Dépannage

Les rubriques suivantes décrivent les façons de diagnostiquer les problèmes que vous pouvez rencontrer avec le système Firepower :

Premiers pas de dépannage

- Avant d'apporter des modifications pour tenter de résoudre un problème, générez un fichier de dépannage pour capturer le problème d'origine. Consultez Rapports de surveillance de l'intégrité pour le dépannage, à la page 14 et ses sous-sections.

  Vous aurez peut-être besoin de ce fichier de dépannage si vous devez communiquer avec l'assistance technique TAC de Cisco pour obtenir de l'aide.

- Commencez votre recherche en consultant les messages d'erreur et d'avertissement dans le centre de messages. Voir la section Messages système, à la page 2.

- Recherchez les notes techniques applicables et d'autres ressources de dépannage sous l'en-tête « Dépannage et alertes » sur la page de documentation de votre produit. Consultez Premiers pas de dépannage, à la page 1.

Messages système

Lorsque vous devez retracer des problèmes qui se produisent dans le système Firepower, le centre de messages est l'endroit où commencer votre enquête. Cette fonctionnalité vous permet de visualiser les messages que le système Firepower génère continuellement sur les activités et l'état du système.

Pour ouvrir le centre de messages, cliquez sur l'icône d'état du système, située à côté du menu Deploy (déployer) dans le menu principal. Cette icône peut prendre l'une des formes suivantes, selon l'état du système :

- : Indique qu'une ou plusieurs erreurs et un certain nombre d'avertissements sont présents sur le système.
- : indique un ou plusieurs avertissements et qu'aucune erreur n'est présente sur le système.
- : Indique qu'aucun avertissement ou erreur n'est présent sur le système.

Si un nombre est associé à l'icône , il s'agit du nombre total actuel de messages d'erreur ou d'avertissement.

Pour fermer le centre de messages, cliquez n'importe où en dehors de celui-ci dans l'interface Web du système Firepower.

En plus du centre de messages, l'interface Web affiche des notifications contextuelles en réponse immédiate à vos activités et aux activités en cours sur le système. Certaines notifications contextuelles disparaîtront automatiquement après cinq secondes, tandis que d'autres sont « persistantes », c'est-à-dire qu'elles s'affichent jusqu'à ce que vous les fermez explicitement en cliquant sur **Ignorer** (). Cliquez sur le lien **Supprimer** en haut de la liste des notifications pour fermer toutes les notifications à la fois.

Astuces Si vous passez votre curseur sur une notification contextuelle non persistante, celle-ci devient persistante.

Le système détermine les messages qu'il affiche aux utilisateurs dans les notifications contextuelles et dans le centre de messages en fonction de leurs licences, domaines et rôles d'accès.

Types de message

Le centre de messages affiche des messages signalant les activités et l'état du système, organisés sous trois onglets différents :

Déploiements

Cet onglet affiche l'état actuel du déploiement de la configuration pour chaque appareil de votre système, regroupé par domaine. Le système signale les valeurs d'état de déploiement suivantes sous cet onglet. Vous pouvez obtenir des renseignements supplémentaires sur les tâches de déploiement en cliquant sur **Afficher l'historique**.

- En cours d'exécution (**Spinning**) : la configuration est en cours de déploiement.
- **Success** (réussite) : la configuration a été déployée avec succès.
- **Avertissement** () : les états de déploiement des avertissements contribuent au nombre de messages affichés en même temps que l'**icône d'avertissement concernant l'état du système**.

- **Failure** (échec) : la configuration n'a pas pu être déployée; voir Modifications de la configuration qui nécessitent un déploiement. Les déploiements échoués contribuent au nombre de messages affichés en même temps que l'**icône d'erreur d'état du système**.

Mises à Niveau

Cet onglet affiche l'état actuel des tâches de mise à niveau logicielle pour les périphériques gérés. Le système signale les valeurs d'état de mise à niveau suivantes sous cet onglet :

- **En cours** : indique que la tâche de mise à niveau est en cours.
- **Terminée** : Indique que la tâche de mise à niveau logicielle s'est terminée avec succès.
- **Échec** : indique que la tâche de mise à niveau logicielle ne s'est pas terminée.

Santé

Cet onglet affiche des renseignements sur l'état d'intégrité actuel de chaque appareil de votre système, regroupés par domaine. L'état d'intégrité est généré par les modules d'intégrité comme décrit dans À propos de la surveillance de l'intégrité. Le système signale les valeurs d'état d'intégrité suivantes sous cet onglet :

- **Avertissement** () : indique que les limites d'avertissement ont été dépassées pour un module d'intégrité sur un appareil et que le problème n'a pas été corrigé. La page Health Monitoring (surveillance de l'intégrité) indique ces conditions par un **Triangle jaune** (). Les états d'avertissement contribuent au nombre de messages affichés avec l'**icône d'avertissement concernant l'état du système** .
- **Critique** () : Indique que les limites critiques ont été dépassées pour un module d'intégrité sur un appareil et que le problème n'a pas été corrigé. La page Health Monitoring (surveillance de l'intégrité) indique ces conditions par une icône **Critique** (). Les états critiques contribuent au nombre de messages affichés avec l'**icône d'erreur dans l'état du système** .
- **Erreur** () : Indique qu'un module de surveillance de l'intégrité est défaillant sur un appareil et n'a pas été réexécuté avec succès depuis que la défaillance s'est produite. La page Health Monitoring (surveillance de l'intégrité) indique ces conditions par une **icône d'erreur** . Les états d'erreur contribuent au nombre de messages affichés avec l'**icône d'erreur dans l'état du système** .

Vous pouvez cliquer sur les liens dans l'onglet Health (intégrité) pour afficher des informations détaillées connexes sur la page de surveillance de l'intégrité. S'il n'y a aucune condition d'état d'intégrité actuelle, l'onglet Health (intégrité) n'affiche aucun message.

Tâches

Certaines tâches (comme les sauvegardes de configuration ou l'installation des mises à jour) peuvent prendre un certain temps. Cet onglet affiche l'état de ces tâches de longue durée et peut inclure des tâches initiées par vous ou, si vous avez les accès appropriés, par d'autres utilisateurs du système. Cet onglet présente les messages dans l'ordre chronologique inverse en fonction de l'heure de mise à jour la plus récente pour chaque message. Certains messages d'état de tâches comprennent des liens vers des informations plus détaillées sur la tâche en question. Le système signale les valeurs d'état de tâche suivantes sous cet onglet :

- **En attente**() : indique une tâche en attente d'exécution jusqu'à ce qu'une autre tâche en cours soit terminée. Ce type de message affiche une barre de progression mise à jour.

- En cours d'**exécution** : indique une tâche en cours. Ce type de message affiche une barre de progression mise à jour.
- **Nouvelle tentative** : indique une tâche qui effectue une nouvelle tentative automatiquement. Notez que toutes les tâches ne sont pas autorisées à réessayer. Ce type de message affiche une barre de progression mise à jour.
- **Réussite** : indique une tâche qui s'est terminée avec succès.
- **Échec** indique une tâche qui ne s'est pas terminée avec succès. Les tâches ayant échoué contribuent au nombre de messages affichés avec l'**icône d'erreur d'état du système**.
- **Arrêtée ou suspendue** : indique une tâche qui a été interrompue en raison d'une mise à jour du système. Les tâches arrêtées ne peuvent pas être reprises. Une fois les opérations normales rétablies, redémarrez la tâche.
- Ignorée : un processus en cours a empêché la tâche de démarrer. Réessayez de démarrer la tâche.

De nouveaux messages s'affichent dans cet onglet au fur et à mesure que de nouvelles tâches sont démarrées. Lorsque les tâches sont terminées (états de réussite, d'échec ou arrêtée), cet onglet continue d'afficher des messages avec l'état final indiqué jusqu'à ce que vous les supprimiez. Cisco vous recommande de supprimer les messages pour réduire l'encombrement dans l'onglet Tasks (Tâches) ainsi que dans la base de données des messages.

Gestion des messages

À partir du centre de messages, vous pouvez :

- Choisissez d'afficher les notifications contextuelles.
- Affichez d'autres messages d'état des tâches provenant de la base de données du système (s'il en existe qui n'ont pas été supprimés).
- Supprimez les messages d'état des tâches individuelles. (Cela affecte tous les utilisateurs qui peuvent afficher les messages supprimés.)
- Supprimez les messages d'état des tâches en bloc. (Cela affecte tous les utilisateurs qui peuvent afficher les messages supprimés.)

Astuces Cisco vous recommande de supprimer régulièrement les messages d'état des tâches accumulés de l'onglet Task (Tâches) pour réduire l'encombrement à l'écran et dans la base de données. Lorsque le nombre de messages dans la base de données approche des 100 000, le système supprime automatiquement les messages d'état des tâches que vous avez supprimés.

Afficher les informations de base sur le système

La page À propos de affiche des informations sur votre appareil, notamment le modèle, le numéro de série et les informations sur la version des divers composants du système. Elles comprennent également des informations sur les droits d'auteur de Cisco.

Procédure

Étape 1 Cliquez sur **Aide** ( ) dans la barre d'outils en haut de la page.

Étape 2 Choisissez **À propos de**.

Afficher les Informations relatives à l'appareil

Procédure

Choisissez **System** ( ) > **Configuration**.

Gestion des messages système

Procédure

Étape 1 Cliquez sur **Notifications** pour afficher le centre de messages.

Étape 2 Vous avez les choix suivants :

- Cliquez sur **Deployments** (Déploiements) pour afficher les messages relatifs aux déploiements de configuration. Consultez Affichage des messages de déploiement, à la page 6. Vous devez être un utilisateur Admin ou avoir l'autorisation de déployer la configuration sur les appareils (**Deploy Configuration to Devices**) pour afficher ces messages.
- Cliquez sur **Mises à niveau** pour afficher les messages relatifs aux tâches de mise à niveau de périphériques. Reportez-vous à la section Affichage des messages de mise à niveau. Reportez-vous à la section Affichage des messages de mise à niveau. Vous devez être un utilisateur Admin ou avoir l'autorisation **Updates** (mises à jour) pour voir ces messages.
- Cliquez sur **Health** (intégrité) pour afficher les messages relatifs à l'intégrité de votre centre de gestion et des périphériques qui y sont enregistrés. Consultez Affichage des messages d'intégrité, à la page 7. Vous devez être un utilisateur Admin ou avoir l'autorisation **Health** (Intégrité) pour voir ces messages.

  Vous pouvez accéder à la page Health Monitor (Moniteur d'intégrité) en cliquant sur le lien **Health Monitor**.

- Cliquez sur **Tasks** pour afficher ou gérer les messages relatifs aux tâches de longue durée. Reportez-vous aux sections Affichage des messages en lien avec les tâches, à la page 8 ou Gestion des messages relatifs aux tâches, à la page 8. Chacun peut voir ses propres tâches. Pour voir les tâches d'autres utilisateurs, vous devez être un administrateur ou avoir l'autorisation de consulter les tâches des autres utilisateurs (**View Other Users' Tasks**). Vous pouvez supprimer les tâches terminées de la notification en cliquant sur le lien **Supprimer les tâches terminées**.

- Cliquez sur le curseur **Show Notifications** (Afficher les notifications) pour activer ou désactiver l'affichage des notifications contextuelles.

Affichage des messages de déploiement

Vous devez être un utilisateur Admin ou avoir l'autorisation de déployer la configuration sur les appareils (**Deploy Configuration to Devices**) pour afficher ces messages.

Procédure

Étape 1 Cliquez sur **Notifications** pour afficher le centre de messages.

Étape 2 Cliquez sur **Deployments** (déploiements).

Étape 3 Vous avez les choix suivants :

- Cliquez sur **total** pour afficher les états de toutes les déploiements en cours.
- Cliquez sur une valeur d'état pour afficher uniquement les messages avec cet état de déploiement.
- Placez votre curseur sur l'indicateur de temps écoulé pour un message (par exemple, **1 min 5s**) pour afficher le temps écoulé et les heures de début et de fin du déploiement.

Étape 4 Cliquez sur afficher **l'historique de déploiement** pour afficher des informations plus détaillées sur les tâches de déploiement.

Le tableau historique de déploiement répertorie les tâches de déploiement dans la colonne de gauche dans l'ordre chronologique inverse.

a) Sélectionnez un travail de déploiement.

Le tableau dans la colonne de droite affiche chaque périphérique inclus dans le travail et l'état de déploiement par périphérique.

b) Pour afficher les réponses de l'appareil et les commandes envoyées à l'appareil pendant le déploiement, cliquez sur télécharger dans la colonne **Transcript** (transcription) de l'appareil.

Elle comprend les sections suivantes :

- **Snort Apply** : En cas de défaillance ou de réponse des politiques Snort, des messages apparaissent dans cette section. Normalement, la section est vide.
- **CLI Apply** : Cette section couvre les fonctionnalités qui sont configurées à l'aide des commandes envoyées au processus Lina.
- **Infrastructure Messages** : Cette section affiche l'état des différents modules de déploiement.

Dans la section **CLI Apply**, la transcription de déploiement comprend les commandes envoyées à l'appareil et toutes les réponses renvoyées par l'appareil. Ces réponses peuvent être des messages informatifs ou des messages d'erreur. En cas d'échec des déploiements, recherchez les messages indiquant des erreurs dans les commandes. L'examen de ces erreurs peut être particulièrement utile si vous utilisez des règles FlexConfig pour configurer des fonctionnalités personnalisées. Ces erreurs peuvent vous aider à corriger le script dans l'objet FlexConfig qui tente de configurer les commandes.

Remarque Il n'y a aucune distinction faite dans la transcription entre les commandes envoyées pour les fonctionnalités gérées et celles générées par les politiques FlexConfig.

Par exemple, la séquence suivante montre que les commandes centre de gestion envoyées pour configurer GigabitEthernet0/0 avec le nom logique à l'extérieur. L'appareil a répondu qu'il avait automatiquement réglé le niveau de sécurité sur 0. Le défense contre les menaces n'utilise pas le niveau de sécurité pour quoi que ce soit.

```
========= CLI APPLY =========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

Affichage des messages de mise à niveau

Vous devez être un utilisateur Admin ou avoir l'autorisation **Updates** (mises à jour) pour voir ces messages.

Procédure

Étape 1 Cliquez sur **Notifications** pour afficher le centre de messages.

Étape 2 Cliquez sur **Mises à niveau**.

Étape 3 Vous pouvez effectuer les opérations suivantes :

- Cliquez sur **total** pour afficher les états de toutes les tâches en cours.
- Cliquez sur une valeur d'état pour afficher uniquement les messages comportant cet état.
- Cliquez sur **Device Management** (Gestion des périphériques) pour plus de détails sur la tâche de mise à niveau.

Affichage des messages d'intégrité

Vous devez être un utilisateur Admin ou avoir l'autorisation **Health** (Intégrité) pour voir ces messages.

Procédure

Étape 1 Cliquez sur **Notifications** pour afficher le centre de messages.

Étape 2 Cliquez sur **Health** (intégrité).

Étape 3 Vous avez les choix suivants :

- Cliquez sur **total** pour afficher tous les états d'intégrité en cours. La répartition selon la gravité, à savoir avertissement, critique et erreur, est également affichée.
- Cliquez sur une valeur d'état pour afficher uniquement les messages comportant cet état.
- Placez votre curseur sur l'indicateur d'heure relative d'un message (par exemple, **il y a 3 jours**) pour afficher l'heure de la dernière mise à jour de ce message.

- Pour afficher des informations détaillées sur l'intégrité d'un message en particulier, cliquez sur le message.
- Pour afficher l'état d'intégrité complet dans la page Health Monitoring (surveillance de l'intégrité), cliquez sur **Health Monitor** (Surveiller l'intégrité).

Affichage des messages en lien avec les tâches

Chacun peut voir ses propres tâches. Pour voir les tâches d'autres utilisateurs, vous devez être un administrateur ou avoir l'autorisation de consulter les tâches des autres utilisateurs (**View Other Users' Tasks**).

Procédure

Étape 1 Cliquez sur **Notifications** pour afficher le centre de messages.

Étape 2 Cliquez sur **Tasks** (tâches).

Étape 3 Vous avez les choix suivants :

- Cliquez sur **total** pour afficher les états de toutes les tâches en cours. Pour afficher les tâches en fonction de l'état, à savoir en attente, en cours d'exécution, nouvelle tentative, réussite et échec, cliquez sur celles-ci.
- Cliquez sur une valeur d'état pour afficher uniquement les messages pour les tâches correspondant à cet état.

  Remarque Les messages pour les tâches arrêtées apparaissent uniquement dans la liste totale des messages liés aux état des tâches. Vous ne pouvez pas filtrer les tâches arrêtées.

- Placez votre curseur sur l'indicateur d'heure relative d'un message (par exemple, **il y a 3 jours**) pour afficher l'heure de la dernière mise à jour de ce message.
- Cliquez sur un lien dans un message pour afficher plus d'informations sur la tâche.
- Si d'autres messages sur l'état des tâches peuvent être affichés, cliquez sur **Fetch more messages** au bas de la liste des messages pour les récupérer.

Gestion des messages relatifs aux tâches

Chacun peut voir ses propres tâches. Pour voir les tâches d'autres utilisateurs, vous devez être un administrateur ou avoir l'autorisation de consulter les tâches des autres utilisateurs (**View Other Users' Tasks**).

Procédure

Étape 1 Cliquez sur System Status (état du système) pour afficher le centre de messagerie (Message Center).

Étape 2 Cliquez sur Tasks (tâches).

Étape 3 Vous avez les choix suivants :

- Si d'autres messages sur l'état des tâches peuvent être affichés, cliquez sur **Fetch more messages** (Récupérer d'autres messages) au bas de la liste des messages pour les récupérer.

- Pour supprimer un message pour une tâche terminée (état arrêté, réussite ou échec), cliquez sur **Enlever** ( ) à côté du message.
- Pour supprimer tous les messages pour toutes les tâches qui sont terminées (état arrêté, réussite ou échec), filtrez les messages par **total** et cliquez sur **Supprimer toutes les tâches terminées**.
- Pour supprimer tous les messages pour toutes les tâches qui se sont terminées avec succès, filtrez les messages en fonction de la **réussite**, et cliquez sur **Supprimer toutes les tâches réussies**.
- Pour supprimer tous les messages pour toutes les tâches qui ont échoué, filtrez les messages en fonction de l' **échec**et cliquez sur **Supprimer toutes les tâches ayant échoué**.

Seuils d'utilisation de la mémoire pour les alertes de la surveillance de l'intégrité

Le module d'intégrité Utilisation de la mémoire compare l'utilisation de la mémoire sur un appareil aux limites configurées pour le module et alerte lorsque l'utilisation dépasse les niveaux configurés. Le module surveille les données des périphériques gérés et de centre de gestion.

Deux seuils configurables pour l'utilisation de la mémoire, Critique et Avertissement, peuvent être définis en tant que pourcentage de mémoire utilisée. Lorsque ces seuils sont dépassés, une alarme d'intégrité est générée avec le niveau de gravité spécifié. Cependant, le système d'alerte d'intégrité ne calcule pas ces seuils de manière exacte.

Avec les périphériques disposant d'une capacité de mémoire élevée, certains processus sont susceptibles d'utiliser un pourcentage plus important de la mémoire totale du système qu'avec un périphérique à faible capacité de mémoire. Le principe de conception est d'utiliser autant de mémoire physique que possible tout en laissant une petite valeur de mémoire libre pour les processus auxiliaires.

Comparez deux périphériques, un avec 32 Go de mémoire et l'autre avec 4 Go de mémoire. Pour le périphérique doté de 32 Go de mémoire, 5 % de la mémoire (1,6 Go) est une valeur de mémoire beaucoup plus importante à réserver aux processus auxiliaires que dans le cas du périphérique doté de 4 Go de mémoire (5 % de 4 Go = 200 Mo).

Pour tenir compte du pourcentage d'utilisation plus élevé de la mémoire système par certains processus, le centre de gestion calcule la mémoire totale de manière à inclure la mémoire physique totale et la mémoire totale d'échange (swap). Ainsi, l'application du seuil de mémoire pour le seuil configuré par l'utilisateur peut entraîner un événement d'intégrité dans lequel la colonne « Value » de l'événement ne correspond pas à la valeur saisie pour déterminer le seuil dépassé.

Le tableau suivant donne des exemples de seuils saisis par l'utilisateur et de seuils appliqués, en fonction de la mémoire système installée.

Remarque Les valeurs dans ce tableau sont des exemples. Vous pouvez utiliser ces renseignements pour extrapoler les seuils des périphériques qui ne correspondent pas à la quantité de RAM installée indiquée ici, ou vous pouvez communiquer avec Cisco TAC pour obtenir des calculs de seuil plus précis.

Tableau 1 : Seuils d'utilisation de la mémoire en fonction de la RAM installée

Valeur de seuil saisie par l'utilisateur	Seuil appliqué par mémoire installée (RAM)			
	4 Go	6 Go	32 Go	48 Go
10 %	10 %	34 %	72 %	81 %
20 %	20 %	41 %	75 %	83 %
30 %	30 %	48 %	78 %	85 %
40 %	40 %	56 %	81 %	88 %
50 %	50 %	63 %	84 %	90 %
60 %	60 %	70 %	88 %	92 %
70 %	70 %	78 %	91 %	94 %
80 %	80 %	85 %	94 %	96 %
90 %	90 %	93 %	97 %	98 %
100 %	100 %	100 %	100 %	100 %

Utilisation du disque et vidage des événements d'alertes du moniteur d'intégrité

Le module d'intégrité de l'utilisation du disque compare l'utilisation du disque sur le disque dur d'un périphérique géré et l'ensemble de stockage de logiciel malveillant aux limites configurées pour le module et alerte lorsque l'utilisation dépasse les pourcentages configurés pour le module. Ce module alerte également lorsque le système supprime un nombre excessif de fichiers dans les catégories d'utilisation du disque surveillées ou lorsque l'utilisation du disque à l'exclusion de ces catégories atteint des niveaux excessifs, en fonction des seuils du module.

Cette rubrique décrit les symptômes et les directives de dépannage pour deux alertes d'intégrité générées par le module d'intégrité de l'utilisation du disque :

- Déversement fréquent des événements
- Déversement d'événements non traités

Le processus de gestionnaire de disques gère l'utilisation du disque d'un périphérique. Chaque type de fichier surveillé par le gestionnaire de disques est doté d'un silo. En fonction de la quantité d'espace disque disponible sur le système, le gestionnaire de disques calcule un seuil élevé (HWM) et un seuil inférieur (LWM) pour chaque silo.

Pour afficher des informations détaillées sur l'utilisation du disque pour chaque partie du système, y compris les silos, les LWM et les HWM, utilisez la commande **show disk-manager**.

Exemples

Voici un exemple des informations du gestionnaire de disques :

```
> show disk-manager
Silo                                Used        Minimum     Maximum
Temporary Files                     0 KB        499.197 MB  1.950 GB
Action Queue Results                0 KB        499.197 MB  1.950 GB
User Identity Events                0 KB        499.197 MB  1.950 GB
UI Caches                           4 KB        1.462 GB    2.925 GB
Backups                             0 KB        3.900 GB    9.750 GB
Updates                             0 KB        5.850 GB    14.625 GB
Other Detection Engine              0 KB        2.925 GB    5.850 GB
Performance Statistics              33 KB       998.395 MB  11.700 GB
Other Events                        0 KB        1.950 GB    3.900 GB
IP Reputation & URL Filtering       0 KB        2.437 GB    4.875 GB
Archives & Cores & File Logs        0 KB        3.900 GB    19.500 GB
Unified Low Priority Events         1.329 MB    4.875 GB    24.375 GB
RNA Events                          0 KB        3.900 GB    15.600 GB
File Capture                        0 KB        9.750 GB    19.500 GB
Unified High Priority Events        0 KB        14.625 GB   34.125 GB
IPS Events                          0 KB        11.700 GB   29.250 GB
```

Format de l'alerte d'intégrité

Lorsque le processus de surveillance de l'intégrité de centre de gestion s'exécute (une fois toutes les 5 minutes ou lorsqu'une exécution manuelle est déclenchée), le module d'utilisation du disque examine le fichier diskmanager.log et, si les conditions appropriées sont réunies, une alerte d'intégrité est déclenchée.

Les structures de ces alertes d'intégrité sont les suivantes :

- Déversement fréquent de*[NOM DU SILO]*
- Déversement d'événements non traités de <*NOM DU SILO*>

Par exemple :

- Déversement fréquent des événements de priorité faible
- Déversement des événements non traités des événements de priorité faible.

Il est possible pour n'importe quel silo de générer une alerte d'intégrité *déversement fréquent de <NOM DU SILO>*.. Cependant, les plus fréquentes sont les alertes liées aux événements. Parmi les silos d'événements, les *événements de priorité faible* sont souvent observés, car le périphérique génère fréquemment ce type d'événements.

Un *déversement fréquent d'événement de <NOM DU SILO>* possède un niveau de gravité **Avertissement** en rapport avec un silo lié aux événements, car les événements seront mis en file d'attente pour être envoyés à centre de gestion. Pour un silo non lié à un événement, tel que le silo des *sauvegardes*, l'alerte a un niveau de gravité **Critique**, car cette information est perdue.

Important Seuls les silos d'événements génèrent un *déversement des événements d'alerte d'intégrité non traités à partir de <NOM DU SILO>*. Cette alerte a toujours un niveau de gravité **Critique**.

Outre les alertes, d'autres symptômes peuvent apparaître :

- Lenteur de l'interface utilisateur centre de gestion
- Perte d'événements

Scénarios de dépannage courants

L'événement *Déversement fréquent du <NOM DU SILO>* est dû à une trop grande quantité d'entrées dans le silo par rapport à sa taille. Dans ce cas, le gestionnaire de disques vide (purge) ce fichier au moins deux fois au cours des 5 dernières minutes. Dans un silo de type événement, cela est généralement causé par une journalisation excessive de ce type d'événement.

Une alerte d'intégrité *Déversement des événements non traités de <NOM DU SILO>* est due à un goulot d'étranglement dans le circuit de traitement des événements.

Il existe trois goulots d'étranglement potentiels en ce qui concerne ces alertes d'utilisation du disque :

- Journalisation excessive : le processus de gestionnaire d'événements sur défense contre les menaces est sursouscrit (il lit plus lentement que ce que Snort écrit).
- Goulot d'étranglement Sftunnel : l'interface Eventing est instable ou sursouscrite.
- Goulot d'étranglement SFDataCorrelator : le canal de transmission de données entre le centre de gestion et le périphérique géré est sursouscrit.

Journalisation excessive

L'une des causes les plus courantes des alertes d'intégrité de ce type est une entrée excessive. La différence entre la borne inférieure (LWM) et la borne supérieure (HWM) obtenue à partir de la commande **show disk-manager** montre l'espace disponible dans ce silo pour passer de LWM (fraîchement vidé) à la valeur HWM. Si le déversement d'événements est fréquent (avec ou sans événements non traités), passez en revue la configuration de la journalisation.

- Vérifier la double journalisation : les scénarios de double journalisation peuvent être identifiés si vous examinez les *perfstats* du corrélateur sur centre de gestion :

  ```
  admin@FMC:~$ sudo perfstats -Cq < /var/sf/rna/correlator-stats/now
  ```

- Vérification des paramètres de journalisation de la politique de contrôle d'accès : passez en revue les paramètres de journalisation de la politique de contrôle d'accès (Access Control Policy ou Access Control Policy). Si le paramètre de journalisation comprend à la fois le « début » et la « fin » de la connexion, modifiez le paramètre pour journaliser uniquement la fin afin de réduire le nombre d'événements.

Goulot d'étranglement des communications : Sftunnel

Sftunnel est responsable des communications chiffrées entre le centre de gestion et le périphérique géré. Les événements sont envoyés par le tunnel vers centre de gestion. Les problèmes de connectivité ou l'instabilité du canal de communication (sftunnel) entre le périphérique géré et le centre de gestion peuvent être dus aux éléments suivants :

- Sftunnel est en panne ou instable (clapets).

  Vérifiez que centre de gestion et le périphérique géré sont accessibles entre leurs interfaces de gestion sur le port TCP 8305.

  Le processus sftunnel doit être stable et ne doit pas redémarrer de manière inattendue. Vérifiez-le en consultant le fichier **/var/log/message** et recherchez les messages qui contiennent la chaîne ***sftunneld***.

- Sftunnel est sursouscrit.

  Examinez les données de tendances du moniteur d'intégrité et recherchez des signes de surabonnement de l'interface de gestion de centre de gestion. Il peut s'agir d'un pic du trafic de gestion ou d'un surabonnement constant.

  Utiliser comme interface de gestion secondaire pour la création d'événements. Pour utiliser cette interface, vous devez configurer son adresse IP et d'autres paramètres de l'interface de ligne de commande défense contre les menaces à l'aide de la commande**configure network management-interface**.

Goulot d'étranglement des communications : SFDataCorrelator

Le SFDataCorrelator gère la transmission de données entre le centre de gestion et le périphérique géré; sur centre de gestion, il analyse les fichiers binaires créés par le système pour générer des événements, des données de connexion et des cartographies du réseau. La première étape consiste à consulter le fichier **diskmanager.log** pour recueillir des informations importantes, telles que :

- La fréquence du déversement.
- Le nombre de fichiers avec des événements non traités vidés.
- L'occurrence du déversement avec des événements non traités.

Chaque fois que le processus du gestionnaire de disque s'exécute, il génère une entrée pour chacun des différents silos de son propre fichier journal, qui se trouve sous **[/ngfw]/var/log/diskmanager.log**. Les renseignements recueillis dans le fichier diskmanager.log (en format CSV) peuvent être utilisés pour aider à affiner la recherche d'une cause.

Étapes de dépannage supplémentaires :

- La commande **stats_unified.pl** peut vous aider à déterminer si le périphérique géré contient des données qui doivent être envoyées à centre de gestion. Cette situation peut se produire lorsque le périphérique géré et centre de gestion rencontrent un problème de connectivité. Le périphérique géré stocke les données du journal sur un disque dur.

  ```
  admin@FMC:~$ sudo stats_unified.pl
  ```

- La commande **manage_proc.pl** peut reconfigurer le corrélateur sur le côté centre de gestion.

  ```
  root@FMC:~# manage_procs.pl
  ```

Avant de communiquer avec le centre d'assistance technique de Cisco (TAC)

Il est fortement recommandé de récupérer ces éléments avant de communiquer avec Cisco TAC :

- Captures d'écran de l'alerte d'intégrité consultées.
- Fichier de dépannage généré par le centre de gestion.
- Fichier de dépannage généré à partir du périphérique géré concerné.

  Date et heure auxquelles le problème a été observé pour la première fois.

- Des renseignements sur toutes les modifications récentes apportées aux politiques (le cas échéant).

  La sortie de la commande stats_unified.pl décrite dans Goulot d'étranglement des communications : SFDataCorrelator, à la page 13.

Rapports de surveillance de l'intégrité pour le dépannage

Dans certains cas, si vous rencontrez un problème avec votre appareil, le service d'assistance peut vous demander de fournir des fichiers de dépannage pour les aider à diagnostiquer le problème. Le système peut produire des fichiers de dépannage contenant des informations ciblées sur des domaines fonctionnels spécifiques, ainsi que des fichiers de dépannage avancé que vous récupérez en collaboration avec le service d'assistance. Vous pouvez sélectionner l'une des options répertoriées dans le tableau ci-dessous pour personnaliser le contenu d'un fichier de dépannage pour une fonction spécifique.

Notez que certaines options se chevauchent en ce qui concerne les données qu'elles déclarent, mais les fichiers de dépannage ne contiendront pas de copies redondantes, quelles que soient les options que vous sélectionnez.

Tableau 2 : Options de dépannage sélectionnables

Cette option...	Crée des rapports comportant...
Configuration et performance de Snort	les données et les paramètres de configuration liés à Snort sur l'appareil
Journaux et performance du matériel	les données et les journaux liés aux performances du matériel de l'appareil
Configuration du système, politique et journaux	les paramètres de configuration, données et journaux liés à la configuration système actuelle de l'appareil
Configuration de la détection, politique et journaux	les paramètres, données et journaux de configuration liés à la détection sur l'appareil
Données relatives au réseau et à l'interface	les paramètres de configuration, données et journaux liés aux ensembles en ligne et à la configuration réseau de l'appareil
Découverte, sensibilisation, données VDB et journaux	les paramètres, les données et les journaux de configuration liés à la configuration de découverte et de détection actuelle sur l'appareil
Mettre à jour les données et les journaux	les données et les journaux liés aux mises à niveau antérieures de l'appareil
Toutes les données de la base de données	toutes les données relatives à la base de données incluses dans un rapport de dépannage
Toutes les données du journal	tous les journaux collectés par la base de données de l'appareil
Renseignement de la carte de réseau	les données de topologie actuelle du réseau

Production de fichiers de dépannage liés à des fonctions système spécifiques

Vous pouvez générer et télécharger des fichiers de dépannage personnalisés que vous pouvez envoyer au service d'assistance.

Dans un déploiement multidomaine, vous pouvez générer et télécharger des fichiers de dépannage pour les périphériques des domaines descendants.

Avant de commencer

Vous devez être un utilisateur administrateur, de maintenance, analyste de sécurité ou analyste de sécurité (lecture seule) pour effectuer cette tâche.

Procédure

Étape 1 Choisissez **System** (⚙) **> Health** > **Monitor** (Moniteur d'intégrité), cliquez sur le périphérique dans le panneau de gauche, puis cliquez sur **View System & Troubleshoot Details (Afficher les détails du système et du dépannage)**, puis cliquez sur **Generate Troubleshooting Files (Générer les fichiers de dépannage)**.

Remarque
- Lorsque vous générez des fichiers de dépannage centre de gestion à partir de l'interface Web Centre de gestion, le fichier est stocké dans le répertoire centre de gestion. Notez que seul le dernier fichier de dépannage sera stocké dans centre de gestion.
- Lorsque vous générez des fichiers de dépannage défense contre les menaces à partir de l'interface Web Centre de gestion, le fichier est généré dans défense contre les menaces et copié dans le répertoire centre de gestion. Notez que seul le dernier fichier de dépannage défense contre les menaces sera stocké dans centre de gestion.
- Lorsque les fichiers de dépannage pour centre de gestion et défense contre les menaces sont générés à partir de la CLI, toutes les versions des fichiers de dépannage sont conservées dans centre de gestion et défense contre les menaces respectivement.

Étape 2 Choisissez All Data (Toutes les données) pour générer toutes les données de dépannage possibles, ou cochez les cases individuelles, comme décrit dans Affichage des messages en lien avec les tâches, à la page 8.

Étape 3 Cliquez sur **Generate** (Générer).

Étape 4 Afficher les messages de tâches dans le centre de messagerie; voir Affichage des messages en lien avec les tâches, à la page 8.

Étape 5 Trouvez la tâche qui correspond aux fichiers de dépannage que vous avez générés.

Étape 6 Une fois que le périphérique a généré les fichiers de dépannage et que l'état de la tâche est passé à `Terminé`, cliquez sur **Click to retrieve generated files** (Cliquez pour récupérer les fichiers générés).

Étape 7 Suivez les instructions de votre navigateur pour télécharger le fichier. (Les fichiers de dépannage sont téléchargés dans un seul fichier `.tar.gz`.)

Étape 8 Suivez les instructions de l'assistance pour envoyer les fichiers de dépannage à Cisco.

Téléchargement des fichiers de dépannage avancé

Dans un déploiement multidomaine, vous pouvez générer et télécharger des fichiers de dépannage pour les périphériques des domaines descendants. Vous pouvez télécharger des fichiers à partir de centre de gestion uniquement à partir du domaine global.

Avant de commencer

Vous devez être un utilisateur administrateur, de maintenance, analyste de sécurité ou analyste de sécurité (lecture seule) pour effectuer cette tâche.

Procédure

Étape 1 Afficher le moniteur d'intégrité du périphérique .

Étape 2 Choisissez **System** (⚙) **> Moniteur** > **d'intégrité**, cliquez sur le périphérique dans le panneau de gauche, puis cliquez sur **Afficher les détails du système et du dépannage**, puis cliquez sur **Dépannage avancé.**

Étape 3 Dans le menu **Téléchargement de fichier**, saisissez le nom du fichier fourni par le service d'assistance.

Étape 4 Cliquez sur **Télécharger**.

Étape 5 Suivez les instructions de votre navigateur pour télécharger le fichier.

Remarque Pour les périphériques gérés, le système renomme le fichier en faisant précéder le nom du périphérique du nom du fichier.

Étape 6 Suivez les instructions de l'assistance pour envoyer les fichiers de dépannage à Cisco.

Généralités sur la résolution des problèmes

Une panne de courant interne (défaillance matérielle, surtension, etc.) ou une panne de courant externe (cordon débranché) peut entraîner un arrêt ou un redémarrage malfaisant du système. Cela pourrait corrompre les données.

Dépannage basé sur la connexion

Le dépannage ou le débogage basé sur la connexion fournit un débogage uniforme dans tous les modules afin de recueillir les journaux appropriés pour une connexion spécifique. Il prend également en charge le débogage basé sur les niveaux jusqu'à sept niveaux et permet un mécanisme uniforme de collecte de journaux pour tous les modules. Le débogage basé sur la connexion prend en charge les éléments suivants :

- Sous-système courant de débogage basé sur la connexion pour résoudre les problèmes dans défense contre les menaces S
- Format uniforme pour les messages de débogage dans tous les modules
- Messages de débogage persistants pendant les redémarrages
- Débogage de bout en bout sur les modules en fonction d'une connexion existante
- Débogage des connexions en cours

Remarque Le débogage basé sur la connexion n'est pas pris en charge sur les périphériques de la série Firepower 2100.

Pour en savoir plus sur le dépannage des connexions, consultez Dépanner une connexion , à la page 17.

Dépanner une connexion

Procédure

Étape 1 Configurez un filtre pour identifier une connexion à l'aide de la commande de **debug packet-condition**.

Exemple :

```
Debug packet-condition match tcp 192.168.100.177 255.255.255.255 192.168.102.177
255.255.255.255
```

Étape 2 Activez le débogage des modules concernés et des niveaux correspondants. Saisissez la commande **debug packet**.

Exemple :

```
Debug packet acl 5
```

Étape 3 Commencez à déboguer les paquets à l'aide de la commande suivante :

```
debug packet-start
```

Étape 4 Récupérez les messages de débogage de la base de données pour les analyser à l'aide de la commande suivante :

```
show packet-debugs
```

Étape 5 Arrêtez le débogage des paquets à l'aide de la commande suivante :

```
debug packet-stop
```

Dépannage avancé pour le périphérique Cisco Secure Firewall Threat Defense

Vous pouvez utiliser les fonctionnalités de Packet Tracer et de Packet Capture pour effectuer une analyse de dépannage approfondie sur un périphérique Cisco Secure Firewall Threat Defense. Packet-Tracer permet à un administrateur de pare-feu d'injecter un paquet virtuel dans le périphérique de sécurité et de suivre le flux de l'entrée à la sortie. En cours de route, le paquet est évalué en fonction des recherches de flux et de routage, des listes de contrôle d'accès, de l'inspection de protocole, de la NAT et de la détection de prévention des intrusions. La puissance de cet utilitaire réside dans sa capacité à simuler le trafic du monde réel en spécifiant les adresses de source et de destination avec des informations sur le protocole et le port. La capture de paquet est disponible avec l'option de trace, qui vous fournit un verdict pour savoir si le paquet est abandonné ou réussi.

Pour en savoir plus sur les fichiers de dépannage, consultez Téléchargement des fichiers de dépannage avancé, à la page 15.

Présentation de la capture de paquets

La fonction de capture de paquets avec l'option de traçage permet de tracer les paquets réels enregistrés sur l'interface d'entrée à travers le système. Les informations de trace sont affichées ultérieurement. Ces paquets

ne sont pas abandonnés à l'interface de sortie, car il s'agit d'un vrai trafic de données. La capture de paquets pour les périphériques défense contre les menaces prend en charge le dépannage et l'analyse des paquets de données.

Une fois le paquet acquis, Snort détecte l'indicateur de traçage activé dans le paquet. Snort écrit des éléments de traçage, à travers lesquels le paquet passe. Le verdict de Snort à la suite de la capture de paquets peut être l'un des éléments suivants :

Tableau 3 : Verdicts Snort

Verdict	Description
Réussite	Autoriser le paquet analysé.
Bloquer	Paquet non transféré
Remplacement	Paquet modifié.
AllowFlow	Le flux est passé sans inspection.
BlockFlow	Le flux a été bloqué.
Ignorer	Le flux a été bloqué; se produit uniquement pour les sessions dont les flux sont bloqués sur les interfaces passives.
Nouvelle tentative	Le flux est bloqué en attente d'une requête de catégorie ou de réputation de logiciel malveillant masqué ou de catégorie d'URL. Si le délai est dépassé, le traitement se poursuit avec un résultat inconnu : dans le cas d'un logiciel malveillant masqué, le fichier est autorisé; dans le cas de la catégorie ou de la réputation d'URL, la recherche de la règle de CA se poursuit avec une réputation inconnue et non classée.

En fonction du verdict Snort, les paquets sont abandonnés ou autorisés. Par exemple, le paquet est abandonné si le verdict Snort est (Liste noire) **BlockFlow** (Blocage) et les paquets suivants de la session sont abandonnés avant d'atteindre Snort. Lorsque le verdict Snort est **Block** (Bloquer) ou **BlockFlow**Liste noire > Blocage de flux) , le motif d'abandon **Drop Reason** peut être :

Tableau 4 : Motifs d'abandon

Bloqué ou Flux bloqué par...	Cause
Snort	Snort est incapable de traiter le paquet, par exemple, snort ne peut pas décoder le paquet parce qu'il est endommagé ou a un format non valide.
ID d'application prétraité	Le module d'ID d'application/prétraité ne bloque pas les paquets lui-même; mais cela peut indiquer que la détection d'ID d'application fait en sorte qu'un autre module (pare-feu) correspond à une règle de blocage.

Bloqué ou Flux bloqué par...	Cause
le SSL prétraité	La politique SSL comporte une règle de blocage ou de réinitialisation qui correspond au trafic.
le pare-feu	Il existe une règle de blocage/réinitialisation dans la politique de pare-feu qui correspond au trafic.
le portail captif a été prétraité	Il existe une règle de blocage/réinitialisation qui utilise la politique d'identité pour mettre en correspondance le trafic.
la recherche sécurisée prétraitée	Il existe une règle de blocage ou de réinitialisation qui utilise la fonction de recherche sécurisée dans la politique de pare-feu pour correspondre au trafic.
le SI prétraité	Il existe une règle de blocage/réinitialisation a dans l'onglet Security Intelligence de la politique de contrôle d'accès qui permet de bloquer le trafic, l'activation, le DNS ou l'URL SI.
le filtre a prétraité	Il existe une règle de blocage/réinitialisation dans l'onglet du filtre de la politique de contrôle d'accès pour correspondre au trafic.
le flux prétraité	Il y a un blocage de règle de prévention des intrusions/réinitialisation de connexion de flux, par exemple, un blocage en cas d'erreur de normalisation TCP.
la session a été prétraitée	Cette session a déjà été bloquée précédemment par un autre module, donc la session prétraitée bloque d'autres paquets de la même session.
la fragmentation prétraitée	Blocage, car le fragment précédent des données est bloqué.
la réponse Snort prétraitée	Il existe une règle de réaction Snort, par exemple, qui envoie une page de réponse sur un trafic HTTP particulier.
la réponse Snort prétraitée	Il existe une règle snort qui permet d'envoyer une réponse personnalisée aux paquets correspondant aux conditions.
la réputation prétraitée	Le paquet correspond à une règle de réputation, c'est-à-dire le blocage d'une adresse IP donnée.
x-Link2State prétraité	Blocage en raison d'une vulnérabilité de débordement de la mémoire tampon détectée dans SMTP.
Orifice arrière prétraité	Blocage en raison de la détection de données de l'orifice arrière.

Bloqué ou Flux bloqué par...	Cause
le SMB prétraité	Il existe une règle snort pour bloquer le trafic SMB.
le processus de fichier prétraité	Il existe une politique de fichiers qui bloque un fichier, notamment les programmes malveillants masqués.
l'IPS prétraité	Il y a une règle snort qui utilise IPS, erg, le filtrage de débit.

La fonction de capture de paquets vous permet de capturer et de télécharger des paquets stockés dans la mémoire système. Cependant, la taille de la mémoire tampon est limitée à 32 Mo en raison de contraintes de mémoire. Les systèmes capables de gérer un très grand volume de captures de paquets dépassent rapidement la taille de la mémoire tampon maximale, et il est donc nécessaire d'augmenter la limite de capture de paquets. Pour ce faire, utilisez la mémoire secondaire (en créant un fichier pour écrire les données de capture). La taille de fichier maximale prise en charge est de 10 Go.

Lorsque la **taille du fichier** est configurée, les données capturées sont stockées dans le fichier et le nom de fichier est attribué en fonction du nom de la capture **recapture**.

L'option **taille du fichier** est utilisée lorsque vous devez capturer des paquets dont la taille limite est supérieure à 32 Mo.

Pour en savoir plus, consultez Référence des commandes de défense contre les menaces de Cisco Secure Firewall.

Utiliser la trace de capture

La capture de paquets est un utilitaire qui fournit un instantané en direct du trafic réseau passant par l'interface spécifiée d'un périphérique en fonction de critères définis. Ce processus continue de capturer les paquets tant qu'il n'est pas en pause ou que la mémoire allouée n'est pas épuisée.

Les données de capture de paquets comprennent des informations Snort et des préprocesseurs sur les verdicts et les actions que le système entreprend lors du traitement d'un paquet. La capture de plusieurs paquets est possible à la fois. Vous pouvez configurer le système pour modifier, supprimer, effacer et enregistrer les captures.

Remarque La capture de paquets de données nécessite une copie de paquets. Cette opération peut entraîner des retards dans le traitement des paquets et peut également dégrader le débit de paquets. Nous vous recommandons d'utiliser des filtres de paquets pour capturer des données de trafic spécifiques.

Avant de commencer

Pour utiliser l'outil de capture de paquets sur des périphériques Cisco Secure Firewall Threat Defense, vous devez être un utilisateur administrateur ou de maintenance.

Procédure

Étape 1 Dans centre de gestion, choisissez **Périphériques** > **Capture de paquets**.

Étape 2 Sélectionnez un appareil.

Étape 3 Cliquez sur **Add Capture** (ajouter une capture).

Étape 4 Saisissez le **nom** pour la capture de la trace.

Étape 5 Sélectionnez l' **interface** pour la capture de la trace.

Étape 6 Préciser les détails **des critères de correspondance** :

a) Sélectionnez le **protocole**.
b) Saisissez l'adresse IP pour l'**hôte source**.
c) Saisissez l'adresse IP de l'**hôte de destination**.
d) (Facultatif) Cochez la case **Numéro SGT** et saisissez une balise de groupe de sécurité (SGT).

Étape 7 Précisez les détails de la **mémoire tampon** :

a) (Facultatif) Saisissez une **taille de paquet** maximale.
b) (Facultatif) Saisissez une **taille minimale de mémoire tampon**.
c) Sélectionnez **Capture continue** si vous souhaitez que le trafic soit capturé sans interruption, ou **Arrêter lorsqu'il est plein** si vous souhaitez que la capture s'arrête lorsque la taille maximale de la mémoire tampon est atteinte.

Remarque Si l'option **Continues Capture** (continue la capture) est activée et que la mémoire allouée est pleine, les paquets capturés les plus anciens dans la mémoire sont remplacés par les nouveaux paquets capturés.

d) Cochez la case **Trace**(trace) si vous souhaitez saisir les détails pour chaque paquet.
e) Saisissez la valeur dans le champ **Trace Count** (Nombre de traces). La valeur par défaut est 128. Vous pouvez saisir des valeurs comprises entre 1 et 1 000.

Étape 8 Cliquez sur **Save** (enregistrer).

L'écran de capture de paquets affiche les détails de la capture de paquets et son état. Pour que la page de capture de paquets soit actualisée automatiquement, cochez la case **Enable Auto Refresh** (activer l'actualisation automatique) et saisissez l'intervalle d'actualisation automatique en secondes.

Vous pouvez effectuer ce qui suit sur la capture de paquets :

- **Edit** ( ) pour modifier les critères de capture.
- **Supprimer** ( ) pour supprimer la capture de paquets et les paquets capturés.
- **Effacer** ( ) pour effacer tous les paquets capturés d'une capture de paquets. Pour effacer les paquets capturés de toutes les captures de paquets existantes, cliquez sur **Clear All Packets** (Effacer tous les paquets).
- **Pause** ( ) pour interrompre temporairement la capture de paquets.
- **Enregistrer** ( ) pour enregistrer une copie des paquets capturés sur un ordinateur local au format ASCII ou PCAP. Choisissez l'option de formatage requise, puis cliquez sur **Save**(Enregistrer). La capture de paquets enregistrée est téléchargée sur votre ordinateur local.
- Pour afficher les détails des paquets capturés, cliquez sur la ligne de capture requise.

Présentation de l'outil de trace de paquets

La fonction Packet Tracer (Traceur de paquets) vous permet de tester la configuration de politique en modélisant un paquet avec des adresses de source et de destination, et des caractéristiques de protocole. La trace effectue une recherche de politique pour vérifier si le paquet est autorisé ou refusé en fonction des règles d'accès configurées, de la NAT, du routage, des politiques d'accès et de limitation de débit. Le flux de paquets est simulé en fonction des interfaces, de l'adresse de source, de l'adresse de destination, des ports et des protocoles. Cette méthode de test des paquets vous permet de vérifier l'efficacité de vos politiques et de tester si les types de trafic que vous souhaitez autoriser ou refuser sont gérés comme vous le souhaitez. En plus de vérifier votre configuration, vous pouvez utiliser le traceur pour déboguer un comportement inattendu, tel que le refus de paquets alors qu'ils devraient être autorisés. Pour simuler entièrement le paquet, Packet Tracer (Traceur de paquets) trace le chemin de données; modules de chemin lent et de chemin rapide. Initialement, le traitement était effectué par session et par paquet. Packet Tracer (Traceur de paquets) et les fonctionnalités de capture avec trace enregistrent les données de traçage par paquet lorsque le pare-feu traite les paquets par session ou par paquet.

Fichier PCAP

Vous pouvez lancer un traceur de paquets à l'aide d'un fichier PCAP qui a un flux complet. Actuellement, le protocole PCAP avec un seul flux TCP/UDP, avec un maximum de 100 paquets, est pris en charge. L'outil Packet Tracer (Traceur de paquets) lit le fichier PCAP, initialise l'état pour les entités de relecture client et serveur. L'outil commence à lire les paquets de manière synchronisée en collectant et en stockant la sortie de trace de chaque paquet dans PCAP pour un traitement et un affichage ultérieurs.

Relecture PCAP

La relecture de paquet est exécutée par la séquence du paquet dans le fichier PCAP et toute interférence avec l'activité de relecture l'interrompt et met fin à la relecture. La sortie de la trace est générée pour tous les paquets dans PCAP sur une interface d'entrée et une interface de sortie spécifiées, fournissant ainsi un contexte complet d'évaluation de flux.

La relecture PCAP n'est pas prise en charge pour certaines fonctionnalités qui modifient dynamiquement le paquet pendant la relecture, comme IPsec, VPN, le déchiffrement SSL ou HTTPs, la NAT, etc.

Utiliser l'outil de trace de paquets Packet Tracer

Vous pouvez utiliser un Packet Tracer (Traceur de paquets) sur les périphériques Cisco Secure Firewall Threat Defense. Vous devez être un utilisateur administrateur ou utilisateur de maintenance pour utiliser cet outil.

Procédure

Étape 1 Dans centre de gestion, choisissez **Devices (appareils)** > **Packet Tracer (traceurs de paquets)**.

Étape 2 Dans la liste déroulante **Select Device** (sélectionner un périphérique), choisissez le périphérique sur lequel vous souhaitez exécuter la trace.

Étape 3 Dans la liste déroulante **Ingress Interface** (interface d'entrée), choisissez l'interface d'entrée pour la trace de paquets.

Remarque Ne sélectionnez pas VTI. Le VTI comme interface d'entrée n'est pas pris en charge par Packet Tracer.

Étape 4 Pour utiliser une relecture PCAP dans Packet Tracer, procédez comme suit :

a) Cliquez sur **Select a PCAP File** (Sélectionner un fichier PCAP).

b) Pour téléverser un nouveau fichier PCAP, cliquez sur **Upload a PCAP file**. Pour réutiliser un fichier récemment téléversé, cliquez sur le fichier dans la liste.

Remarque Seuls les formats de fichier pcap et pcapng sont pris en charge. Le fichier PCAP ne peut contenir qu'un seul flux TCP/UDP avec un maximum de 100 paquets. La limite maximale de caractères dans le nom de fichier PCAP (y compris les formats de fichier) est de 64.

c) Dans la zone **Upload PCAP** (téléverser PCAP), vous pouvez soit faire glisser un fichier PCAP, soit cliquer dans la zone pour parcourir es répertoires et téléverser le fichier. Lors de la sélection du fichier, le processus de téléversement démarre automatiquement.

d) Passez à cette Étape 13.

Étape 5 Pour définir les paramètres de trace, dans le menu déroulant **Protocol** (protocole), sélectionnez le type de paquet pour la trace et précisez les caractéristiques du protocole :

- **ICMP** : saisissez le type ICMP, le code ICMP (0 à 255) et éventuellement l'identifiant ICMP.
- **TCP/UDP/SCTP** : saisissez les numéros de port source et de destination.
- **GRE/IPIP** : saisissez le numéro de protocole, 0 à 255.
- **ESP** : saisissez la valeur SPI pour la source, 0 à 4294967295.
- **RAWIP** : saisissez le numéro de port, 0 à 255.

Étape 6 Sélectionnez le **type de source** pour la trace de paquets et saisissez l'adresse IP source.

Les types de source et de destination comprennent IPv4, IPv6 et les noms de domaine complets (FQDN). Vous pouvez spécifier des adresses IPv4 ou IPv6 et un nom de domaine complet (FQDN) si vous utilisez Cisco TrustSec.

Étape 7 Sélectionnez le **port source** pour la trace des paquets.

Étape 8 Sélectionnez le type de **destination** pour la trace de paquets et saisissez l'adresse IP de destination.

Les options de type de destination varient selon le type de source que vous sélectionnez.

Étape 9 Sélectionnez le **port de destination** pour la trace des paquets.

Étape 10 Si vous souhaitez suivre un paquet dont la valeur de balise de groupe de sécurité (SGT) est intégrée dans l'en-tête CMD de couche 2 (TrustSec), saisissez un **numéro SGT** valide.

Étape 11 Si vous souhaitez que Packet Tracer entre dans une interface parente, qui est ensuite redirigée vers une sous-interface, saisissez un **ID de VLAN**.

Cette valeur est facultative uniquement pour les interfaces non subordonnées, puisque tous les types d'interface peuvent être configurés sur une sous-interface.

Étape 12 Précisez une **adresse MAC de destination** pour la trace de paquets.

Si le périphérique Cisco Secure Firewall Threat Defense fonctionne en mode de pare-feu transparent et que l'interface d'entrée est VTEP, **Destination MAC Address** (adresse MAC de destination) est requise si vous saisissez une valeur dans **VLAN ID**. Alors que, si l'interface est membre d'un groupe de ponts, **l'adresse MAC de destination** est facultative si vous saisissez une valeur **d'ID VLAN**, mais obligatoire si vous n'saisissez pas de valeur **d'ID VLAN**.

Si Cisco Secure Firewall Threat Defense est exécuté en mode de pare-feu routé, **l'ID de VLAN** et **l'adresse MAC de destination** sont facultatifs si l'interface d'entrée est membre d'un groupe de ponts.

Étape 13 (Facultatif) Si vous souhaitez que Packet-Tracer ignore les contrôles de sécurité sur le paquet simulé, cliquez sur **Bypass all security checks for simulated packet** (Contourner tous les contrôles de sécurité pour les paquets simulés). Cela permet au traceur de paquets de continuer à tracer les paquets dans le système qui, autrement, auraient été abandonnés.

Étape 14 (Facultatif) Pour autoriser l'envoi du paquet par l'interface de sortie à partir du périphérique, cliquez sur **Allow simulated packet to transmit from device** (autoriser la transmission du paquet simulé à partir du périphérique).

Étape 15 (Facultatif) Si vous souhaitez que le traceur de paquets considère le paquet injecté comme un paquet décrypté IPsec/SSL VPN, cliquez sur **Treat simulated packet as IPsec/SSL VPN decrypt** (Traiter le paquet simulé comme un déchiffrement IPsec/SSL VPN).

Étape 16 Cliquez sur **Trace** (Suivi).

Le résultat de la **trace** affiche les résultats pour chaque phase que les paquets PCAP ont passée dans le système. Cliquez sur le paquet individuel pour afficher les résultats des suivis pour le paquet. Vous pouvez effectuer les opérations suivantes :

- Copiez ( ) les résultats de la trace dans le presse-papier.
- Développez ou réduisez ( ) les résultats affichés.
- Maximisez ( ) l'écran de résultats du traçage.

Les renseignements sur le temps écoulé qui sont utiles pour évaluer les efforts de traitement sont affichés pour chaque phase. Le temps total nécessaire pour que l'ensemble du flux de paquets passe d'une interface d'entrée à une interface de sortie est également affiché dans la section des résultats.

Le volet **Historique du suivi** affiche les détails de suivi enregistrés pour chaque suivi PCAP. Il peut stocker jusqu'à 100 suivis de paquets. Vous pouvez sélectionner un suivi enregistré et exécuter à nouveau l'activité de suivi de paquets. Vous pouvez effectuer les opérations suivantes :

- Recherchez un suivi à l'aide de l'un des paramètres de trace.
- Désactivez l'enregistrement du suivi dans l'historique en utilisant le bouton .
- Supprimez des résultats de suivi précis.
- Effacez tous les suivis.

Utilisation de l'interface de ligne de commande de dépistage Défense contre les menaces à partir de l'interface Web

Vous pouvez exécuter les commandes de l'interface de ligne de dépistage défense contre les menaces (CLI de dépistage) sélectionnées à partir de la commande centre de gestion. Ces commandes s'exécutent dans l'interface de ligne de commande de dépistage plutôt que dans la CLI normale. Ces commandes sont les commandes **ping** (sauf **ping system**), **traceroute** et sélectionnez **show**.

Pour les commandes **show**, si vous obtenez le message « Impossible d'exécuter la commande correctement. Consultez les journaux pour plus de détails », cela signifie que la commande n'est pas valide dans l'interface de ligne de commande de dépistage. Par exemple, **show access-list** fonctionne, mais vous obtiendrez ce message si vous saisissez **show access-control-policy**. Si vous devez utiliser des commandes CLI hors dépistage, vous devez vous connecter en SSH sur le périphérique à l'extérieur du centre de gestion.

Pour en savoir plus sur l'interface de ligne de commande défense contre les menaces , consultez le document Référence des commandes de défense contre les menaces de Cisco Secure Firewall.

Avant de commencer

- Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour utiliser l'interface de commande en ligne de dépistage.
- Le but de cette fonctionnalité est d'activer l'utilisation rapide de quelques commandes qui pourraient vous être utiles pour dépanner un périphérique. Pour tout travail sérieux d'interface de ligne de commande, y compris l'accès à l'ensemble des commandes, ouvrez une session SSH directement sur le périphérique.
- Dans un déploiement multidomaine, vous pouvez entrer des commandes CLI défense contre les menaces pour les périphériques gérés dans les domaines descendants.
- Dans les déploiements faisant appel à centre de gestion haute disponibilité , cette fonctionnalité est disponible uniquement dans centre de gestion actif.

Procédure

Étape 1 Choisissez **Périphériques** > **CLI Threat Defense** (Interface de ligne de commande pour Défense contre les menaces).

Vous pouvez également accéder à l'outil d'interface de ligne de commande par le biais du moniteur d'intégrité du périphérique (**System** (⚙) > **Moniteur** > **d'intégrité**). À partir de là, vous pouvez sélectionner le périphérique, cliquer sur le lien **Afficher les détails du système et du dépannage**, cliquer sur **Dépannage avancé**, puis sur **l'interface de ligne de commande de Threat Defense** sur cette page.

Étape 2 Dans la liste des **périphériques**, sélectionnez le périphérique sur lequel exécuter la commande de dépistage.

Étape 3 Dans la liste des **commandes**, sélectionnez la commande que vous souhaitez exécuter.

Étape 4 Saisissez les paramètres de la commande dans la zone de texte **Paramètres**.

Consultez la référence des commandes pour connaître les paramètres valides.

Par exemple, pour exécuter **show access-list**, vous devez sélectionner **show** dans la liste des **commandes**, puis saisir **access-list** dans la zone **Paramètres**.

Ne tapez pas la commande complète dans la zone des **paramètres**.

Étape 5 Cliquez sur **Exécuter** pour afficher le résultat de la commande.

Si vous obtenez le message « Impossible d'exécuter la commande correctement. Veuillez consulter les journaux pour plus de détails », examinez de près les paramètres. Il y a peut-être des erreurs de syntaxe.

Ce message peut également signifier que la commande que vous essayez d'exécuter n'est pas une commande valide dans le contexte de l'interface de commande en ligne de dépistage (que vous saisiriez à partir du périphérique en utilisant la commande **system support diagnostic-cli**). Connectez-vous au périphérique en utilisant SSH pour utiliser ces commandes.

Dépannage spécifique aux fonctionnalités

Consultez le tableau suivant pour obtenir des conseils et des techniques de dépannage propres à la fonction.

Tableau 5 : Sujets de dépannage propres aux fonctionnalités

Fonctionnalités	Renseignements de dépannage pertinents
Contrôle des applications	*Bonnes pratiques pour le contrôle des applications* dans Guide de configuration Cisco Secure Firewall Management Center Device
Authentification externe LDAP	Résolution de problèmes liés aux connexions d'authentification LDAP
Licence	Dépannage des licences Smart
Conditions des règles d'utilisateur	*Dépannage du contrôle utilisateur* dans Guide de configuration Cisco Secure Firewall Management Center Device
Source d'identité de l'utilisateur	Pour des renseignements de dépannage concernant ISE/ISE-PIC, la source d'identité de l'agent TS, la source d'identité du portail captif et la source d'identité de l'accès à distance VPN, consultez les sections correspondantes dans Guide de configuration Cisco Secure Firewall Management Center Device Résolution de problèmes liés aux connexions d'authentification LDAP
Filtrage d'URL	*Dépannage du filtrage d'URL* dans Guide de configuration Cisco Secure Firewall Management Center Device
Téléchargements des domaines et de données des utilisateurs	*Dépanner les domaines et les téléchargements d'utilisateur* dans Guide de configuration Cisco Secure Firewall Management Center Device
Détection du réseau	*Dépannage de votre politique de découverte de réseau* dans Guide de configuration Cisco Secure Firewall Management Center Device
Conditions des règles SGT (Balise de groupe de sécurité) personnalisées	*Conditions de règles SGT personnalisées* dans Guide de configuration Cisco Secure Firewall Management Center Device
Règles SSL	Chapitre sur les règles SSL dans Guide Cisco Secure Firewall Device Manager Configuration
Cisco Threat Intelligence Director (TID)	*Dépanner Directeur de Cisco Secure Firewall threat intelligence* le Guide de configuration Cisco Secure Firewall Management Center Device
Cisco Secure Firewall Threat Defense syslog	*À propos de la configuration de Syslog* dans Guide de configuration Cisco Secure Firewall Management Center Device
Statistiques de performance des intrusions	*Configuration de la journalisation des statistiques de performance de prévention des intrusions* dans Guide de configuration Cisco Secure Firewall Management Center Device
Dépannage basé sur la connexion	Dépannage basé sur la connexion, à la page 16

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.