Cisco Security Analytics and Logging

À propos de Security Analytics and Logging

Security Analytics and Logging (SAL) est un service centralisé de gestion des journaux et de détection des menaces avancées qui offre une journalisation évolutive des pare-feux Cisco et des analyses corrélées. La journalisation centralisée permet la visibilité, aide au dépannage des problèmes d'accès au réseau, y compris les perturbations, et permet la surveillance des périphériques et de l'état général du réseau. Les analyses permettent de détecter les menaces avancées.

Le service SAL est disponible selon les deux méthodes suivantes :

- Security Analytics and Logging (SaaS) : un logiciel-service (SaaS) hébergé qui stocke les événements et fournit des données pour l'analyse de la sécurité à l'aide de Secure Cloud Analytics (anciennement Stealthwatch Cloud). Ce service connecte le magasin de données en nuage Security Analytics and Logging au gestionnaire en nuage du pare-feu, Cisco Defense Orchestrator (CDO).

  Dans la présente documentation, cette méthode est également appelée SAL (SaaS).

- Security Analytics and Logging (On Premises) : service qui fonctionne sur les périphériques Cisco Secure Network Analytics (anciennement Stealthwatch) pour stocker les journaux des événements dans les locaux du client. Ce service connecte les données Security Analytics and Logging (On Premises) au gestionnaire sur site, Cisco Secure Firewall Management Center.

  Dans la présente documentation, cette méthode est également appelée SAL (local).

Pour en savoir plus sur Security Analytics and Logging, consultez le site https://www.cisco.com/c/en/us/products/security/security-analytics-logging/index.html.

Comparaison des options de stockage et de surveillance des événements à distance SAL

L'intégration deSAL affiche des options similaires pour le stockage de données d'événements en externe dans un centre de gestion et un CDO :

	SAL (local)	SAL (SaaS)
Pourquoi choisir cette solution?	Vous souhaitez augmenter la capacité de stockage des données d'événements de votre pare-feu sur site, conserver ces données plus longtemps et exporter vos données d'événements vers le périphérique Cisco Secure Network Analytics.	Vous souhaitez envoyer les événements de pare-feu pour stockage et éventuellement rendre vos données d'événements de pare-feu disponibles pour l'analyse de sécurité à l'aide de Secure Cloud Analytics.
Licence	Achetez une licence et configurez le système de stockage derrière votre pare-feu. Pour en savoir plus, consultez Licences pour SAL (local), à la page 3	Achetez une licence et un forfait de stockage de données et envoyez vos données au nuage de Cisco. Pour en savoir plus, consultez Licences pour SAL (SaaS), à la page 9
Types d'événements pris en charge	• Connexion • Fichiers et programmes malveillants • Intrusion • LINA • Renseignements de sécurité	• Connexion • Fichiers et programmes malveillants • Intrusion • Renseignements de sécurité
Méthodes prises en charge pour envoyer des événements	Prend en charge à la fois syslog et l'intégration directe.	Prend en charge à la fois syslog et l'intégration directe.
Affichage des événements	• Affichez les événements sur Cisco Secure Network Analytics Manager. • Lancement croisé à partir de la visionneuse d'événements centre de gestion pour afficher les événements sur Cisco Secure Network Analytics Manager. • Affichez les connexions stockées à distance et les événements de sécurité dans le centre de gestion.	Affichez les événements dans CDO ou Cisco Secure Network Analytics Manager, selon votre licence. Lancement croisé à partir de la visionneuse d'événements centre de gestion.

À propos de SAL (local)

Vous pouvez configurer SAL (local) pour stocker les données d'événements du pare-feu afin d'augmenter le stockage pendant une période de conservation plus longue. En déployant des périphériques Cisco Secure Network Analytics et en les intégrant à votre déploiement de pare-feu, vous pouvez exporter vos données d'événements vers un appareil Cisco Secure Network Analytics.

Cela vous offre les fonctionnalités suivantes :

- Enregistre les événements sur le périphérique Cisco Secure Network Analytics.
- Spécifiez cette source de données distante pour afficher ces événements dans le centre de gestion.
- Examinez les données d'événements de l'interface utilisateur de l'application Web de Cisco Secure Network Analytics Manager (anciennement la console de gestion Stealthwatch) à l'aide de la *visionneuse d'événements*.
- Le lancement croisé de l'interface utilisateur du centre de gestion vers la *visionneuse d'événements* pour afficher un contexte supplémentaire sur les informations à partir de laquelle vous avez effectué le lancement croisé.

Licences pour SAL (local)

Vous devez obtenir la licence Smart de journalisation et de dépannage pour utiliser SAL (local). Vous pouvez obtenir la licence en fonction de la quantité de données que vous prévoyez lors de l'envoi quotidien des données du journal système de votre déploiement de pare-feu à votre appareil Cisco Secure Network Analytics.

Pour en savoir plus sur l'octroi de licences pour les périphériques Cisco Secure Network Analytics, consultez le guide des licences de Cisco Secure Network Analytics Smart.

Pour en savoir plus sur les options de licence SAL (local) disponibles, consultez le Guide de commande de Cisco Security Analytics and Logging.

Remarque Pour le calcul des licences, la quantité de données est arrondie au Go entier le plus proche. Par exemple, si vous envoyez 4,9 Go par jour, 4 Go seront indiqués.

Gérer les périphériques contre les menaces SAL (local) pilotés par Défense contre les menaces géré par CDO

À partir de la version 7.2 Cisco Secure Firewall Threat Defense (anciennement Firepower Threat Defense), vous pouvez choisir d'envoyer les événements entièrement qualifiés générés par les périphériques défense contre les menaces gérés par CDO au centre de gestion. Le centre de gestion reçoit et affiche les analyses de données pour ces événements. Le centre de gestion qui reçoit et affiche les données d'événements est également désigné comme centre de gestion à usage unique pour l'analyse. .

Si vos périphériques sont activés pour envoyer des événements de connexion à un Cisco Secure Network Analytics Manager à l'aide de SAL (local), vous pouvez afficher et utiliser ces événements stockés à distance

dans la visionneuse d'événements et l'explorateur de contexte du centre de gestion, et les inclure lors de la génération de rapports. En déployant le périphérique Cisco Secure Network Analytics et en l'intégrant au déploiement de pare-feu, vous pouvez exporter les données de l'événement vers le périphérique Secure Network Analytics. Cela vous permet d'afficher et de gérer les événements dans l'interface utilisateur du centre de gestion. À partir de l'interface du centre de gestion, vous pouvez également effectuer un lancement croisé sur Cisco Secure Network Analytics Manager pour afficher et gérer les données des événements.

Le centre de gestion peut recevoir et afficher les analyses d'événements pour les périphériques gérés par CDO défense contre les menaces suivants :

- Périphériques défense contre les menaces nouveaux ou existants intégrés à CDO

  Pour en savoir plus sur l'intégration d'un périphérique défense contre les menaces à CDO, consultez Conditions préalables à l'intégration d'un périphérique à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

  Le flux de travail est le suivant :

  1. Intégrer un périphérique défense contre les menaces à CDO.

     Intégrer les périphériques défense contre les menaces à l'aide des méthodes d'intégration décrites dans Conditions préalables à l'intégration d'un périphérique à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). Le processus d'intégration comprend l'attribution des politiques et le choix des licences appropriées.

  2. Enregistrez ce périphérique défense contre les menaces dans le centre de gestion approprié.

     Pour que le centre de gestion affiche les événements générés par un périphérique défense contre les menaces géré par CDO, vous devez enregistrer le périphérique défense contre les menaces dans le centre de gestion. Pour enregistrer ce périphérique dans centre de gestion, permettez au périphérique d'être enregistré à l'aide du **configure manager add** {*nom d'hôte* | *adresse_IPv4* | *adresse_IPv6*}*reg_key*[*nat_id*]), puis ajoutez le périphérique à centre de gestion en cochant la case **appareil géré par CDO**.

     Remarque La clé d'enregistrement et l'ID NAT doivent être uniques parmi ceux utilisés lors de l'intégration du périphérique à CDO.

     Pour en savoir plus, consultez *Ajouter un périphérique au centre de gestion* et *Terminer la configuration initiale de Threat Defense à l'aide de la CLI* du Guide de configuration des périphériques du centre de gestion Cisco Firepower Management Center.

  3. Afficher les événements dans le centre de gestion ou le lancement croisé sur un Cisco Secure Network Analytics Manager.

     Pour afficher et utiliser les événements dans la visionneuse d'événements du centre de gestion. Si le périphérique Cisco Secure Network Analytics est déployé et intégré au déploiement du pare-feu, vous pouvez exporter les données d'événement vers le périphérique Cisco Secure Network Analytics. Cela vous permet d'effectuer un lancement croisé de l'interface utilisateur du centre de gestion vers Cisco Secure Network Analytics Manager pour afficher et gérer les données des événements.

     Pour en savoir plus, consultez les pages *Événements et ressources* et *Analyse des événements à l'aide d'outils externes*.

- Périphériques défense contre les menaces existants sur le centre de gestion.

Vous pouvez modifier la gestion des périphériques défense contre les menaces du centre de gestion vers CDO en utilisant la fonctionnalité de modification du gestionnaire ThreatDefense. La fonctionnalité de modification des fonctionnalités du gestionnaire Threat Defense vous permet de transférer la gestion des périphériques défense contre les menaces du centre de gestion à CDO. Lors du changement de gestionnaire, vous pouvez choisir de conserver les données d'événements générées par ces périphériques de défense contre les menaces sur le centre de gestion. Si vous choisissez de conserver les données d'événements sur le centre de gestion, une copie du périphérique défense contre les menaces dans un mode d'analyse uniquement est conservée sur le centre de gestion.

Pour en savoir plus, consultez la section Migration de Secure Firewall Threat Defense vers le nuage.

Le flux de travail est le suivant :

1. Intégration du centre de gestion au CDO

   Pour intégrer les périphériques défense contre les menaces existants du centre de gestion à CDO, vous devez intégrer le centre de gestion approprié à CDO.

   Consultez la section Intégrer un FMC pour obtenir de plus amples renseignements sur le sujet.

2. Terminer le processus de modification de la gestion de la défense contre les menaces.

   Pendant le processus de gestion des modifications de défense contre les menaces, lors du changement de gestionnaire de périphériques, vous pouvez choisir de conserver les données d'événements générées par ces périphériques défense contre les menaces sur le centre de gestion.

   Pour en savoir plus, consultez la section Migration de Secure Firewall Threat Defense vers le nuage.

3. Afficher les événements dans le centre de gestion ou le lancement croisé avec le périphérique Cisco Secure Network Analytics configuré.

   Pour afficher et utiliser les événements dans la visionneuse d'événements du centre de gestion. Si le périphérique Cisco Secure Network Analytics est déployé et intégré au déploiement du pare-feu, vous pouvez exporter les données d'événement vers le périphérique Cisco Secure Network Analytics. Cela vous permet d'effectuer un lancement croisé de l'interface utilisateur du centre de gestion vers Cisco Secure Network Analytics Manager pour afficher et gérer les données des événements.

   Pour en savoir plus, consultez les pages Événements et ressources et Analyse des événements à l'aide d'outils externes.

Configurer l'intégration SAL (local)

Vous pouvez configurer CDO pour envoyer des événements au périphérique Cisco Secure Network Analytics en utilisant l'une des options de déploiement suivantes :

- Cisco Secure Network Analytics Manager Only : déployez un gestionnaire autonome pour recevoir et stocker les événements. Les périphériques de défense contre les menaces envoient des données d'événements au gestionnaire d'analyses réseau. Toutes les données d'événements sont stockées sur Network Analytics Manager. À partir de l'interface utilisateur du centre de gestion, vous pouvez lancer plusieurs fois le gestionnaire pour afficher plus d'informations sur les événements stockés.
- Banque de données Cisco Secure Network Analytics : déployer un collecteur de flux Cisco Secure Network Analytics pour recevoir les événements, une banque de données Cisco Secure Network Analytics (contenant trois nœuds de données Cisco Secure Network Analytics) pour stocker les événements et un gestionnaire . Les périphériques de défense contre les menaces envoient les données d'événements au

collecteur de flux à partir d'où les événements sont envoyés au magasin de données pour le stockage. À partir de l'interface utilisateur du centre de gestion, vous pouvez lancer plusieurs fois le gestionnaire pour afficher plus d'informations sur les événements des magasins.

À partir de la version 7.2 de défense contre les menaces , vous pouvez choisir d'associer différents collecteurs de flux à différents périphériques.

Configurer un Cisco Secure Network Analytics Manager

Configurer le déploiement de Cisco Secure Network Analytics Manager pour intégrer SAL (local) aux périphériques défense contre les menaces gérés par CDO.

Avant de commencer

Veillez à ce que les points suivants soient respectés :

- Vous avez un détenteur CDO provisionné et vous avez les rôles d'utilisateur CDO suivants :
  - Admin
  - Super admin
- Vos périphériques défense contre les menaces fonctionnent comme prévu et génèrent des événements.
- Si vous utilisez actuellement le journal système pour envoyer des événements au Cisco Secure Network Analytics Manager à partir des versions de périphériques qui prennent en charge l'envoi direct d'événements, désactivez le journal système pour ces périphériques (ou attribuez à ces périphériques une politique de contrôle d'accès qui n'inclut pas les configurations syslog) pour éviter la duplication des événements sur le périphérique distant volume maximal.
- Vous avez le nom d'hôte ou l'adresse IP de votre Cisco Secure Network Analytics Manager.

Remarque Il se peut que vous soyez déconnecté de Cisco Secure Network Analytics Manager pendant le processus d'inscription; terminez tout travail en cours avant de commencer avec l'assistant de déploiement.

Procédure

Étape 1 Ouvrez une session sur CDO

Étape 2 Dans le menu CDO, accédez à **Outils et services** > **Centre de gestion du pare-feu**.

Étape 3 Sélectionnez **Firewall Management Center** et cliquez sur **Configuration**.

Étape 4 Accédez à **Integration** > **Security Analytics and Logging (analyse et journalisation de la sécurité d'intégration)**.

Étape 5 Dans le gadget **Cisco Secure Network Analytics Manager uniquement**, cliquez sur **Démarrer**.

Étape 6 Saisissez le nom d'hôte ou l'adresse IP et le numéro de port de Cisco Secure Network Analytics Manager, puis cliquez sur **Next**(suivant).

Étape 7 Déployez les modifications sur les périphériques gérés.

Les données de l'événement ne sont pas enregistrées dans SAL (local) tant que les modifications à la politique de journalisation ne sont pas déployées sur les périphériques défense contre les menaces enregistrés.

Remarque Si vous devez modifier l'une de ces configurations, réexécutez l'assistant. Si vous désactivez la configuration ou réexécutez l'assistant, tous les paramètres, à l'exception des informations d'authentification du compte, sont conservés.

Vous pouvez afficher et utiliser ces événements stockés à distance dans la visionneuse d'événements et l'explorateur de contexte dans le centre de gestion, puis les inclure lors de la génération de rapports. Vous pouvez également effectuer le lancement croisé à partir d'un événement dans le centre de gestion pour afficher les données associées sur le périphérique de votre Cisco Secure Network Analytics.

Pour plus de renseignements, voir l'aide en ligne du centre de gestion.

Étape 8 Cliquez sur **OK**.

Configurer un magasin de données Cisco Secure Network Analytics

Configurer un déploiement de magasin de données Cisco Secure Network Analytics pour intégrer SAL (local) aux périphériques défense contre les menaces gérés par CDO.

Avant de commencer

Veillez à ce que les points suivants soient respectés :

- Vous avez un détenteur CDO provisionné et vous avez les rôles d'utilisateur CDO suivants :
  - Admin
  - Super admin
- Vos périphériques défense contre les menaces fonctionnent comme prévu et génèrent des événements.
- Si vous utilisez actuellement syslog pour envoyer des événements au périphérique Cisco Secure Network Analytics à partir de versions de périphérique qui prennent en charge l'envoi direct des événements, désactivez syslog pour ces périphériques (ou affectez à ces périphériques une politique de contrôle d'accès qui n'inclut pas les configurations syslog) pour éviter les événements en double sur le volume distant.
- Recueillez les informations suivantes :
  - Le nom d'hôte ou l'adresse IP de votre Cisco Secure Network Analytics Manager.
  - L'adresse IP de votre collecteur de flux.

Remarque Il se peut que vous soyez déconnecté de Cisco Secure Network Analytics Manager pendant le processus d'inscription; terminez tout travail en cours avant de commencer avec l'assistant de déploiement.

Procédure

Étape 1 Ouvrez une session sur CDO

Étape 2 Dans le menu CDO, naviguez sur **Outils et services** > **Centre de gestion du pare-feu** pour ouvrir la page des **services**.

Étape 3 Choisissez **Cloud-Delivered FMC** (FMC en nuage) et cliquez sur **Configuration**.

Étape 4 Accédez à **Integration** > **Security Analytics and Logging (analyse et journalisation de la sécurité d'intégration)**.

Étape 5 Dans le gadget **Cisco Secure Network Analytics Data Store**, cliquez sur **Démarrer**.

Étape 6 Saisissez le nom d'hôte ou l'adresse IP et le numéro de port du collecteur de flux.

Pour ajouter d'autres collecteurs de flux, cliquez sur **+Ajouter un autre collecteur de flux**.

Étape 7 Si vous avez configuré plusieurs collecteurs de flux, associez les périphériques gérés à différents collecteurs de flux :

Remarque Par défaut, tous les périphériques gérés sont affectés au collecteur de flux par défaut.

a) Cliquez sur **Affecter des périphériques**
b) Sélectionnez les périphériques gérés que vous souhaitez affecter.
c) Dans la liste déroulante Réaffecter le périphérique, choisissez le collecteur de flux.

Si vous ne souhaitez pas qu'un périphérique géré envoie des données d'événement à l'un des collecteurs de flux, sélectionnez ce périphérique et choisissez **Ne pas connecter au collecteur de flux dans la liste déroulante réaffecter le périphérique.**

Vous pouvez modifier le collecteur de flux par défaut en passant le curseur sur le collecteur de flux souhaité et en cliquant sur **Définir par défaut**.

d) Cliquez sur **Apply Changes** (appliquer les modifications).
e) Cliquez sur **Next** (suivant).

Étape 8 Cliquez sur **Next** (suivant).

Étape 9 Déployez les modifications sur les périphériques gérés enregistrés.

Les données de l'événement ne sont pas enregistrées dans SAL (local) tant que les modifications à la politique de journalisation ne sont pas déployées sur les périphériques défense contre les menaces enregistrés.

Remarque Si vous devez modifier l'une de ces configurations, réexécutez l'assistant. Si vous désactivez la configuration ou réexécutez l'assistant, tous les paramètres, à l'exception des informations d'authentification du compte, sont conservés.

Vous pouvez afficher et utiliser ces événements stockés à distance dans la visionneuse d'événements et l'explorateur de contexte dans le centre de gestion, puis les inclure lors de la génération de rapports. Vous pouvez également effectuer le lancement croisé à partir d'un événement dans le centre de gestion pour afficher les données connexes sur votre Cisco Secure Network Analytics Manager.

Pour plus de renseignements, voir l'aide en ligne du centre de gestion.

À propos de SAL (SaaS)

SAL (SaaS) vous permet de capturer les événements de connexions, de prévention des intrusions, de fichiers, de programmes malveillants et de renseignements sur la sécurité de tous vos périphériques de défense contre les menaces et de les afficher en un seul endroit dans CDO. Les événements sont stockés dans le nuage de Cisco et peuvent être consultés à partir de la page de journalisation des événements dans CDO, où vous pouvez les filtrer et les examiner pour obtenir une compréhension claire des règles de sécurité qui se déclenchent dans votre réseau.

Avec des licences supplémentaires, après avoir capturé ces événements, vous pouvez effectuer un lancement croisé de CDO vers le portail Cisco Secure Cloud Analytics qui vous est destiné. Cisco Secure Cloud Analytics est un logiciel-service (SaaS) qui suit l'état de votre réseau en effectuant une analyse comportementale des événements et des flux du réseau. En recueillant des renseignements sur votre trafic réseau à partir de sources telles que les événements de pare-feu et les données de flux de réseau, il crée des observations sur le trafic et identifie automatiquement les rôles des entités du réseau en fonction de leurs schémas de trafic. En combinant ces informations à d'autres sources de renseignements sur les menaces, telles que Talos, Cisco Secure Cloud Analytics génère des alertes qui constituent un avertissement qu'un comportement peut être de nature malveillante. En plus des alertes, Cisco Secure Cloud Analytics fournit une visibilité du réseau et de l'hôte, ainsi que des renseignements contextuels qu'il a recueillis pour vous fournir une meilleure base de recherche de l'alerte et localiser les sources de comportement malveillant.

Licences pour SAL (SaaS)

Les licences SAL (SaaS) vous permettent d'utiliser un détenteur CDO pour afficher les journaux de pare-feu et une instance Cisco Secure Cloud Analytics à des fins d'analyse, sans détenir de licences distinctes pour ces produits.

Pour en savoir plus sur les options de licence SAL (SaaS) disponibles, consultez le Guide de commande de Cisco Security Analytics and Logging.

Configurer l'intégration SAL (SaaS)

Pour déployer cette intégration, vous devez configurer le stockage des données d'événements dans SAL (SaaS) à l'aide de syslog ou d'une connexion directe.

- Envoyer des événements gérés par Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) à SAL (SaaS) à l'aide de Syslog, à la page 10
- Envoyer les journaux des événements gérés par Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) à SAL (SaaS) à l'aide d'une connexion directe, à la page 13

Exigences, directives et limites de l'intégration SAL (SaaS)

Type	Description
Cisco Secure Firewall Threat Defense	• Dispositifs de défense contre les menaces autonomes gérés par CDO, versions 7.2 et ultérieures. • Pour envoyer des événements à l'aide de syslog, vous devez disposer de Threat Defense, version 6.4 ou ultérieure. • Pour envoyer directement des événements, vous devez disposer de la version Threat Defense 7.2 ou ultérieure. • Votre système de pare-feu doit être déployé et générer des événements avec succès.
Nuage régional	• Déterminez le nuage régional vers lequel vous souhaitez envoyer les événements. • Les événements ne peuvent pas être affichés ou déplacés entre les différents nuages régionaux. • Si vous utilisez une connexion directe pour envoyer les événements au nuage en vue de l'intégration avec Cisco SecureX ou Cisco SecureX threat response, vous devez utiliser la même région du nuage pour cette intégration. • Si vous envoyez les événements directement, le nuage régional que vous spécifiez dans CDO doit correspondre à la région de votre détenteur CDO.
Forfait de données	• Vous devez acheter un forfait de données qui reflète le nombre d'événements que Cisco reçoit quotidiennement sur le nuage de vos périphériques de défense contre les menaces. C'est ce qu'on appelle votre taux d'assimilation quotidien. • Utilisez l' outil d'estimation du volume de journalisation pour évaluer vos besoins en stockage de données.
Comptes	Lorsque vous achetez une licence pour cette intégration, un compte de détenteur CDO vous est fourni pour prendre en charge l'intégration.

Envoyer des événements gérés par Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) à SAL (SaaS) à l'aide de Syslog

Cette procédure fournit des informations sur la configuration d'envoi de messages syslog pour les événements de sécurité (connexions, données de sécurité, intrusions, fichiers et programmes malveillants) des périphériques gérés par CDO.

Avant de commencer

- Configurez les politiques pour générer des événements de sécurité et vérifiez que les événements que vous vous attendez à voir sont affichés dans les tableaux applicables sous le menu **Analyse**.
- Rassemblez des informations relatives à l'adresse IP, au port et au protocole du serveur Syslog (UDP ou TCP).
- Assurez-vous que vos périphériques peuvent atteindre le serveur syslog.

Procédure

Étape 1 Ouvrez une session sur CDO

Étape 2 Dans le menu CDO, cliquez sur **Outils et services** > **Centre de gestion du pare-feu** pour ouvrir la page **Services**.

Étape 3 Cliquez sur et sélectionnez **FMC en nuage**, puis cliquez sur **Configuration**.

Étape 4 Configurez les paramètres du journal système pour votre périphérique de défense contre les menaces :

a) Cliquez sur **Devices** > **Platform Settings** (paramètres de la plateforme des périphériques) et modifiez la politique de paramètres de plateforme associée à votre appareil de défense contre les menaces.

b) Dans le volet de navigation de gauche, cliquez sur **Syslog** et configurez les paramètres du journal comme suit :

Cliquez sur cet élément d'interface utilisateur...	Pour effectuer ce qui suit :
Configuration des connexions	Activez la journalisation, définissez les paramètres du serveur FTP et l'utilisation de Flash.
Destination de la journalisation	Activez la journalisation vers des destinations spécifiques et pour spécifier le filtrage par niveau de gravité des messages, par classe d'événements ou par liste d'événements personnalisée.
Configuration de la messagerie	Spécifiez l'adresse courriel utilisée comme adresse source pour les messages syslog envoyés sous forme de courriel.
Liste d'événements	Définissez une liste d'événements personnalisée qui comprend une classe d'événement, un niveau de gravité et un ID d'événement.
Limite du débit	Précisez le volume de messages envoyés à toutes les destinations configurées et définissez le niveau de gravité des messages auquel vous souhaitez affecter des limites de débit.
Paramètres journal système	Précisez la fonction de journalisation, activez l'inclusion d'un horodatage et activez d'autres paramètres pour configurer un serveur comme destination syslog.

Cliquez sur cet élément d'interface utilisateur...	Pour effectuer ce qui suit :
Serveurs journal système	Précisez l'adresse IP, le protocole utilisé, le format et la zone de sécurité du serveur Syslog désigné comme destination de journalisation.

c) Cliquez sur **Save** (enregistrer).

Étape 5 Configurez les paramètres généraux de journalisation pour la politique de contrôle d'accès (y compris la journalisation des fichiers et des programmes malveillants) :

a) Cliquez sur **Politiques** > **Contrôle d'accès**, puis modifiez la politique de contrôle d'accès associée à votre périphérique de défense contre les menaces.

b) Cliquez sur **More** (plus), puis choisissez **Logging(**journalisation). Configurez les paramètres généraux de journalisation pour la politique de contrôle d'accès (y compris la journalisation des fichiers et des programmes malveillants) comme suit :

Cliquez sur cet élément d'interface utilisateur...	Pour effectuer ce qui suit :
Envoyer en utilisant une alerte de journal système spécifique	Sélectionnez une alerte de journal système dans la liste des alertes prédéfinies existantes ou ajoutez-en une en précisant le nom, l'hôte de journalisation, le port, l'installation et la gravité.
Utilisez les paramètres de journal système configurés dans la stratégie de paramètres de la plateforme FTD déployée dans l'appareil	Unifiez la configuration du journal système en la configurant dans les **paramètres de la plateforme** et réutilisez les paramètres dans la politique de contrôle d'accès. Le niveau de gravité sélectionné est appliqué à tous les événements de connexion et de prévention des intrusions. La gravité par défaut est **ALERT**.
Envoyer des messages au journal système pour les événements IPS	Envoyer les événements sous forme de messages syslog. Les paramètres par défaut du journal système sont utilisés, sauf si vous les remplacez.
Envoyer des messages au journal système pour les événements de fichier et de maliciel	Envoyer les événements liés aux fichiers et aux programmes malveillants sous forme de messages syslog. Les paramètres par défaut du journal système sont utilisés, sauf si vous les remplacez.

c) Cliquez sur **Save** (enregistrer).

Étape 6 Activer la journalisation des événements de veille de sécurité pour la politique de contrôle d'accès :

a) Dans la même politique de contrôle d'accès, cliquez sur l'onglet **Security Intelligence**.

b) Cliquez sur **Logging** et activez la journalisation des renseignements sur la sécurité en utilisant les critères suivants :

- Par nom de domaine : cliquez sur l'enregistrement à côté de la liste déroulante **Politique DNS**.
- Par adresse IP : cliquez sur Journalisation à côté de **Networks** (Réseau).
- Par URL : cliquez sur Journalisation à côté de **URL**.

c) Cliquez sur **Save** (enregistrer).

Étape 7 Activer la journalisation syslog pour chaque règle de la politique de contrôle d'accès :

a) Dans la même politique de contrôle d'accès, cliquez sur l'onglet **Rules** (règles).
b) Cliquez sur une règle pour la modifier.
c) Cliquez sur l'onglet **Logging** (Journalisation) dans la règle.
d) Cochez les cases **Journaliser au début de la connexion** et **Journaliser à la fin de la connexion**.
e) Si vous souhaitez consigner les événements d'un fichier, cochez la case **Log Files** (Journaliser les fichiers).
f) Cochez la case. **Serveur Syslog**.
g) Vérifier que la règle est : **En utilisant la configuration syslog par défaut dans la journalisation des contrôles d'accès**.
h) Cliquez sur **Save** (enregistrer).
i) Répétez les étapes 7.a à 7.h pour chaque règle de la politique.

Prochaine étape

Si vous avez effectué toutes les modifications requises, déployez-les sur les périphériques gérés.

Envoyer les journaux des événements gérés par Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) à SAL (SaaS) à l'aide d'une connexion directe

Configurez Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) pour envoyer les événements directement à SAL (SaaS). Suivez cette procédure pour activer le paramètre global d'événement dans le nuage Cisco dans Firewall Management Center fourni en nuage. Au besoin, vous pouvez exclure des périphériques FTD individuels de l'envoi de journaux des événements à SAL (SaaS). Pour en savoir plus, consultez Activer ou désactiver les périphériques Threat Defense pour envoyer des journaux d'événements à SAL (SaaS) en utilisant une connexion directe.

Avant de commencer

- Intégrer les périphériques à Cisco Firewall Management Center en nuage, attribuer des licences à ces périphériques et configurer ces derniers pour envoyer les événements directement à SAL (SaaS).
- Activez la journalisation des connexions fondée sur les règles en modifiant une règle et en sélectionnant les options **Log at Beginning of Connection (Journaliser en début de connexion)** et **Log at End of Connection (Journaliser en fin de connexion)**.

Procédure

Étape 1 Ouvrez une session sur CDO

Étape 2 Dans le menu CDO, cliquez sur **Outils et services** > **Centre de gestion du pare-feu**.

Étape 3 Cliquez sur **FMC en nuage** dans le volet **Système** situé sur le côté droit, cliquez sur **Cisco Cloud Events**(Événements Cisco Cloud).

Étape 4 Dans le gadget **Configurer les événements Cisco Cloud**, procédez comme suit :

1. Cliquez sur le bouton à bascule **Send Events to the Cisco Cloud** (envoyer les événements à Cisco Cloud) pour activer la configuration globale.
2. Cochez la case **Send Intrusion Events to the cloud** (envoyer les incidents d'intrusion au nuage) pour envoyer les incidents d'intrusion au nuage.
3. Cochez la case **Send File and Malware Events to the cloud** (envoyer les événements de fichier et de programme malveillant dans le nuage) pour envoyer les événements de fichier et de logiciel malveillant au nuage.
4. Choisissez une option pour envoyer les événements de connexion au nuage :
   - Cliquez sur le bouton radio **Aucun** pour ne pas envoyer d'événements de connexion au nuage.
   - Cliquez sur le bouton radio **Security Events** pour envoyer uniquement les événements de sécurité au nuage.
   - Cliquez sur le bouton radio **All** (tout) pour envoyer tous les événements de connexion au nuage.
5. Cliquez sur **Save** (enregistrer).

Afficher et utiliser les événements dans CDO

Procédure

Étape 1 Ouvrez une session sur CDO

Étape 2 Dans le menu CDO, choisissez **Analyses** > **Journalisation des événements**.

Étape 3 Utilisez l'onglet **Historical** (Historique) pour afficher toutes les données des événements historiques. Par défaut, la visionneuse affiche cet onglet.

Étape 4 Pour afficher les événements en direct, cliquez sur l'onglet **Livet** (En direct).

Pour plus d'informations sur ce que vous pouvez faire sur cette page, consultez l'aide en ligne de CDO.

Afficher et utiliser des événements dans Cisco Secure Cloud Analytics

Avant de commencer

Pour assurer le flux continu des événements, avant d'utiliser la visionneuse d'événements, procédez comme suit dans le portail Stealthwatch Cloud :

- Vérifier si Cisco Secure Cloud Analytics est intégré au bon détenteur CDO.

  Pour afficher le détenteur CDO, cliquez sur **Settings** > **Sensors** (Paramètres > Capteurs).
- Ajoutez les sous-réseaux que vous souhaitez surveiller à Cisco Secure Cloud Analytics.

  Pour ajouter des sous-réseaux, cliquez sur **Paramètres** > **Sous-réseaux**.

Procédure

Étape 1 Ouvrez une session sur CDO

Étape 2 Dans le menu CDO, choisissez **Analyses** > **Secure Cloud Analytics**.

Le portail Cisco Secure Cloud Analytics s'ouvre dans un nouvel onglet de navigateur.

Étape 3 Cliquez sur **Investigate** > **Event Viewer** (enquêter sur l visionneuse d'événements).

Pour en savoir plus, consultez l'aide en ligne de Cisco Secure Cloud Analytics.

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.