Détection des applications

Les rubriques suivantes décrivent la détection des applications du système Firepower :

Présentation : détection d’applications

Lorsque le système Firepower analyse le trafic IP, il tente de déterminer les applications couramment utilisées sur votre réseau. La connaissance des applications est essentielle au contrôle des applications.

Le système détecte trois types d’applications :

- *protocoles d’application* tels que HTTP et SSH, qui représentent les communications entre les hôtes
- *les clients* tels que les navigateurs Web et les clients de courriel, qui représentent les logiciels en cours d’exécution sur l’hôte
- *des applications Web* telles que vidéo MPEG et Facebook, qui représentent le contenu ou l’URL demandée pour le trafic HTTP

Le système identifie les applications dans votre trafic réseau en fonction des caractéristiques spécifiées dans le détecteur. Par exemple, le système peut identifier une application grâce à un schéma ASCII dans l’en-tête du paquet. En outre, les détecteurs de protocole SSL (Secure socket Layers) utilisent les informations de la session sécurisée pour identifier l’application à partir de la session.

Il existe deux sources de détecteurs d’application dans le système Firepower :

- *Les détecteurs fournis par le système* détectent les applications Web, les clients et les protocoles d’application.

La disponibilité des détecteurs fournis par le système pour les applications (et les systèmes d'exploitation) dépend de la version du système Firepower et de la version de VDB que vous avez installées. Les notes de version et les avis contiennent des informations sur les détecteurs nouveaux et mis à jour. Vous pouvez également importer des détecteurs individuels créés par les services professionnels.

- *Les détecteurs de protocoles d'application personnalisés* sont créés par l'utilisateur et détectent les applications Web, les clients et les protocoles d'application.

Vous pouvez également détecter les protocoles d'application par *la détection implicite de protocole d'application*, qui sous-entend l'existence d'un protocole d'application en fonction de la détection d'un client.

Le système identifie uniquement les protocoles d'application exécutés sur les hôtes de vos réseaux surveillés, comme le précise la politique de découverte de réseau. Par exemple, si un hôte interne accède à un serveur FTP sur un site distant que vous ne surveillez pas, le système n'identifie pas le protocole d'application comme FTP. En revanche, si un hôte distant ou interne accède à un serveur FTP sur un hôte que vous surveillez, le système peut identifier formellement le protocole d'application.

Si le système peut identifier le client utilisé par un hôte surveillé pour se connecter à un serveur non surveillé, le système identifie le protocole d'application correspondant du client, mais n'ajoute pas le protocole à la cartographie du réseau. Notez que les sessions client doivent inclure une réponse du serveur pour que la détection de l'application ait lieu.

Le système effectue la description de chaque application détectée. voir Caractéristiques des applications. Le système utilise ces caractéristiques pour créer des groupes d'applications, appelés *filtres d'applications*. Les filtres d'application sont utilisés pour effectuer le contrôle d'accès et pour restreindre les résultats de recherche et les données utilisées dans les rapports et les gadgets du tableau de bord.

Vous pouvez également compléter les données du détecteur d'applications en utilisant les enregistrements NetFlow exportés, les analyses actives de Nmap et la fonctionnalité d'entrée de l'hôte.

Sujets connexes

Bonnes pratiques pour la configuration du contrôle des applications
Principes fondamentaux des détecteurs d'applications, à la page 2

Principes fondamentaux des détecteurs d'applications

Le système Firepower utilise *des détecteurs d'applications* pour identifier les applications couramment utilisées sur votre réseau. Utilisez la page Détecteurs (**Policies (politiques)** > **Application Detectors (détecteurs d'applications)**) pour afficher la liste des détecteurs et personnaliser la capacité de détection.

L'autorisation de modifier un détecteur ou son état (actif ou inactif) dépend de son type. Le système utilise uniquement des détecteurs actifs pour analyser le trafic des applications.

Remarque Les détecteurs fournis par Cisco peuvent changer avec les mises à jour du système Firepower et de la VDB. Consultez les notes de version et les avis pour obtenir des renseignements sur les détecteurs mis à jour.

Remarque Pour l'identification des applications Firepower, les ports ne sont pas répertoriés intentionnellement. Les ports associés à l'application ne sont mentionnés pour aucune application Cisco, car la plupart des applications sont indépendantes du port. Les capacités de détection de notre plateforme peuvent identifier les services en cours d'exécution sur n'importe quel port du réseau.

Détecteurs internes fournis par Cisco

Les détecteurs internes appartiennent à une catégorie spéciale de détecteurs pour le trafic des clients, des applications Web et des protocoles d'application. Les détecteurs internes sont livrés avec des mises à jour du système et sont toujours allumés.

Si une application correspond à des détecteurs internes conçus pour détecter l'activité d'un client et qu'aucun détecteur de client particulier n'existe, un client générique peut être signalé.

Détecteurs clients fournis par Cisco

Les détecteurs clients détectent le trafic client et sont envoyés via la base de données sur la base de données ou une mise à jour du système, ou sont fournis pour importation par les services professionnels de Cisco. Vous pouvez activer et désactiver les détecteurs clients. Vous pouvez exporter un détecteur client uniquement si vous l'importez.

Détecteurs d'applications Web fournis par Cisco

Les détecteurs d'applications Web détectent les applications Web dans les charges utiles de trafic HTTP et sont transmises via VDB ou une mise à jour du système. Les détecteurs d'applications Web sont toujours activés.

Détecteurs de protocole d'application (port) fournis par Cisco

Les détecteurs de protocole d'application par port utilisent des ports bien connus pour identifier le trafic réseau. Ils sont fournies par la VDB ou d'une mise à jour du système, ou sont fournis pour importation par les services professionnels de Cisco. Vous pouvez activer et désactiver les détecteurs de protocole d'application, et afficher une définition de détecteur pour l'utiliser comme base pour un détecteur personnalisé.

Détecteurs de protocole d'application (Firepower) fournis par Cisco

Les détecteurs de protocole d'application basés sur Firepower analysent le trafic réseau à l'aide des empreintes d'application Firepower et sont fournis par l'intermédiaire de VDB ou de mises à jour de système. Vous pouvez activer et désactiver les détecteurs de protocole d'application.

Détecteurs pour applications personnalisées

Les détecteurs d'applications personnalisés sont basés sur des modèles. Ils détectent des schémas dans les paquets de trafic des clients, des applications web ou des protocoles d'application. Vous avez un contrôle total sur les détecteurs importés et personnalisés.

Identification des protocoles d'application dans l'interface Web

Le tableau suivant décrit comment le système identifie les protocoles d'application détectés :

Tableau 1 : Identification du système des protocoles d'application

Identification	Description
Nom du protocole d'application	Le centre de gestion identifie un protocole d'application par son nom si le protocole d'application était : • identifié positivement par le système • identifié à l'aide des données NetFlow et qu'il existe une corrélation entre les protocoles de port et d'application dans `/etc/sf/services` • identifié manuellement à l'aide de la fonction d'entrée de l'hôte • identifié par Nmap ou une autre source active
`en attente`	centre de gestion identifie un protocole d'application comme `en attente` si le système ne peut pas l'identifier positivement ou négativement. Le plus souvent, le système doit recueillir et analyser plus de données de connexion avant de pouvoir identifier une application en attente. Dans les tableaux Détails de l'application et Serveurs, ainsi que dans le profil d'hôte, l'état `En attente` ne s'affiche que pour les protocoles d'application où un trafic de protocole d'application spécifique a été détecté (plutôt qu'inféré du trafic détecté de client ou d'application Web).
`inconnu`	centre de gestion identifie un protocole d'application comme `inconnu` dans les cas suivants : • l'application ne correspond à aucun détecteur du système. • le protocole d'application a été identifié à l'aide des données NetFlow, mais il n'y a pas de corrélation port-protocole d'application dans `/etc/sf/services`. • Snort a fermé la session, mais elle persiste sur le périphérique. Ici, le trafic est autorisé à traverser le pare-feu, mais l'application n'est pas détectée.
vide	Toutes les données détectées disponibles ont été examinées, mais aucun protocole d'application n'a été défini. Dans les tableaux Application Details et Servers, ainsi que dans le profil d'hôte, le protocole d'application n'est pas renseigné pour le trafic client générique non HTTP pour lequel aucun protocole d'application n'est détecté.

Détection implicite du protocole d'application à partir de la détection du client

Si le système peut identifier le client utilisé par un hôte surveillé pour accéder à un serveur non surveillé, le centre de gestion en conclut que la connexion utilise le protocole d'application qui correspond au client. (Comme le système ne suit les applications que sur les réseaux surveillés, les journaux de connexion n'incluent généralement pas les informations de protocole d'application pour les connexions où un hôte surveillé accède à un serveur non surveillé.)

Ce processus, ou *détection implicite de protocole d'application*, a les conséquences suivantes :

- Comme le système ne génère pas d'événement Nouveau port TCP ou Nouveau port UDP pour ces serveurs, le serveur n'apparaît pas dans le tableau Serveurs. En outre, vous ne pouvez pas déclencher

d'alertes d'événement de découverte ou de règles de corrélation en utilisant la détection de ces protocoles d'application comme critère.

- Puisque le protocole d'application n'est pas associé à un hôte, vous ne pouvez pas afficher ses détails dans les profils d'hôte, définir son identité de serveur ou utiliser ses informations dans les qualifications de profil d'hôte pour les profils de trafic ou les règles de corrélation. En outre, le système n'associe pas les vulnérabilités aux hôtes en fonction de ce type de détection.

Vous pouvez, cependant, déclencher des événements de corrélation si des informations de protocole d'application sont présentes dans une connexion. Vous pouvez également utiliser les informations de protocole d'application contenues dans les journaux de connexion pour créer des suiveurs de connexion et des profils de trafic.

Limites d'hôtes et journalisation des événements de découverte

Lorsque le système détecte un client, un serveur ou une application Web, il génère un événement de découverte, sauf si l'hôte associé a déjà atteint son nombre maximal de clients, de serveurs ou d'applications Web.

Les profils d'hôte affichent jusqu'à 16 clients, 100 serveurs et 100 applications Web par hôte.

Notez que les actions tributaires de la détection de clients, de serveurs ou d'applications Web ne sont pas touchées par cette limite. Par exemple, les règles de contrôle d'accès configurées pour se déclencher sur un serveur consigneront toujours les événements de connexion.

Considérations particulières relatives à la détection d'applications

SFTP

Afin de détecter le trafic SFTP, la même règle doit également détecter SSH.

Squid

Le système identifie clairement le trafic du serveur Squid dans les cas suivants :

- le système détecte une connexion entre un hôte de votre réseau surveillé et un serveur Squid sur lequel l'authentification proxy est activée, ou
- le système détecte une connexion entre un serveur proxy Squid de votre réseau surveillé et un système cible (c'est-à-dire le serveur de destination où le client demande des renseignements ou une autre ressource).

Cependant, le système ne peut pas identifier le trafic de service Squid dans les cas suivants :

- un hôte de votre réseau surveillé se connecte à un serveur Squid où l'authentification mandataire est désactivée, ou
- le serveur mandataire Squid est configuré pour supprimer les champs d'en-tête Via (Via:header) de ses réponses HTTP.

Détection d'applications SSL

Le système fournit des détecteurs d'applications qui peuvent utiliser les informations de session provenant d'une session SSL (Secure socket Layers) pour identifier le protocole d'application, l'application client ou l'application Web dans la session.

Lorsque le système détecte une connexion chiffrée, il marque cette connexion comme une connexion HTTPS générique ou comme un protocole sécurisé plus spécifique, comme SMTPS, le cas échéant. Lorsque le système détecte une session SSL, il ajoute `SSL client` (client SSH) au champ **Client** dans les événements de connexion de la session. S'il identifie une application Web pour la session, le système génère des événements de découverte pour le trafic.

Pour le trafic d'application SSL, les périphériques gérés peuvent également détecter le nom commun à partir du certificat du serveur et le faire correspondre à un client ou à une application Web d'un schéma hôte SSL. Lorsque le système identifie un client particulier, il remplace `client SSL` par le nom du client.

Étant donné que le trafic des applications SSL est chiffré, le système ne peut utiliser que les informations du certificat à des fins d'identification, et non les données d'application du flux chiffré. Pour cette raison, les schémas d'hôte SSL ne peuvent parfois qu'identifier l'entreprise qui a créé l'application, de sorte que les applications SSL produites par la même entreprise peuvent avoir la même identification.

Dans certains cas, par exemple lorsqu'une session HTTPS est lancée à partir d'une session HTTP, les périphériques gérés détectent le nom du serveur du certificat client dans un paquet côté client.

Pour activer l'identification d'application SSL, vous devez créer des règles de contrôle d'accès qui surveillent le trafic du répondeur. Ces règles doivent avoir une condition d'application pour l'application SSL ou des conditions d'URL utilisant l'URL du certificat SSL. Pour la découverte de réseau, l'adresse IP du répondeur ne doit pas nécessairement être dans les réseaux à surveiller dans la politique de découverte de réseau; la configuration du contrôle d'accès détermine si le trafic est identifié. Pour identifier les détections pour les applications SSL, vous pouvez filtrer par la balise de `protocole SSL`, dans la liste des détecteurs d'application ou lors de l'ajout de conditions d'application dans les règles de contrôle d'accès.

Applications Web référencées

Les serveurs Web dirigent parfois le trafic vers d'autres sites Web, qui sont souvent des serveurs de publicité. Pour vous aider à mieux comprendre le contexte dans lequel le trafic référencé se produit sur votre réseau, le système répertorie l'application Web qui a référencé le trafic dans le champ **Application Web** dans les événements de la session référencée. La VDB contient une liste de sites référencés connus. Lorsque le système détecte du trafic en provenance de l'un de ces sites, le nom du site de référence est enregistré avec l'événement pour ce trafic. Par exemple, si une publicité accessible via Facebook est en fait hébergée sur Publicité.com, le trafic Publicité.com détecté est associé à l'application Web Facebook. Le système peut également détecter les URL de référence dans le trafic HTTP, par exemple lorsqu'un site Web fournit un lien simple vers un autre site. dans ce cas, l'URL de référence s'affiche dans le champ d'événement référent HTTP.

Dans les événements (s'il existe une application de référence), elle est répertoriée comme application Web pour le trafic, tandis que l'URL est celle du site référencé. Dans l'exemple ci-dessus, l'application Web associée à l'événement de connexion pour ce trafic serait Facebook, mais l'URL serait Publicité.com. Une application Web référée peut s'afficher si aucune application Web référente n'est détectée, si l'hôte fait référence à lui-même ou s'il y a une chaîne de recommandations. Dans le tableau de bord, le nombre de connexions et d'octets pour les applications Web comprend les sessions pendant lesquelles l'application Web est associée au trafic référencé par cette application.

Notez que si vous créez une règle pour agir spécifiquement sur le trafic référencé, vous devez ajouter une condition pour l'application référencée, plutôt que l'application de référence. Pour bloquer le trafic Publicité.com provenant de Facebook, par exemple, ajoutez une condition d'application à votre règle de contrôle d'accès pour l'application Publicité.com.

Détection d'applications dans Snort 2 et Snort 3

Dans Snort 2, vous pouvez activer ou désactiver la détection d'applications par le biais des contraintes dans les politiques de contrôle d'accès et des filtres de réseau dans les politiques de découverte de réseau. Cependant, les contraintes de la politique de contrôle d'accès peuvent remplacer les filtres réseau et activer la détection des applications. Par exemple, si vous avez défini des filtres de réseau dans la politique de découverte de réseau et lorsque la politique de contrôle d'accès comporte des contraintes telles que SSL, URL SI, DNS SI, etc., qui nécessitent la détection d'applications, ces filtres de découverte de réseau sont remplacés et tous les réseaux sont surveillés afin de détecter les applications. Cette fonctionnalité de Snort 2 n'est pas prise en charge dans Snort 3.

Remarque Snort 3 est maintenant à parité avec Snort 2 en ce qui concerne l'activation de l'inspection AppID exclusivement sur des sous-réseaux particuliers qui sont définis dans les filtres de la politique de découverte de réseau **si** aucune autre configuration dans la politique de CA n'exige qu'AppID surveille tout le trafic.

Dans Snort 3, la détection des applications est toujours activée par défaut pour tous les réseaux. Pour désactiver la détection des applications, procédez comme suit :

Procédure

Étape 1 Choisissez **Policies** > **Access Control** (contrôle d'accès aux politiques), cliquez sur Edit Policy (modifier la politique) et supprimez les règles d'application.

Étape 2 Choisissez **Policies (Politiques)** > **SSL**, cliquez sur Delete pour supprimer la politique SSL.

Étape 3 Choisissez **Policies** > **Network Discovery**(politiques de découverte de réseau), cliquez sur delete pour supprimer la politique de découverte de réseau.

Étape 4 Choisissez **Policies** > **Access Control** (contrôle d'accès aux politiques) , cliquez sur **Edit** ( ) pour la politique que vous souhaitez modifier, puis cliquez sur l'onglet **Security Intelligence** > **URLs** pour supprimer la liste d'autorisation ou de blocage d'URL.

Étape 5 Comme vous ne pouvez pas supprimer les règles DNS par défaut, choisissez **Policies (Politiques)** > **DNS**, cliquez sur Edit (Modifier) et décochez la case Enabled pour désactiver la politique DNS.

Étape 6 Dans la politique de contrôle d'accès, sous les paramètres **avancés**, désactivez les options *Enable Threat Intelligence Director* (activer Threat Intelligence Director) et *Enable réputation enforcement on DNS traffic* (Activer l'application de la réputation sur le trafic DNS).

Étape 7 Enregistrez et déployez la politique de contrôle d'accès.

Exigences et conditions préalables de la détection d'applications

Prise en charge des modèles

Tout.

Domaines pris en charge

N’importe quel

Rôles utilisateur

- Admin
- Discovery Admin (administrateur de découverte)

Détecteurs pour applications personnalisées

Si vous utilisez une application personnalisée sur votre réseau, vous pouvez créer une application Web personnalisée, un client ou un détecteur de protocole d’application qui fournit au système les informations dont il a besoin pour identifier l’application. Le type de détecteur d’application est déterminé par vos sélections dans les champs **Protocole**, **Type** et **Direction**.

Les sessions client doivent inclure un paquet répondeur du serveur pour que le système commence à détecter et à identifier les protocoles d’application dans le trafic du serveur. Notez que, pour le trafic UDP, le système désigne la source du paquet du répondeur comme serveur.

Si vous avez déjà créé un détecteur sur un autre centre de gestion, vous pouvez l’exporter, puis l’importer sur ce centre de gestion. Vous pouvez ensuite modifier le détecteur importé selon vos besoins. Vous pouvez exporter et importer des détecteurs personnalisés ainsi que des détecteurs fournis par les services professionnels de Cisco. Cependant, vous **ne pouvez pas** exporter ou importer d’autres types de détecteurs fournis par Cisco.

Détecteur d’application personnalisé et champs d’application définis par l’utilisateur

Vous pouvez utiliser les champs suivants pour configurer les détecteurs d’applications personnalisées et les applications définies par l’utilisateur.

Champs du détecteur d’applications personnalisés : général

Utilisez les champs suivants pour configurer les détecteurs d’applications personnalisées de base et avancés.

Protocole d'application

Le protocole d’application que vous souhaitez détecter Il peut s’agir d’une application fournie par le système ou d’une application définie par l’utilisateur.

Si vous souhaitez que l’application soit disponible pour une dispense d’authentification active (configurée dans vos règles d’identité), vous devez sélectionner ou créer un protocole d’application avec la balise d’**`exclusion d’agent utilisateur`**.

Description

Une description du détecteur d’application.

Nom

Un nom du détecteur d’application.

Type de détecteur

Le type du détecteur, De **base** ou **avancé**. Les détecteurs d'applications de base sont créés dans l'interface Web sous la forme d'une série de champs. Les détecteurs d'application avancés sont créés en externe et chargés en tant que fichiers .lua personnalisés.

Champs du détecteur d'applications personnalisés : schémas de détection

Utilisez les champs suivants pour configurer les schémas de détection pour les détecteurs d'applications personnalisées de base.

Direction

La source du trafic que le détecteur doit inspecter, **client** ou **serveur**.

Décalage

L'emplacement dans un paquet, en octets à partir du début de la charge utile du paquet, où le système doit commencer la recherche du schéma.

Étant donné que les charges utiles de paquet commencent à l'octet 0, calculez le décalage en soustraire 1 du nombre d'octets que vous souhaitez déplacer à partir du début de la charge utile de paquet. Par exemple, pour rechercher le modèle dans le 5e bit du paquet, saisissez 4 dans le champ **Offset** (Décalage).

Schéma

La chaîne de schémas associée au **type** que vous avez sélectionné.

Ports

Le port du trafic que le détecteur doit inspecter.

Protocole

Le protocole que vous souhaitez détecter. Votre sélection de protocole détermine si le **type** ou le champ **URL** s'affiche.

Le protocole (et, dans certains cas, vos sélections ultérieures dans les champs **Type** et **Direction**) détermine(nt) le type de détecteur d'application que vous créez : application Web, client ou protocole d'application.

Type de détecteur	Protocole	Type ou direction
Application Web	HTTP	**Le Type** est le Type **de contenu** ou l' **URL.**
	RTMP	N'importe lequel
	SSL	N'importe lequel
Client	HTTP	**Le type** est **agent utilisateur**
	SIP	N'importe lequel
	TCP ou UDP.	La **direction** est **Client**
Protocole d'application	TCP ou UDP.	La **direction** est **Serveur**

Type

Le type de chaîne de schéma que vous avez saisie. Les options que vous voyez sont déterminées par le **protocole** que vous avez sélectionné. Si vous avez sélectionné **`RTMP`** comme protocole, le champ **URL** s'affiche à la place du champ **Type**.

Remarque Si vous sélectionnez **`User Agent`** (agent utilisateur) comme **type**, le système définit automatiquement la **balise** de l'application sur **`User-Agent Exclusion`** (exclusion de l'agent utilisateur).

Sélection du type	Caractéristiques de la chaîne
`Ascii`	La chaîne est codée en ASCII.
`Nom usuel`	La chaîne est valeur indiquée dans le champ CommonName du message de réponse du serveur.
`Type de contenu`	La chaîne est la valeur dans le champ content-type dans l'en-tête de réponse du serveur.
`hex`	La chaîne est en notation hexadécimale.
`Unité organisationnelle`	Il s'agit de la valeur indiquée dans le champ organizationName dans le message de réponse du serveur.
`Serveur SIP`	Il s'agit de la valeur du champ De dans l'en-tête du message.
`Hôte SSL`	Il s'agit de la valeur du champ server_name du message ClientHello.
`URL`	La chaîne est une URL. **Remarque** Le détecteur suppose que la chaîne que vous saisissez est une section complète de l'URL. Par exemple, si vous saisissez **`cisco.com`**, vous trouverez **`www.cisco.com/support`** et **`www.cisco.com`**, mais pas **`www.wearecisco.com`**.
`Agent d'utilisateur`	La chaîne est la valeur dans le champ user-agent dans l'en-tête de demande GET. Elle est également disponible pour le protocole SIP et indique que la chaîne est la valeur du champ User-Agent dans l'en-tête du message SIP.

URL

Soit une URL complète, soit une section d'une URL du champ swfURL dans le message C2 d'un paquet RTMP. Ce champ s'affiche à la place du champ **Type** lorsque vous sélectionnez **`RTMP`** comme **protocole**.

Remarque Le détecteur suppose que la chaîne que vous saisissez est une section complète de l'URL. Par exemple, si vous saisissez **`cisco.com`**, vous trouverez **`www.cisco.com/support`** et **`www.cisco.com`**, mais pas **`www.wearecisco.com`**.

Champs d'application définis par l'utilisateur

Utilisez les champs suivants pour configurer des applications définies par l'utilisateur dans les détecteurs d'applications personnalisées de base et avancés.

Pertinence commerciale

La probabilité que l'application soit utilisée dans le cadre des activités commerciales de votre organisation plutôt qu'à des fins récréatives : **`très élevée`**, **`élevée`**, **`moyenne`**, **`faible`** ou **`très faible`**. Sélectionnez l'option qui décrit le mieux l'application.

Catégories

Une classification générale de l'application qui décrit sa fonction la plus essentielle.

Description

Une description de l'application.

Nom

Un nom pour l'application.

Risque

La probabilité que l'application soit utilisée à des fins qui pourraient être contraires à la politique de sécurité de votre organisation : **`Très élevée`**, **`Élevée`**, **`Moyenne`**, **`Faible`** ou **`Très faible`**. Sélectionnez l'option qui décrit le mieux l'application.

Étiquettes

Une ou plusieurs balises prédéfinies qui fournissent des informations supplémentaires sur l'application. Si vous souhaitez qu'une application soit disponible pour une dispense d'authentification active (configurée dans vos règles d'identité), vous devez ajouter la balise d'**`exclusion d'agent utilisateur`** à votre application.

Configuration de détecteurs d'applications personnalisés

Vous pouvez configurer des détecteurs d'applications personnalisées de base ou avancés.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Cliquez sur **Créer un détecteur personnalisé**.

Étape 3 Saisissez des valeurs dans **Name** (nom) et **Description**.

Étape 4 Choisissez un **protocole d'application** dans la liste déroulante Application. Vous avez les options suivantes :

- Si vous créez un détecteur pour un protocole d'application existant (par exemple, si vous souhaitez détecter un protocole d'application particulier sur un port non standard), sélectionnez le protocole d'application dans la liste déroulante.
- Si vous créez un détecteur pour une application définie par l'utilisateur, suivez la procédure décrite dans Création d'une application définie par l'utilisateur, à la page 12.

Étape 5 Cliquez sur **Type de détecteur** comme **De base** ou **Avancé**.

Étape 6 Cliquez sur **OK**.

Étape 7 Configurer les **schémas de détection**, les **critères de détection** ou **les affectations de processus de la fonctionnalité Encrypted Visibility Engine**(Moteur de visibilité chiffrée) :

- Si vous configurez un détecteur de base, spécifiez les **schémas de détection** prédéfinis comme décrit dans Spécification des schémas de détection dans les détecteurs de base, à la page 13.
- Si vous configurez un détecteur avancé, spécifiez des **critères de détection** personnalisés comme décrit dans Spécification des critères de détection dans les détecteurs avancés, à la page 14.
- Si vous configurez un détecteur de moteur de visibilité chiffrée (ISE), spécifiez des affectations de processus EVE personnalisées comme décrit dans la section *Spécification des affectations de processus EVE* de ce chapitre.

Mise en garde Les détecteurs personnalisés avancés sont complexes et nécessitent des connaissances externes pour créer des fichiers .lua valides. Des détecteurs mal configurés peuvent avoir un impact négatif sur les performances ou la capacité de détection.

Étape 8 Vous pouvez également utiliser la capture de **paquets** pour tester le nouveau détecteur, comme décrit dans Test d'un détecteur de protocole d'application personnalisé, à la page 16.

Étape 9 Cliquez sur **Save** (enregistrer).

Remarque Si vous incluez l'application dans une règle de contrôle d'accès, le détecteur est automatiquement activé et ne peut pas être désactivé pendant l'utilisation.

Prochaine étape

- Activez le détecteur comme décrit dans Activation et désactivation des détecteurs, à la page 20.

Sujets connexes

Détecteur d'application personnalisé et champs d'application définis par l'utilisateur, à la page 8

Création d'une application définie par l'utilisateur

Les applications, les catégories et les balises créées ici sont disponibles dans les règles de contrôle d'accès et dans le gestionnaire d'objets du filtre d'application.

Mise en garde La création d'une application définie par l'utilisateur redémarre immédiatement le processus Snort sans passer par le processus de déploiement. Le système vous avertit que continuer redémarre le processus Snort et vous permet d'annuler; le redémarrage se produit sur tout périphérique géré dans le domaine actuel ou dans l'un de ses domaines enfants. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort pour obtenir de plus amples renseignements.

Avant de commencer

- Commencez à configurer votre détecteur de protocole d'application personnalisé comme décrit dans Configuration de détecteurs d'applications personnalisés, à la page 11.

Procédure

Étape 1 Dans la boîte de dialogue **Create A Personal Application Detector** (créer un détecteur d'application personnalisé), cliquer sur **Ajouter** (+) à côté du champ **Application**.

Étape 2 Entrez un **Nom**.

Étape 3 Entrez une **description**.

Étape 4 Sélectionner une **pertinence commerciale**.

Étape 5 Sélectionner un **risque**

Étape 6 Cliquez sur **Add** à côté de Catégories pour ajouter une catégorie et saisissez un nouveau nom de catégorie, ou sélectionnez une catégorie existante dans la liste déroulante **Catégories**.

Étape 7 Vous pouvez également cliquer sur **Add** (ajouter) à côté de Balises pour ajouter une balise et saisir un nouveau nom de balise, ou sélectionnez une balise existante dans la liste déroulante **Balises**.

Étape 8 Cliquez sur **OK**.

Prochaine étape

- Continuez à configurer votre détecteur de protocole d'application personnalisé comme décrit dans Configuration de détecteurs d'applications personnalisés, à la page 11. Vous devez enregistrer et activer le détecteur avant que le système puisse l'utiliser pour analyser le trafic.

Sujets connexes

Détecteur d'application personnalisé et champs d'application définis par l'utilisateur, à la page 8

Spécification des schémas de détection dans les détecteurs de base

Vous pouvez configurer un détecteur de protocole d'application personnalisé pour rechercher une chaîne de schéma particulière dans les en-têtes de paquet de protocole d'application. Vous pouvez également configurer les détecteurs pour rechercher plusieurs schémas; dans ce cas, le trafic du protocole d'application doit correspondre à tous les schémas pour que le détecteur identifie clairement le protocole d'application.

Les détecteurs de protocoles d'application peuvent rechercher des schémas ASCII ou hexadécimaux en utilisant n'importe quel décalage.

Avant de commencer

- Commencez à configurer votre détecteur de protocole d'application personnalisé comme décrit dans Configuration de détecteurs d'applications personnalisés, à la page 11.

Procédure

Étape 1 Sur la page **Create Detector** (Créer un détecteur) , dans la section **Detection Patterns** (Schéma de détection), cliquez sur **Add** (Ajouter).

Étape 2 Choisissez un type de protocole dans la liste déroulante **Application**.

Étape 3 Choisissez un type de schéma dans la liste déroulante **Type**.

Étape 4 Tapez une chaîne de **schéma** qui correspond au **Type** que vous avez spécifié.

Étape 5 Vous pouvez également saisir le **décalage** (en octets).

Étape 6 Pour identifier le trafic de protocole d'application en fonction du port utilisé, saisissez un port compris entre 1 et 65535 dans le champ **Port(s)**. Pour saisir plusieurs chiffres, séparez-les par des virgules.

Étape 7 Cliquez sur une **Direction** : `Client` ou `Serveur`.

Étape 8 Cliquez sur **OK**.

Astuces Si vous souhaitez supprimer un schéma, cliquez sur **Supprimer** ( ) à côté du schéma que vous souhaitez supprimer.

Prochaine étape

- Continuez à configurer votre détecteur de protocole d'application personnalisé comme décrit dans Configuration de détecteurs d'applications personnalisés, à la page 11. Vous devez enregistrer et activer le détecteur avant que le système puisse l'utiliser pour analyser le trafic.

Sujets connexes

Spécification des critères de détection dans les détecteurs avancés, à la page 14

Spécification des critères de détection dans les détecteurs avancés

Mise en garde Les détecteurs personnalisés avancés sont complexes et nécessitent des connaissances externes pour créer des fichiers .lua valides. Des détecteurs mal configurés peuvent avoir un impact négatif sur les performances ou la capacité de détection.

Mise en garde Ne pas téléverser de fichiers .lua provenant de sources non fiables

Les fichiers personnalisés .lua contiennent les paramètres de votre détecteur d'applications personnalisés. La création de fichiers .lua personnalisés nécessite des connaissances avancées du langage de programmation lua et une expérience de l'API C-lua de Cisco. Cisco vous recommande fortement d'utiliser les éléments suivants pour préparer les fichiers .lua :

- Des instructions et du matériel de référence tiers pour le langage de programmation lua.
- Le guide du développeur de détecteurs à code source libre : https://www.snort.org/downloads
- Ressources de la communauté OpenAppID Snort : http://blog.snort.org/search/label/openappid

Remarque Le système ne prend pas en charge les fichiers .lua qui font référence à des appels système ou à des E/S de fichiers.

Avant de commencer

- Commencez à configurer votre détecteur de protocole d'application personnalisé comme décrit dans Configuration de détecteurs d'applications personnalisés, à la page 11.
- Préparez-vous à créer un fichier .lua valide en téléchargeant et en étudiant les fichiers .lua pour connaître des détecteurs comparables. Pour en savoir plus sur le téléchargement des fichiers du détecteur, consultez Affichage ou téléchargement des détails du détecteur, à la page 17.
- Créez un fichier .lua valide qui contient les paramètres de votre détecteur d'applications personnalisés.

Procédure

Étape 1 Dans la page **Create Detector** (créer un détecteur) pour un détecteur d'application personnalisée avancée, dans la section **Detection Criteria** (critères de détection), cliquez sur **Add** (Ajouter).

Étape 2 Cliquez sur **Parcourir...** pour accéder au fichier `.lua` et le téléverser .

Étape 3 Cliquez sur **OK**.

Prochaine étape

- Continuez à configurer votre détecteur de protocole d'application personnalisé comme décrit dans Configuration de détecteurs d'applications personnalisés, à la page 11. Vous devez enregistrer et activer le détecteur avant que le système puisse l'utiliser pour analyser le trafic.

Sujets connexes

Spécification des schémas de détection dans les détecteurs de base, à la page 13

Spécification des affectations de processus EVE

Vous pouvez configurer vos propres détecteurs d'applications pour mapper les processus détectés par le moteur de visibilité chiffrée (EVE) aux applications nouvelles ou existantes.

Avant de commencer

- Commencez à configurer votre détecteur de protocole d'application personnalisé comme décrit dans Configuration de détecteurs d'applications personnalisés, à la page 11.

Procédure

Étape 1 Dans la page Créer un détecteur, dans la section Affectations de processus d'Encrypted Visibility Engine (affectation de processus du Moteur de visibilité chiffrée), cliquez sur **Add** (Ajouter).

Étape 2 Saisissez le **nom du processus** et la valeur **de confiance minimale du processus**.

Remarque Vous pouvez saisir du texte dans le champ **Process Name** (nom du processus). Cette condition est sensible à la casse. La valeur doit correspondre au nom exact du processus détecté par la fonctionnalité Encrypted Visibility Engine (Moteur de visibilité chiffrée). La **confiance minimale du processus** peut être une valeur comprise entre 0 et 100. Il s'agit de la valeur affichée dans le champ **Note de confiance du processus de visibilité chiffrée** dans Événements de connexion.

Pour en apprendre davantage sur le champ de la **note de confiance du processus de visibilité chiffrée**, consultez la section *Champs d'événement de connexion et Security Intelligence* dans le Guide d'administration du Cisco Firepower Management Center.

Étape 3 Cliquez sur **Save** (enregistrer).

Étape 4 Dans la page de liste Application Detector, activez le détecteur que vous avez créé. Pour en savoir plus, consultez Activation et désactivation des détecteurs, à la page 20. Lorsque vous activez le détecteur, les fichiers du détecteur sont transmis à tous les FTD enregistrés sur centre de gestion.

Prochaine étape

- Continuez à configurer votre détecteur de protocole d'application personnalisé comme décrit dans Configuration de détecteurs d'applications personnalisés, à la page 11. Vous devez enregistrer et activer le détecteur avant que le système puisse l'utiliser pour analyser le trafic.

Test d'un détecteur de protocole d'application personnalisé

Si vous avez un fichier de capture de paquets (pcap) qui contient des paquets avec le trafic du protocole d'application que vous souhaitez détecter, vous pouvez tester un détecteur de protocole d'application personnalisé par rapport à ce fichier pcap. Cisco recommande d'utiliser un fichier pcap simple et propre, sans trafic inutile.

Les fichiers pcap doivent être inférieurs ou égal à 256 Ko; si vous essayez de tester votre détecteur par rapport à un fichier pcap plus volumineux, centre de gestion le tronque automatiquement et teste le fichier incomplet. Vous devez corriger les sommes de contrôle non résolues dans un fichier pcap avant d'utiliser le fichier pour tester un détecteur.

Avant de commencer

- Configurez votre détecteur de protocole d'application personnalisé comme décrit dans Configuration de détecteurs d'applications personnalisés, à la page 11.

Procédure

Étape 1 Sur la page Create Detector (Créer un détecteur), dans la section Packet Captures, (Capture de paquets) cliquez sur **Add** (Ajouter).

Étape 2 Recherchez le fichier pcap dans la fenêtre contextuelle et cliquez sur **OK**.

Étape 3 Pour tester votre détecteur par rapport au contenu du fichier pcap, cliquez sur évaluer à côté du fichier pcap. Un message indique si le test a réussi.

Étape 4 Vous pouvez également répéter les étapes 1 à 3 pour tester le détecteur par rapport à d'autres fichiers pcap.

Astuces Pour supprimer un fichier pcap, cliquez sur **Supprimer** ( ) à côté du fichier que vous souhaitez supprimer.

Prochaine étape

- Continuez à configurer votre détecteur de protocole d'application personnalisé comme décrit dans Configuration de détecteurs d'applications personnalisés, à la page 11. Vous devez enregistrer et activer le détecteur avant que le système puisse l'utiliser pour analyser le trafic.

Affichage ou téléchargement des détails du détecteur

Vous pouvez utiliser la liste des détecteurs pour afficher les détails des détecteurs d'applications (tous les détecteurs) et télécharger les détails des détecteurs (détecteurs d'applications personnalisés uniquement).

Procédure

Étape 1 Pour afficher les détails du détecteur d'application, effectuez l'une des opérations suivantes :

- Reportez-vous au document *Référence du détecteur d'application Cisco Firepower* pour connaître la version de VDB à l'adresse https://www.cisco.com/c/en/us/support/security/defense-center/products-technical-reference-list.html.
- a. Sélectionnez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

  b. Filtrez la liste pour trouver un détecteur spécifique.

  c. Cliquez sur **Information** ( ).

Étape 2 Cliquez sur **Télécharger** ( ) pour télécharger les détails du détecteur pour un détecteur d'application personnalisé.

Si les commandes sont grisées, la configuration appartient à un domaine ancêtre ou vous n'avez pas les autorisations nécessaires.

Tri de la liste des détecteurs

Par défaut, la page Detectors (Détecteurs) dresse la liste des détecteurs par ordre alphabétique de nom. Une flèche vers le haut ou vers le bas à côté d'un en-tête de colonne indique que la page est triée en fonction de cette colonne dans cette direction.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Cliquez sur l'en-tête de colonne approprié.

Filtrage de la liste des détecteurs

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Développez l'un des groupes de filtres décrits dans Groupes de filtres pour la liste de détecteurs, à la page 18 et cochez la case en regard d'un filtre. Pour sélectionner tous les filtres d'un groupe, effectuez un clic droit sur le nom du groupe et sélectionnez **Tout cocher**.

Étape 3 Si vous souhaitez supprimer un filtre, cliquez sur **Enlever** (✕) dans le nom du filtre dans le champ **Filters** ou désactivez le filtre dans la liste de filtres.(Filtres) Pour supprimer tous les filtres d'un groupe, effectuez un clic droit sur le nom du groupe et sélectionnez **Uncheck All** (Désélectionner tout).

Étape 4 Si vous souhaitez supprimer tous les filtres, cliquez sur **Clear all** (effacer tout) à côté de la liste des filtres appliqués aux détecteurs.

Groupes de filtres pour la liste de détecteurs

Vous pouvez utiliser plusieurs groupes de filtres, séparément ou en combinaison, pour filtrer la liste des détecteurs.

Nom

Recherche des détecteurs dont le nom ou la description contient la chaîne que vous saisissez. Les chaînes peuvent contenir n'importe quel caractère alphanumérique ou spécial.

Filtre personnalisé

Recherche les détecteurs correspondant à un filtre d'application personnalisé créé sur la page de gestion des objets.

Auteur

Recherche les détecteurs en fonction de leur créateur. Vous pouvez filtrer les détecteurs par :

- tout utilisateur qui a créé ou importé un détecteur personnalisé
- Cisco, qui représente tous les détecteurs fournis par Cisco, à l'*exception* des détecteurs supplémentaires importés individuellement (vous êtes l'auteur de tout détecteur que vous importez).
- **Tout Utilisateur**, qui représente tous les détecteurs non fournis par Cisco

État

Recherche les détecteurs en fonction de leur état, c'est-à-dire **Actif** ou **Inactif**.

Type

Recherche des détecteurs en fonction de leur type, comme décrit dans Principes fondamentaux des détecteurs d'applications, à la page 2.

Protocole

Recherche les détecteurs en fonction du protocole de trafic qu'il inspecte.

Type

Recherche des détecteurs en fonction des catégories attribuées à l'application qu'ils détectent.

Balise

Recherche des détecteurs en fonction des balises affectées à l'application qu'ils détectent.

Risque

Recherche les détecteurs en fonction des risques affectés à l'application qu'ils détectent : **très élevé**, **élevé**, **moyen**, **faible** et **très faible**.

Pertinence commerciale

Recherche les détecteurs en fonction de la pertinence commerciale attribuée à l'application qu'ils détectent : **très élevée**, **élevée**, **moyenne**, **faible** et **très faible**.

Navigation vers d'autres pages du détecteur

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Si vous souhaitez afficher la page suivante, cliquez sur **Flèche droite** ( ).

Étape 3 Si vous souhaitez afficher la page précédente, cliquez sur **Flèche gauche** ( ).

Étape 4 Si vous souhaitez afficher une page différente, saisissez le numéro de page et appuyez sur Entrée.

Étape 5 Si vous souhaitez passer à la dernière page, cliquez sur **Flèche extrémité droite** ( ).

Étape 6 Si vous souhaitez passer à la première page, cliquez sur **Flèche d'extrémité gauche** ( ).

Activation et désactivation des détecteurs

Vous devez activer un détecteur avant de pouvoir l'utiliser pour analyser le trafic réseau. Par défaut, tous les détecteurs fournis par Cisco sont activés.

Vous pouvez activer plusieurs détecteurs d'application pour chaque port afin de compléter la capacité de détection du système.

Lorsque vous incluez une application dans une règle de contrôle d'accès d'une politique et que cette politique est déployée, s'il n'y a aucun détecteur actif pour cette application, un ou plusieurs détecteurs s'activent automatiquement. De même, lorsqu'une application est utilisée dans une politique déployée, vous ne pouvez pas désactiver un détecteur si la désactivation ne laisse aucun détecteur actif pour cette application.

Astuces Pour améliorer les performances, désactivez tout protocole d'application, client ou détecteur d'application Web que vous n'avez pas l'intention d'utiliser.

Mise en garde L'activation ou la désactivation d'un système ou d'un détecteur d'application personnalisée redémarre immédiatement le processus Snort sans passer par le processus de déploiement. Le système vous avertit que continuer redémarre le processus Snort et vous permet d'annuler; le redémarrage se produit sur tout périphérique géré dans le domaine actuel ou dans l'un de ses domaines enfants. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort pour obtenir de plus amples renseignements.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Cliquez sur le curseur à côté du détecteur que vous souhaitez activer ou désactiver. Si les contrôles sont grisés, la configuration est soit héritée d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.

Remarque Certains détecteurs d'application sont requis par d'autres détecteurs. Si vous désactivez l'un de ces détecteurs, un avertissement s'affiche pour indiquer que les détecteurs qui en dépendent sont également désactivés.

Modification des détecteurs d'applications personnalisés

Utilisez la procédure suivante pour modifier les détecteurs d'applications personnalisées.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Cliquez sur **Edit** (✎) à côté du détecteur que vous souhaitez modifier. Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Apportez des modifications au détecteur comme décrit dans Configuration de détecteurs d'applications personnalisés, à la page 11.

Étape 4 Vous avez les options d'enregistrement suivantes, selon l'état du détecteur :

- Pour enregistrer un détecteur inactif, cliquez sur **Save** (Enregistrer).
- Pour enregistrer un détecteur inactif en tant que nouveau détecteur inactif, cliquez sur **Save as New** (Enregistrer comme nouveau).
- Pour enregistrer un détecteur actif et commencer immédiatement à l'utiliser, cliquez sur **Save and Reactivate** (Enregistrer et réactiver).

  Mise en garde L'enregistrement et la réactivation d'un détecteur d'application personnalisé redémarrent immédiatement le processus Snort sans passer par le processus de déploiement. Le système vous avertit que continuer redémarre le processus Snort et vous permet d'annuler; le redémarrage se produit sur tout périphérique géré dans le domaine actuel ou dans l'un de ses domaines enfants. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort pour obtenir de plus amples renseignements.

- Pour enregistrer un détecteur actif en tant que nouveau détecteur inactif, cliquez sur **Save as New** (Enregistrer comme nouveau).

Suppression des détecteurs

Vous pouvez supprimer des détecteurs personnalisés ainsi que les détecteurs complémentaires importés individuellement et fournis par les services professionnels de Cisco. Vous ne pouvez pas supprimer les autres détecteurs fournis par Cisco, bien que vous puissiez désactiver bon nombre d'entre eux.

Remarque Lorsqu'un détecteur est utilisé dans une politique déployée, vous ne pouvez pas supprimer le détecteur.

Mise en garde La suppression d'un détecteur d'application personnalisé activé redémarre immédiatement le processus Snort sans passer par le processus de déploiement. Le système vous avertit que continuer redémarre le processus Snort et vous permet d'annuler; le redémarrage se produit sur tout périphérique géré dans le domaine actuel ou dans l'un de ses domaines enfants. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort pour obtenir de plus amples renseignements.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Cliquez sur **Supprimer** ( ) à côté du détecteur que vous souhaitez supprimer. Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **OK**.

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.