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

Contenu

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 troisième étape du dépannage du chemin de données Firepower, la fonction Security Intelligence.

Conditions préalables

- Cet article concerne toutes les plates-formes Firepower actuellement prises en charge
- Security Intelligence pour les URL et le DNS a été introduite dans la version 6.0.0

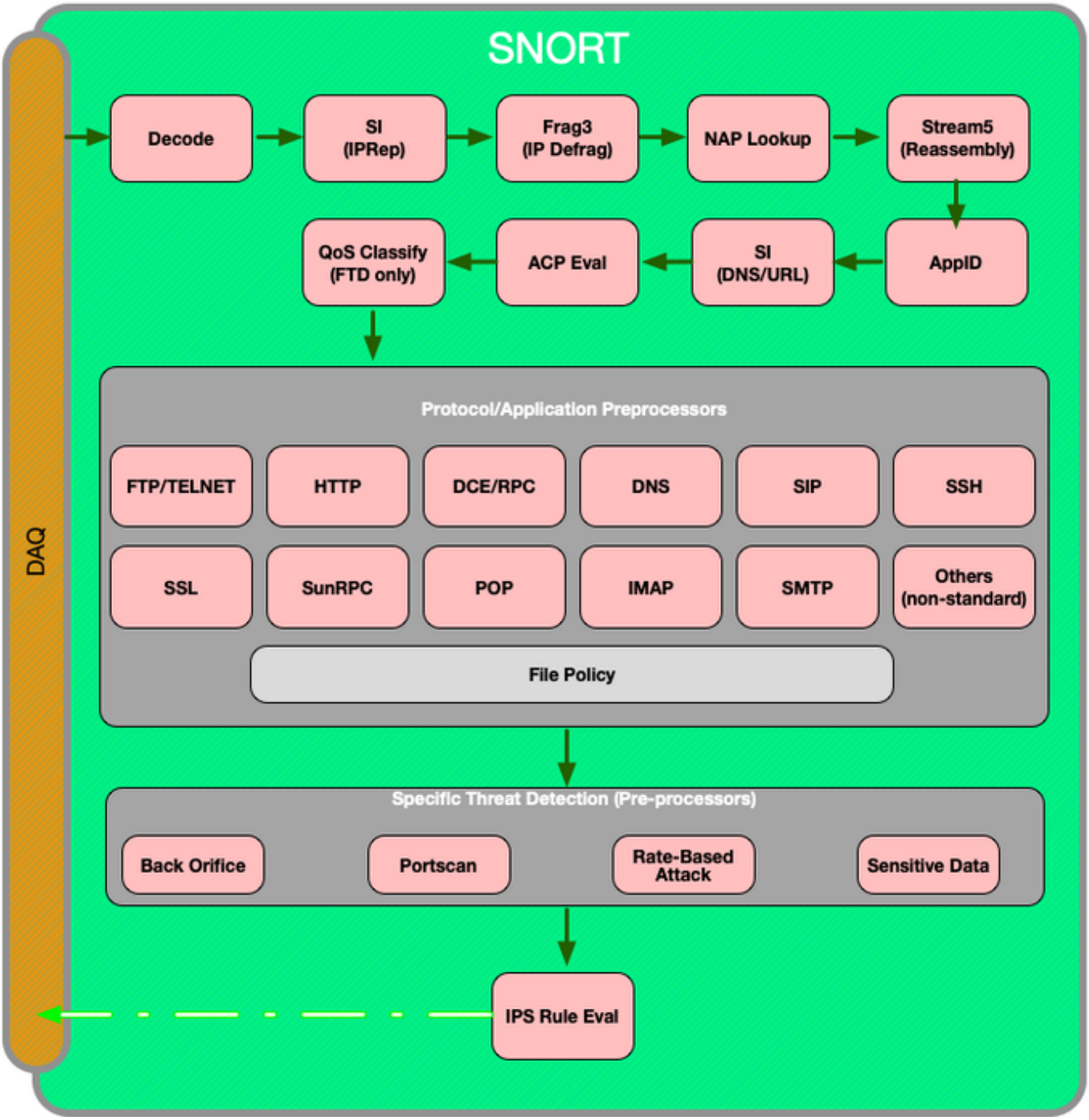
Dépannage de la phase Firepower Security Intelligence

Security Intelligence est une fonction qui effectue des inspections à la fois contre les listes de blocage et les listes blanches pour :

- Adresses IP (également appelées « réseaux » dans certaines parties de l'interface utilisateur)
- URL (Uniform Resource Locators)
- Requêtes DNS (Domain Name System)

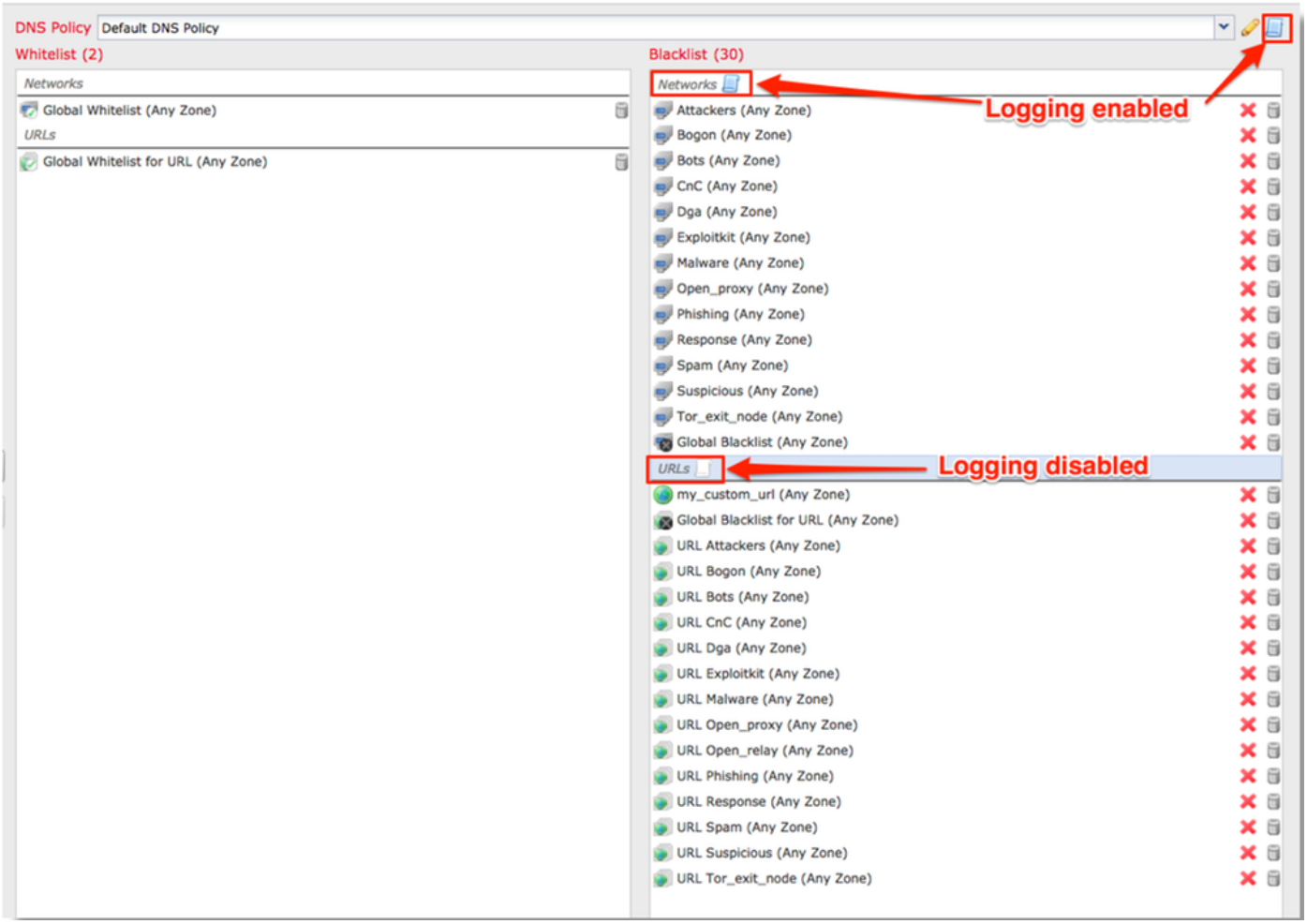
Les listes de Security Intelligence peuvent être remplies par des flux fournis par Cisco et/ou des listes et des flux configurés par l'utilisateur.

La réputation Security Intelligence basée sur les adresses IP est le premier composant de Firepower à inspecter le trafic. L'intelligence de sécurité des URL et DNS est exécutée dès que le protocole d'application approprié est découvert. Vous trouverez ci-dessous un schéma décrivant le workflow d'inspection du logiciel Firepower.



Déterminer que la journalisation est activée pour les événements Security Intelligence

Les blocs au niveau Security Intelligence sont très faciles à déterminer tant que la journalisation est activée. Cela peut être déterminé sur l'interface utilisateur de Firepower Management Center (FMC) en accédant à **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**.

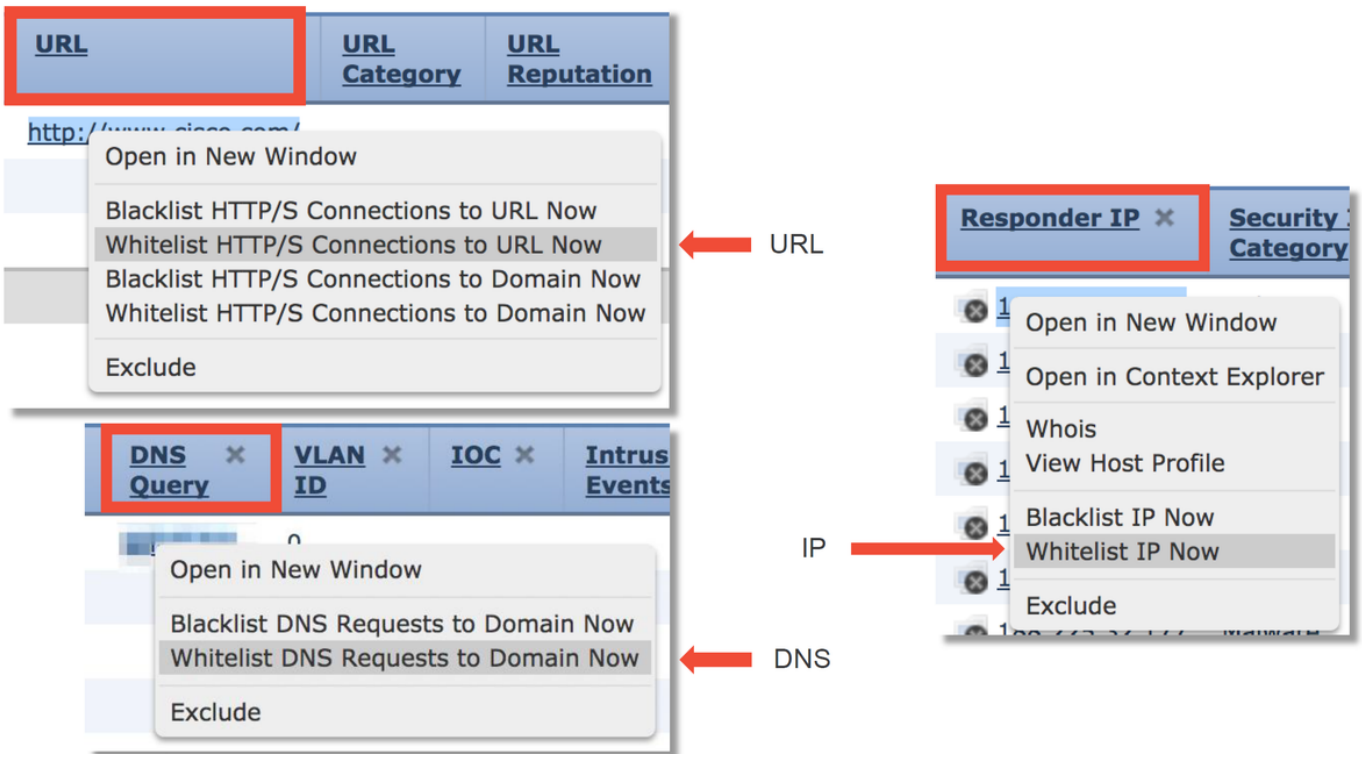


Examiner les événements Security Intelligence

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

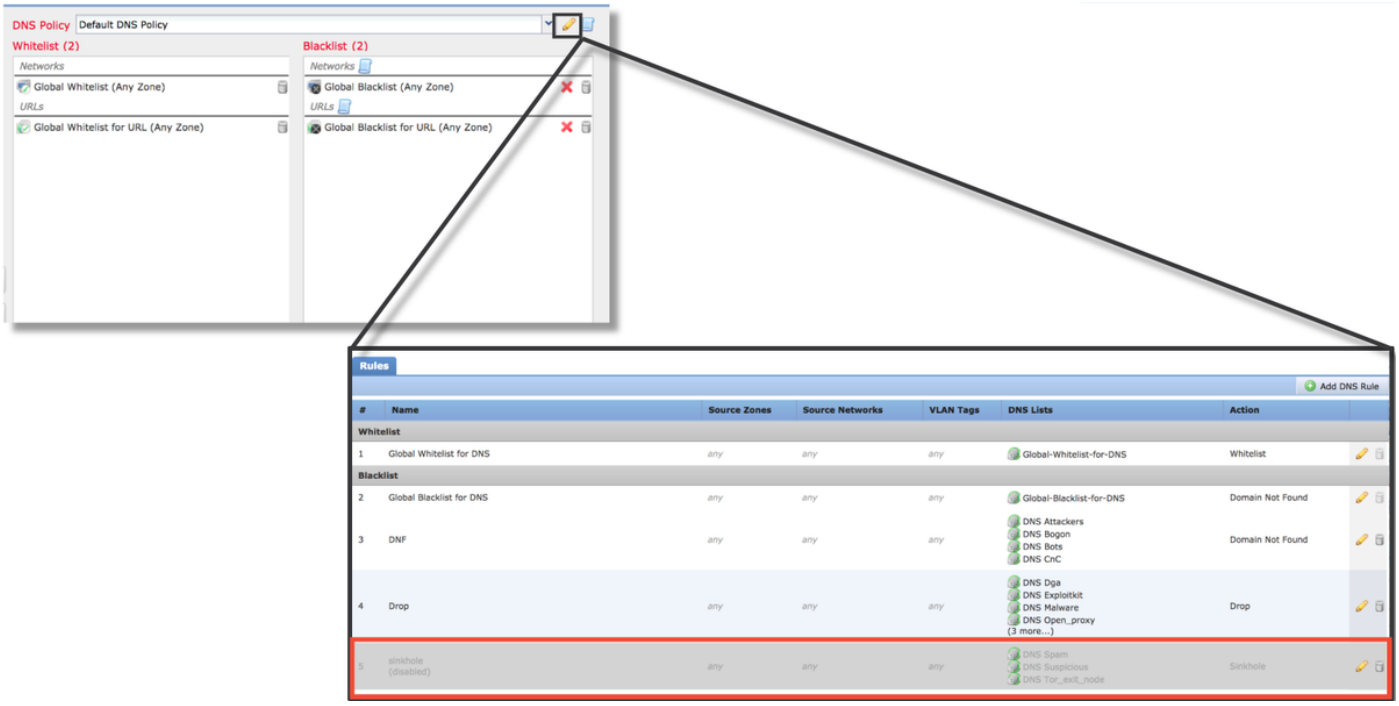
Vous pouvez également fournir les données au centre d'assistance technique Cisco (TAC) pour déterminer si un élément doit être supprimé de la liste noire.

> **Note:** L'ajout à la liste blanche ajoute uniquement une entrée à la liste blanche Security Intelligence en question, ce qui signifie que l'objet est autorisé à passer la vérification Security Intelligence. Cependant, tous les autres composants Firepower peuvent toujours inspecter le trafic.

Comment supprimer les configurations Security Intelligence

Afin de supprimer les configurations Security Intelligence, accédez à l'onglet **Security Intelligence**, comme indiqué ci-dessus. Il y a trois sections ; une pour les réseaux, l'URL ainsi qu'une politique pour DNS.

Àpartir de là, les listes et les flux peuvent être supprimés en cliquant sur le symbole de la poubelle.



Notez dans la capture d'écran ci-dessus que toutes les listes IP et URL Security Intelligence ont été supprimées, à l'exception de la liste noire et de la liste blanche globale.

Dans la stratégie DNS, où est stockée la configuration DNS Security Intelligence, une des règles est désactivée.

> **Note**: Pour afficher le contenu des listes de blocage et d'autorisation globales, accédez à **Objets > Gestion des objets > Intelligence de sécurité**. Cliquez ensuite sur la section qui vous intéresse (Réseau, URL, DNS). La modification d'une liste affiche ensuite le contenu, bien que la configuration doive être effectuée dans la stratégie de contrôle d'accès.

Vérification de la configuration sur le serveur principal

La configuration Security Intelligence peut être vérifiée sur l'interface de ligne de commande via la commande **> show access-control-config**, qui affiche le contenu de la stratégie de contrôle d'accès active exécutée sur le périphérique Firepower.

```
> show access-control-config

==================[ My AC Policy ]==================
Description              :
Default Action            : Allow
Default Policy            : SOC
Logging Configuration
   DC                   : Enabled
   Beginning             : Disabled
   End                  : Enabled
Rule Hits                 : 0
Variable Set              : Default-Set

===[ Security Intelligence - Network Whitelist ]====
   Name                 : Global-Whitelist (List)
   IP Count             : 0
   Zone                 : any

===[ Security Intelligence - Network Blacklist ]====
Logging Configuration     : Enabled
   DC                   : Enabled


--------------------[ Block ]---------------------
   Name                 : Attackers (Feed)
   Zone                 : any

   Name                 : Bogon (Feed)
   Zone                 : any
…[omitted for brevity]
```

Notez dans l'exemple ci-dessus que la journalisation est configurée pour la liste de blocage réseau et qu'au moins deux flux ont été inclus dans la liste de blocage (pirates et connexion).

Vous pouvez déterminer si un élément individuel figure dans une liste Security Intelligence en mode expert. Reportez-vous aux étapes ci-dessous :

```
> expert
$ grep <ip.addr> /var/sf/iprep_download/*
/var/sf/iprep_download/23f2a124-8278-4c03-8c9d-d28fe08b5e98.blf:<ip.addr>

$ head -1 /var/sf/iprep_download/23f2a124-8278-4c03-8c9d-d28fe08b5e98.blf
#Cisco intelligence feed: Malware



$ grep <url> /var/sf/siurl_download/*
/var/sf/siurl_download/00000000-0000-0ed3-0000-073014445223.lf:<url>

$ head -1 /var/sf/siurl_download/00000000-0000-0ed3-0000-073014445223.lf
#URL object: my_custom_url



$ grep <dns.hostname> /var/sf/sidns_download/*
/var/sf/sidns_download/032ba433-c295-11e4-a919-d4ae5275b77b.lf: <dns.hostname>

$ head -1 /var/sf/sidns_download/032ba433-c295-11e4-a919-d4ae5275b77b.lf
#Cisco DNS and URL intelligence feed: DNS Response
```

IP SI lists are in /var/sf/iprep_download/

URL SI lists are in /var/sf/siurl_download/

DNS SI lists are in /var/sf/sidns_download/

Il existe un fichier pour chaque liste Security Intelligence avec un UUID unique. L'exemple ci-

dessus montre comment identifier le nom de la liste à l'aide de la commande **head -n1**.

Données à fournir au TAC

Données	Instructions
Dépanner les fichiers du FMC et du périphérique Firepower inspectant le trafic	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-techn
Captures d'écran des événements (avec horodatage inclus)	Reportez-vous à cet article pour obtenir des instructions.
Sortie de texte des sessions CLI	Reportez-vous à cet article pour obtenir des instructions.
Si vous soumettez un cas faux positif, indiquez l'élément (IP, URL, domaine) à contester.	Fournir les motifs et les preuves de l'exécution du différend.

Étape suivante

S'il a été déterminé que le composant Security Intelligence n'est pas la cause du problème, l'étape suivante consiste à dépanner les règles de la stratégie de contrôle d'accès.

Cliquez ici pour passer à l'article suivant.