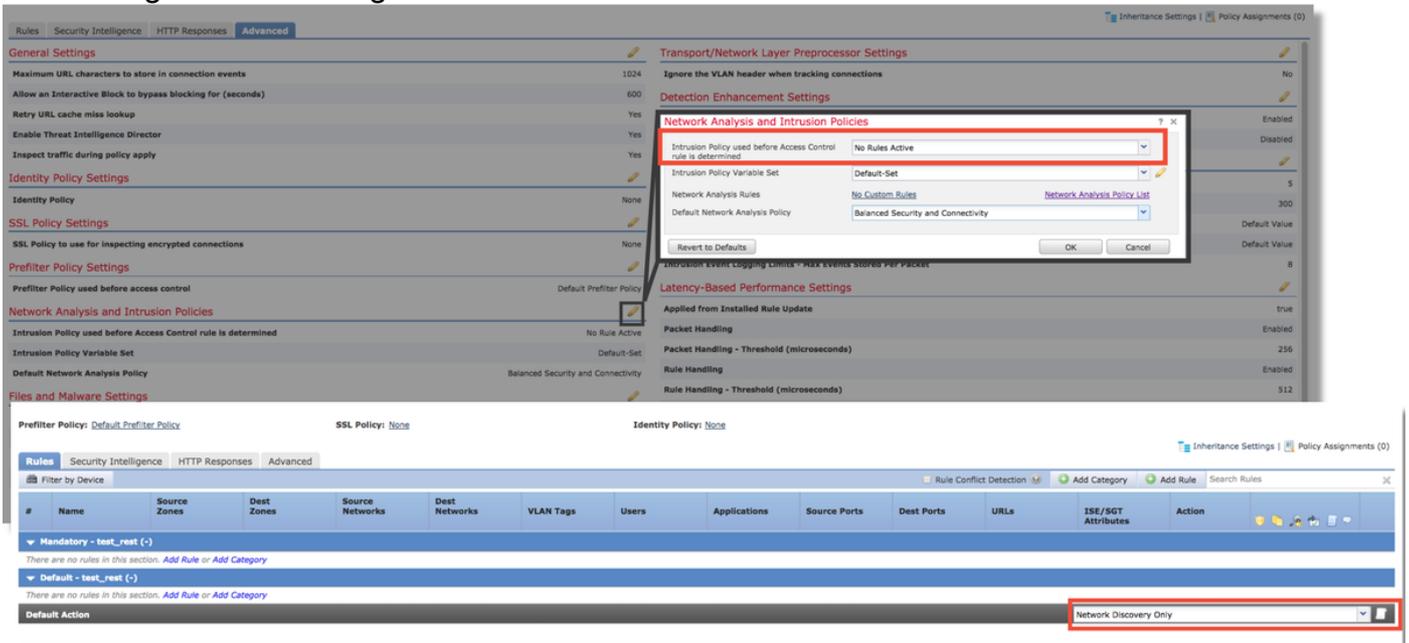
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 match rule order 5, 'inspect it all', action Allow
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 allow action
192.168.62.69-38488 > 173.37.145.84-80 6 Firewall: allow rule, 'inspect it all', allow
192.168.62.69-38488 > 173.37.145.84-80 6 IPS Event: 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 I 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
```

Si vous ne parvenez pas à déterminer si IPS bloque la sortie de trace, mais que vous soupçonnez qu'il est en train de tomber en raison d'une stratégie d'intrusion personnalisée, vous pouvez remplacer la stratégie d'intrusion par une stratégie de sécurité et de connectivité équilibrées ou une stratégie de connectivité sur la sécurité. Il s'agit de politiques d'intrusion fournies par Cisco. Si vous effectuez cette modification, résout le problème, alors la politique d'intrusion personnalisée utilisée précédemment peut être analysée par le TAC. Si une stratégie Cisco par défaut est déjà utilisée, vous pouvez essayer de remplacer la stratégie par défaut par une stratégie moins sécurisée, car ces stratégies ont moins de règles, ce qui peut aider à réduire la portée. Par exemple, si le trafic est bloqué et que vous utilisez une stratégie équilibrée, vous passez à la connectivité par rapport à la stratégie de sécurité et le problème disparaît, il est probable qu'il y ait une règle dans la stratégie équilibrée qui abandonne le trafic qui n'est pas configuré pour abandonner la connectivité par rapport à la stratégie de sécurité.

Les modifications suivantes peuvent être apportées dans la politique de contrôle d'accès pour éliminer toutes les possibilités de blocage d'inspection de la politique d'intrusion (il est

recommandé d'apporter autant de modifications que possible afin de ne pas modifier votre efficacité de sécurité. Il est donc recommandé d'établir des règles AC ciblées pour le trafic en question, plutôt que de désactiver IPS dans l'ensemble de la politique) :

- Dans toutes les règles de contrôle d'accès (ou uniquement la ou les règles correspondant au trafic concerné), supprimez la stratégie d'intrusion de l'onglet Inspection
- Dans l'onglet Avancé, dans la section **Analyse du réseau et stratégies d'intrusion > Stratégie d'intrusion utilisée avant que la règle de contrôle d'accès ne soit déterminée**, sélectionnez la stratégie « Aucune règle active ».



Si cela ne résout toujours pas le problème, passez au dépannage de la stratégie d'analyse du réseau.

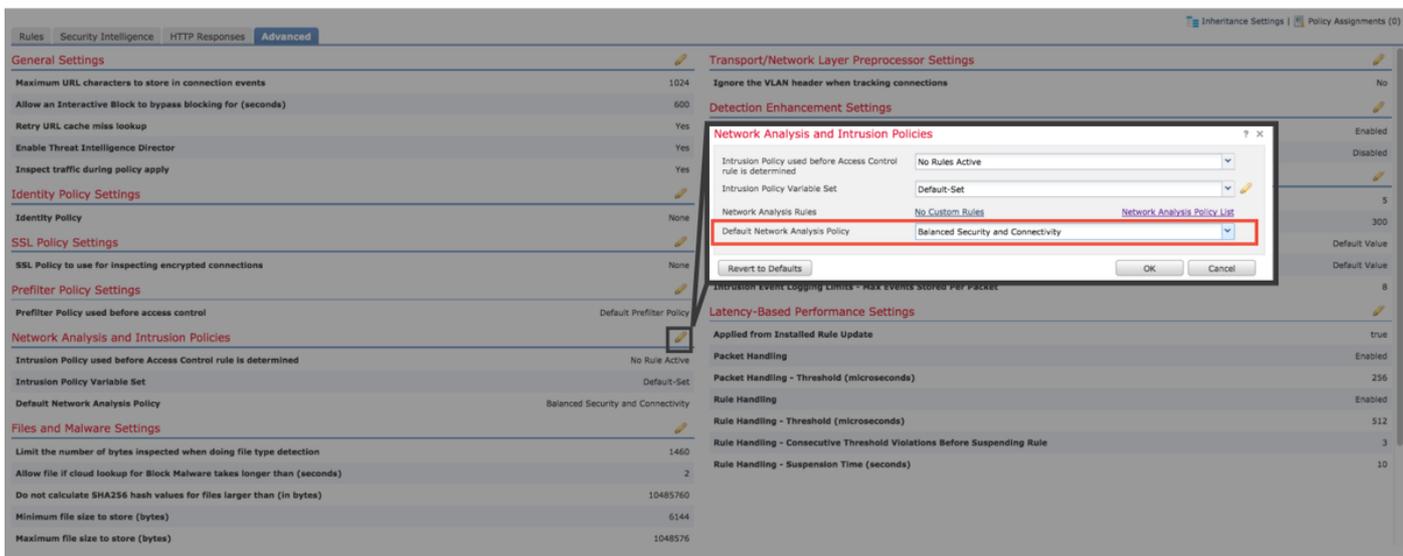
Dépannage plus approfondi de la fonction de stratégie d'intrusion, consultez l'[article](#) de dépannage du chemin de données approprié.

Stratégie d'analyse réseau

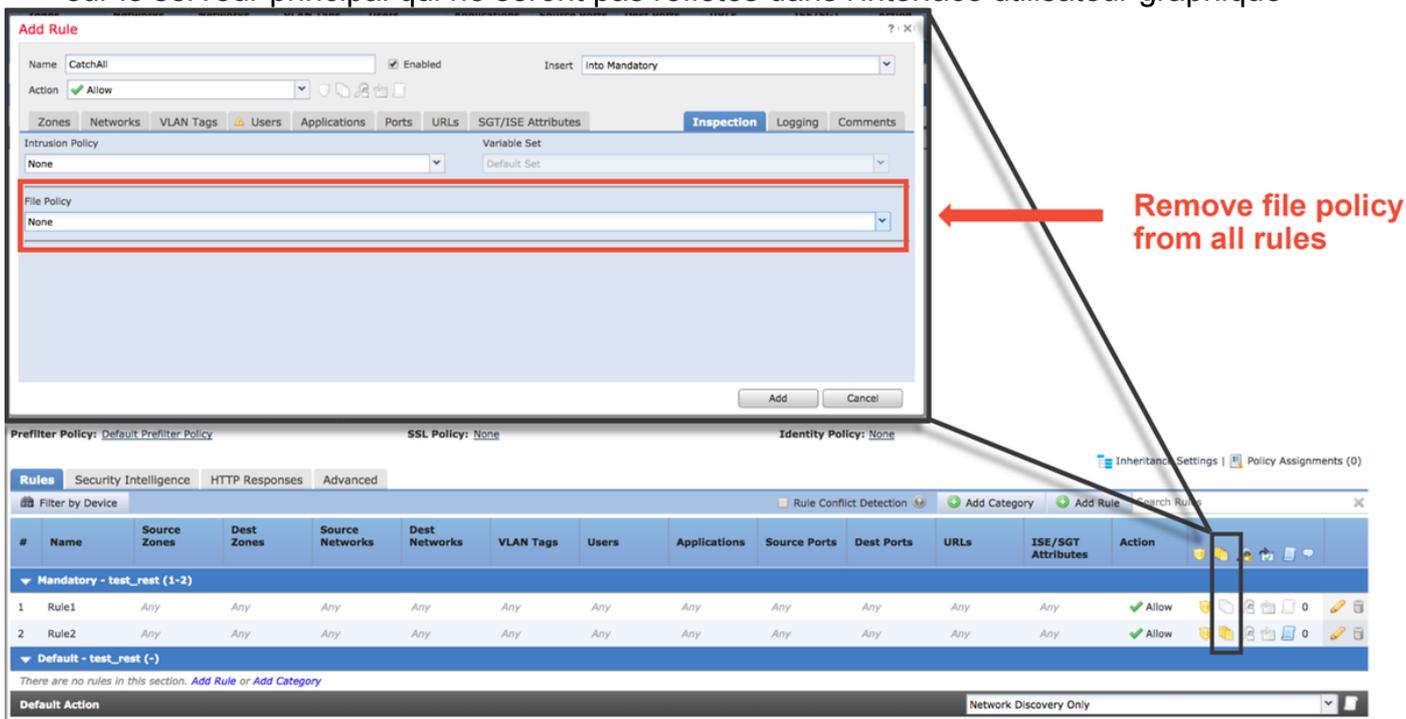
La stratégie d'analyse réseau (NAP) contient les paramètres du préprocesseur Firepower, dont certains peuvent supprimer le trafic. La première étape recommandée pour le dépannage est la même que pour le dépannage IPS, qui est d'utiliser l'outil > **system support trace** pour essayer de trouver ce qui dans snort bloque le trafic. Reportez-vous à la section « Politique d'intrusion » ci-dessus pour plus d'informations sur cet outil et sur l'utilisation de l'exemple.

Pour atténuer rapidement les problèmes éventuels liés au programme d'adaptation aux changements climatiques, vous pouvez effectuer les opérations suivantes :

- Si un NAP personnalisé est utilisé, remplacez-le par une politique 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, supprimez-la temporairement en tant que stratégie de fichier pour activer les paramètres de préprocesseur sur le serveur principal qui ne seront pas reflétés dans l'interface utilisateur graphique



Cet [article](#) présente un dépannage plus approfondi de la fonction Stratégie d'analyse du réseau.

Informations connexes

Liens vers la documentation Firepower

<https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html>