Politiques de découverte du réseau

Les rubriques suivantes décrivent comment créer, configurer et gérer les politiques de découverte de réseau :

Aperçu : politiques de découverte du réseau

La politique de découverte de réseau du centre de gestion contrôle la façon dont le système recueille les données sur les ressources réseau de votre entreprise et les segments de réseau et ports à surveiller.

Les politiques de découverte de réseau ne peuvent être configurées que pour les périphériques Cisco Secure Firewall Threat Defense qui envoient des événements à un gestionnaire d'analyse réseau. (Network Analytics Manager est un Cisco Secure Firewall Management Center local configuré pour fournir des analyses d'événements uniquement.)

Dans un déploiement multidomaine, chaque domaine descendant est doté d'une politique de découverte de réseau indépendante. Les règles de découverte de réseau et les autres paramètres ne peuvent pas être partagés, hérités ou copiés entre les domaines. Chaque fois que vous créez un nouveau domaine, le système crée une politique de découverte de réseau pour le nouveau domaine, en utilisant les paramètres par défaut. Vous devez appliquer explicitement les personnalisations souhaitées à la nouvelle politique.

Les règles de découverte de la politique précisent les réseaux et les ports que le système surveille pour générer des données de découverte en fonction des données réseau dans le trafic et des zones dans lesquelles la politique est déployée. Dans une règle, vous pouvez configurer si les hôtes, les applications et les utilisateurs ne faisant pas autorité sont découverts. Vous pouvez créer des règles pour exclure des réseaux et des zones de la découverte. Vous pouvez configurer la découverte des données à partir des exportateurs NetFlow et restreindre les protocoles au trafic dans lequel les données utilisateur sont découvertes sur votre réseau.

La politique de découverte de réseau comporte une seule règle par défaut en place, configurée pour découvrir des applications pour tout le trafic observé. La règle n'exclut aucun réseau, aucune zone ou aucun port; la découverte d'hôte et d'utilisateur n'est pas configurée et la règle n'est pas configurée pour surveiller un exportateur NetFlow. Cette politique est déployée par défaut sur tous les périphériques gérés lorsqu'ils sont enregistrés dans centre de gestion. Pour commencer à collecter des données sur l'hôte ou l'utilisateur, vous devez ajouter ou modifier des règles de découverte et redéployer la politique sur un périphérique.

Si vous souhaitez ajuster la portée de la découverte de réseau, vous pouvez créer des règles de découverte supplémentaires et modifier ou supprimer la règle par défaut.

N'oubliez pas que la politique de contrôle d'accès de chaque périphérique géré définit le trafic que vous autorisez pour cet appareil et, par conséquent, le trafic que vous pouvez surveiller avec la découverte de réseau. Si vous bloquez une partie du trafic à l'aide du contrôle d'accès, le système ne peut pas examiner ce trafic pour détecter l'activité de l'hôte, de l'utilisateur ou de l'application. Par exemple, si une politique de contrôle d'accès bloque l'accès aux applications de réseaux sociaux, le système ne peut fournir aucune donnée de découverte sur ces applications.

Si vous activez la détection d'utilisateurs basée sur le trafic dans vos règles de découverte, vous pouvez détecter les utilisateurs ne faisant pas autorité grâce à l'activité de connexion des utilisateurs dans le trafic sur un ensemble de protocoles d'application. Vous pouvez désactiver la découverte dans des protocoles particuliers pour toutes les règles, le cas échéant. La désactivation de certains protocoles peut aider à éviter d'atteindre la limite d'utilisateurs associée à votre modèle centre de gestion, en réservant le nombre d'utilisateurs disponibles pour les utilisateurs des autres protocoles.

Les paramètres de découverte réseau avancés vous permettent de gérer quelles données sont journalisées, comment les données de découverte sont stockées, quelles règles Indicateurs de compromission (IOC) sont actives, quels mappages de vulnérabilité sont utilisés pour l'évaluation d'impact et ce qui se passe lorsque des sources offrent des données de découverte contradictoires. Vous pouvez également ajouter des sources à surveiller pour l'entrée de l'hôte et les exportateurs NetFlow.

Exigences et conditions préalables pour les politiques de découverte de réseau

Prise en charge des modèles

Tout.

Domaines pris en charge

Domaine enfant

Rôles utilisateur

- Admin
- Discovery Admin (administrateur de découverte)

Personnalisation de la découverte de réseau

Les informations sur votre trafic réseau collectées par le système Firepower sont plus précieuses pour vous lorsque le système peut corréler ces informations pour identifier les hôtes les plus vulnérables et les plus importants de votre réseau.

Par exemple, si plusieurs périphériques de votre réseau exécutent une version personnalisée de SuSE Linux, le système ne peut pas identifier ce système d'exploitation et ne peut donc pas mapper les vulnérabilités aux hôtes. Cependant, sachant que le système comporte une liste de vulnérabilités pour SuSE Linux, vous pouvez

créer une empreinte personnalisée pour l'un des hôtes. Vous pourrez ensuite l'utiliser pour identifier les autres hôtes exécutant le même système d'exploitation. Vous pouvez inclure un mappage de la liste de vulnérabilités pour SuSE Linux dans l'empreinte afin d'associer cette liste à chaque hôte qui correspond à l'empreinte.

Le système vous permet également de saisir des données sur l'hôte de systèmes tiers directement dans la cartographie du réseau, à l'aide de la fonction de saisie de l'hôte. Cependant, les données d'applications ou de systèmes d'exploitation tiers ne sont pas automatiquement mappées aux informations sur les vulnérabilités. Si vous souhaitez afficher les vulnérabilités et effectuer une corrélation des impacts pour les hôtes à l'aide des données du système d'exploitation, du serveur et du protocole d'application tiers, vous devez mapper les informations sur le fournisseur et la version du système tiers avec celles et celles indiquées dans la base de données sur les vulnérabilités. (VDB). Vous pouvez également conserver les données d'entrée de l'hôte sur une base continue. Notez que même si vous mappez des données d'application avec le fournisseur et les définitions de version du système Firepower, les vulnérabilités tierces importées ne sont pas utilisées pour l'évaluation d'impact pour les clients ou les applications Web.

Si le système ne peut pas identifier les protocoles d'application exécutés sur les hôtes de votre réseau, vous pouvez créer des détecteurs de protocoles d'application définis par l'utilisateur qui permettent au système d'identifier les applications en fonction d'un port ou d'un modèle. Vous pouvez également importer, activer et désactiver certains détecteurs d'applications pour personnaliser davantage la capacité de détection d'applications du système Firepower.

Vous pouvez également remplacer la détection du système d'exploitation et des données d'application par les résultats d'analyse de l'analyseur actif Nmap ou élargir les listes de vulnérabilités par des vulnérabilités tierces. Le système peut concilier des données provenant de plusieurs sources afin de déterminer l'identité pour une application.

Configuration de la politique de découverte du réseau

Dans un déploiement multidomaine, chaque domaine a sa propre politique de découverte de réseau. Si votre compte d'utilisateur peut gérer plusieurs domaines, passez au domaine descendant dans lequel vous souhaitez configurer la politique.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Configurez les composants suivants de votre politique :

- Règles de découverte - Voir Configuration des règles de découverte du réseau, à la page 4.
- Détection basée sur le trafic pour les utilisateurs - Voir Configuration de la détection d'utilisateurs basée sur le trafic, à la page 13.
- Options avancées de découverte de réseau – Voir Configuration des options de découverte de réseau avancée, à la page 14.
- Définitions de système d'exploitation personnalisées (empreintes) – Voir les définitions Création d'une empreinte personnalisée pour les clients et Création d'une empreinte personnalisée pour les serveurs.

Règle de découverte du réseau

Les règles de découverte de réseau vous permettent d'adapter les informations découvertes à la cartographie de votre réseau afin d'inclure uniquement les données spécifiques que vous souhaitez. Les règles de votre politique de découverte de réseau sont évaluées dans l'ordre. Vous pouvez créer des règles dont les critères de surveillance se chevauchent, mais cela peut affecter les performances de votre système.

Lorsque vous excluez un hôte ou un réseau de la surveillance, l'hôte ou le réseau ne s'affiche pas dans la cartographie du réseau et aucun événement n'est signalé pour celui-ci. Cependant, lorsque les règles de découverte d'hôte pour l'adresse IP locale sont désactivées, les instances du moteur de détection sont touchées par une charge de traitement plus élevée, car les données de chaque flux sont créées de nouveau au lieu d'utiliser les données de l'hôte existantes.

Nous vous recommandons d'exclure les équilibreurs de charge (ou des ports spécifiques sur les équilibreurs de charge) et les périphériques NAT de la surveillance. Ces périphériques peuvent créer un nombre excessif et trompeur d'événements, remplir la base de données et surcharger centre de gestion. Par exemple, un périphérique NAT surveillé peut présenter plusieurs mises à jour de son système d'exploitation sur une courte période. Si vous connaissez les adresses IP de vos équilibreurs de charge et périphériques NAT, vous pouvez les exclure de la surveillance.

Astuces Le système peut identifier de nombreux équilibreurs de charge et périphériques NAT en examinant votre trafic réseau.

En outre, si vous devez créer une empreinte de serveur personnalisée, vous devez temporairement exclure de la surveillance l'adresse IP que vous utilisez pour communiquer avec l'hôte à qui vous attribuez des empreintes. Sinon, les affichages de la cartographie du réseau et des événements de découverte seront encombrés d'informations inexactes sur l'hôte représenté par cette adresse IP. Après avoir créé l'empreinte, vous pouvez configurer votre politique pour surveiller à nouveau cette adresse IP.

Cisco recommande également de **ne pas** surveiller le même segment de réseau avec les exportateurs NetFlow et les périphériques gérés. Bien que, dans l' idéal , vous devez configurer votre politique de découverte de réseau avec des règles qui ne se chevauchent pas, le système supprime les journaux de connexions en double générés par les périphériques gérés. Cependant, vous **ne pouvez pas** supprimer les journaux de connexion en double pour les connexions détectées à la fois par un périphérique géré et un exportateur NetFlow.

Configuration des règles de découverte du réseau

Vous pouvez configurer des règles de découverte pour adapter la découverte des données d'hôte et d'application à vos besoins.

Avant de commencer

- Assurez-vous que vous enregistrez des connexions pour le trafic pour lequel vous souhaitez découvrir des données réseau.
- Si vous souhaitez collecter des enregistrements NetFlow exportés, ajoutez un exportateur NetFlow, comme décrit dans Ajout de programmes d'exportation NetFlow à une politique de découverte de réseau, à la page 19.

- Si vous souhaitez afficher les graphiques de performance de découverte, vous devez activer les hôtes, les utilisateurs et les applications dans votre règle de découverte. Notez que cela peut avoir une incidence sur les performances du système.

Astuces Dans la plupart des cas, Cisco suggère de restreindre la découverte aux adresses indiquées dans la RFC 1918.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Add Rule** (ajouter une règle).

Étape 3 Définissez l'**action** de la règle comme décrit dans Actions et ressources découvertes, à la page 5.

Étape 4 Définissez les paramètres de découverte facultatifs :

- Restreindre l'action de règle à des réseaux spécifiques; voir Restrictions du réseau surveillé, à la page 7.
- Restreindre l'action de règle au trafic dans des zones spécifiques; voir Configuration des zones dans les règles de découverte de réseau, à la page 11.
- Exclure les ports de la surveillance; voir Exclusion de ports dans les règles de découverte de réseau, à la page 9.
- Configurer la règle de découverte des données NetFlow; voir Configuration des règles pour la découverte de données NetFlow, à la page 7.

Étape 5 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Actions et ressources découvertes

Lorsque vous configurez une règle de découverte, vous devez sélectionner une action pour la règle. L'effet de cette action dépend de si vous utilisez la règle pour découvrir les données d'un périphérique géré ou d'un exportateur NetFlow.

Le tableau suivant décrit les ressources découvertes par les règles avec les paramètres d'action précisés dans ces deux scénarios.

Tableau 1 : Actions de la règle de découverte

Action	Option	Périphérique géré	Exportateur Netflow
Exclure	--	Exclut le réseau précisé de la surveillance. Si l'hôte source ou de destination d'une connexion est exclu de la découverte, la connexion est enregistrée, mais les événements de découverte ne sont pas créés pour les hôtes exclus.	Exclut le réseau précisé de la surveillance. Si l'hôte source ou de destination d'une connexion est exclu de la découverte, la connexion est enregistrée, mais les événements de découverte ne sont pas créés pour les hôtes exclus.
Découvrir	Hôtes	Ajoute des hôtes à la cartographie du réseau en fonction des événements de découverte. (Facultatif, à moins que la découverte d'utilisateur ne soit activée, dans ce cas devient obligatoire.)	Ajoute des hôtes à la cartographie du réseau et journalise les connexions en fonction des enregistrements NetFlow. (Obligatoire)
Découvrir	Applications	Ajoute des applications au mappage du réseau en fonction des détecteurs d'applications. Notez que vous ne pouvez pas découvrir des hôtes ou des utilisateurs dans une règle sans découvrir également des applications. (Obligatoire)	Ajoute des protocoles d'application à la cartographie du réseau en fonction des enregistrements NetFlow et de la corrélation port-protocole d'application dans `/etc/sf/services`. (Facultatif)
Découvrir	Utilisateurs	Ajoute des utilisateurs au tableau Users (utilisateurs) et consigne l'activité des utilisateurs en fonction de la détection basée sur le trafic sur les protocoles d'utilisateur configurés dans la politique de découverte de réseau. (Facultatif)	S.O.
Journaliser les connexions NetFlow	--	S.O.	Journalise les connexions NetFlow uniquement. Ne détecte pas d'hôtes ni d'applications.

Si vous souhaitez que la règle surveille le trafic des périphériques gérés, la journalisation de l'application est requise. Si vous souhaitez que la règle surveille les utilisateurs, la journalisation de l'hôte est requise. Si vous souhaitez que la règle surveille les enregistrements NetFlow exportés, vous ne pouvez pas la configurer pour journaliser les utilisateurs, et la journalisation des applications est facultative.

Remarque Le système détecte les connexions dans les enregistrements NetFlow exportés en fonction des paramètres d'**action** de la politique de découverte de réseau. Le système détecte les connexions dans le trafic de périphériques gérés en fonction des paramètres de politique de contrôle d'accès.

Réseaux surveillés

Une règle de découverte entraîne la découverte des ressources surveillées uniquement dans le trafic à destination et en provenance des hôtes des réseaux spécifiés. Pour une règle de découverte, la découverte se produit pour les connexions qui ont au moins une adresse IP dans les réseaux spécifiés, les événements étant générés

uniquement pour les adresses IP dans les réseaux à surveiller. La règle de découverte par défaut détecte les applications de tout le trafic observé (`0.0.0.0/0` pour tout le trafic IPv4 et `::/0` pour tout le trafic IPv6).

Si vous configurez une règle pour gérer la découverte NetFlow et consigner uniquement les données de connexion, le système consigne également les connexions vers et à partir des adresses IP dans les réseaux spécifiés. Notez que les règles de découverte de réseau sont le seul moyen d'enregistrer les connexions réseau NetFlow.

Vous pouvez également utiliser l'objet réseau ou les groupes d'objets pour préciser les réseaux à surveiller.

Restrictions du réseau surveillé

Chaque règle de découverte doit inclure au moins un réseau.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Add Rule** (ajouter une règle).

Étape 3 Cliquez sur **Networks**(réseaux), si ce n'est déjà fait.

Étape 4 Vous pouvez également ajouter des objets réseau à la liste des réseaux disponibles, comme décrit dans Création d'objets réseau lors de la configuration des règles de découverte, à la page 8.

Remarque Si vous modifiez un objet réseau utilisé dans la politique de découverte du réseau, les modifications ne prennent pas effet pour la découverte tant que vous n'avez pas déployé les changements de configuration.

Étape 5 Préciser un réseau :

- Choisissez un réseau dans la liste **Available Networks** (réseaux disponibles).

  Astuces Si le réseau n'apparaît pas immédiatement dans la liste, cliquez sur **Recharger** ( ).

- Saisissez l'adresse IP dans la zone de texte sous l'étiquette Available Networks (réseaux disponibles).

Étape 6 Cliquez sur **Add** (ajouter).

Étape 7 Répétez les deux étapes précédentes pour ajouter des réseaux supplémentaires.

Étape 8 Cliquez sur **Save** (Enregistrer) pour enregistrer vos modifications.

Prochaine étape

- Déployer les changements de configuration.

Configuration des règles pour la découverte de données NetFlow

Le système peut utiliser les données des exportateurs NetFlow pour générer des événements de connexion et de découverte et pour ajouter des données d'hôte et d'application à la cartographie du réseau.

Si vous choisissez un exportateur NetFlow dans une règle de découverte, la règle se limite à la découverte des données NetFlow pour les réseaux spécifiés. Choisissez le périphérique NetFlow à surveiller avant de configurer d'autres aspects du comportement des règles, car les actions disponibles des règles changent lorsque vous choisissez un périphérique NetFlow.. Vous ne pouvez pas configurer d'exclusions de ports pour surveiller les exportateurs NetFlow.

Avant de commencer

- Ajouter des périphériques compatibles NetFlow à la politique de découverte de réseau; consultez Ajout de programmes d'exportation NetFlow à une politique de découverte de réseau, à la page 19.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Add Rule** (ajouter une règle).

Étape 3 Choisissez **NetFlow Device** (Périphériques NetFlow).

Étape 4 Dans la liste déroulante **NetFlow Device** (appareil NetFlow), choisissez l'adresse IP de l'exportateur NetFlow à surveiller.

Étape 5 Précisez le type de données NetFlow que vous souhaitez que le périphérique géré par le système collecte :

- Connection only (connexion uniquement) : choisissez `Log NetFlow Connections` (journaliser les connexions NetFlow) dans la liste déroulante **Action**.
- Host, Application, and Connection (Hôte, application et connexion) : choisissez `Discover` (Découvrir) dans la liste déroulante **Action**. Le système coche automatiquement la case **Hosts** (Hôtes) et active la collecte des données de connexion. Vous pouvez également cocher la case **Application** pour recueillir des données d'application.

Étape 6 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Création d'objets réseau lors de la configuration des règles de découverte

Vous pouvez ajouter de nouveaux objets réseau à la liste des réseaux disponibles qui s'affiche dans une règle de découverte en les ajoutant à la liste des objets réseau et des groupes réutilisables.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Dans **Networks**(réseaux), cliquez sur **Add Rule** (ajouter une règle).

Étape 3 Cliquez sur **Ajouter** (+) à côté de **available Networks**(réseaux disponibles).

Étape 4 Créez un objet réseau, comme décrit dans Création d'objets réseau.

Étape 5 Terminez d'ajouter la règle de découverte de réseau comme décrit dans Configuration des règles de découverte du réseau, à la page 4.

Exclusions de port

Tout comme vous pouvez exclure des hôtes de la surveillance, vous pouvez exclure des ports spécifiques de la surveillance. Par exemple :

- Les équilibreurs de charge peuvent signaler plusieurs applications sur le même port sur une courte période. Vous pouvez configurer vos règles de découverte de réseau afin qu'elles excluent ce port de la surveillance, par exemple en excluant le port 80 sur un équilibreur de charge qui gère une batterie de serveurs Web.
- Votre entreprise peut utiliser un client personnalisé qui utilise une plage précise de ports. Si le trafic de ce client génère un nombre excessif et trompeurs d'événements, vous pouvez exclure ces ports de la surveillance. De même, vous pouvez décider que vous ne souhaitez pas surveiller le trafic DNS. Dans ce cas, vous pourriez configurer vos règles de sorte que votre politique de découverte ne surveille pas le port 53.

Lorsque vous ajoutez des ports à exclure, vous pouvez décider d'utiliser un objet de port réutilisable dans la liste des ports disponibles, d'ajouter des ports directement aux listes d'exclusion de source ou de destination, ou de créer un nouveau port réutilisable et de le déplacer dans les listes d'exclusion.

Remarque Vous ne pouvez pas exclure de ports dans les règles qui traitent la découverte des données NetFlow.

Exclusion de ports dans les règles de découverte de réseau

Vous ne pouvez pas exclure de ports dans les règles qui traitent la découverte des données NetFlow.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Add Rule** (ajouter une règle).

Étape 3 Cliquez sur **Exclusions de port**.

Étape 4 Vous pouvez également ajouter des objets de port à la liste des ports disponibles, comme décrit dans Création d'objets port lors de la configuration des règles de découverte, à la page 10.

Étape 5 Excluez des ports sources spécifiques de la surveillance à l'aide de l'une des méthodes suivantes :

- Choisissez un port ou des ports dans la liste des **ports disponibles** et cliquez sur **Ajouter à la source**.

- Pour exclure le trafic d'un port source spécifique sans ajouter d'objet de port, dans la liste **Ports source sélectionnés**, choisissez un **protocole**, saisissez un numéro de **port** (une valeur de 1 à 65535) et cliquez sur **Add** (Ajouter).

Étape 6 Excluez des ports de destination spécifiques de la surveillance à l'aide de l'une des méthodes suivantes :

- Choisissez un port ou des ports dans la liste des **ports disponibles** et cliquez sur **Ajouter à la destination**.
- Pour exclure le trafic d'un port de destination spécifique sans ajouter d'objet de port, dans la liste **Selected Destination Ports** (ports de destination sélectionnés), choisissez un **protocole**, saisissez un numéro de **port**, puis cliquez sur **Add** (Ajouter).

Étape 7 Cliquez sur **Save** (Enregistrer) pour enregistrer vos modifications.

Prochaine étape

- Déployer les changements de configuration.

Création d'objets port lors de la configuration des règles de découverte

Vous pouvez ajouter de nouveaux objets de port à la liste des ports disponibles qui s'affiche dans une règle de découverte en les ajoutant à la liste des objets et des groupes de ports réutilisables qui peuvent être utilisés n'importe où dans le système.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Dans Networks (réseaux), cliquez sur **Add Rule** (ajouter une règle).

Étape 3 Cliquez sur **Exclusions de port**.

Étape 4 Pour ajouter un port à la liste des ports disponibles, cliquez sur **Ajouter** ( ).

Étape 5 Saisir un **nom**.

Étape 6 Dans le champ **Protocol** (protocole), précisez le protocole du trafic que vous souhaitez exclure.

Étape 7 Dans le champ **Port** (port), saisissez les ports que vous souhaitez exclure de la surveillance.

Vous pouvez spécifier un port unique, une plage de ports en utilisant le tiret (-) ou une liste de ports et de plages de ports séparés par des virgules. Les ports valides sont compris entre 1 et 65535.

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

Étape 9 Si le port n'apparaît pas immédiatement dans la liste, cliquez sur **Refresh** (Actualiser) .

Prochaine étape

- Déployer les changements de configuration.

Zones dans les règles de découverte de réseau

Pour améliorer les performances, les règles de découverte peuvent être configurées de sorte que les zones de la règle comprennent les interfaces de détection de vos périphériques gérés qui sont physiquement connectés aux réseaux à surveiller dans la règle.

Malheureusement, vous n'êtes peut-être pas toujours informé des modifications de la configuration du réseau. Un administrateur réseau peut modifier une configuration réseau par du routage ou des changements d'hôte sans vous en informer, ce qui peut compliquer la mise en place d'une politique de découverte de réseau appropriée. Si vous ne savez pas comment les interfaces de détection de vos périphériques gérés sont physiquement connectées à votre réseau, conservez la configuration de zone par défaut. Cette valeur par défaut amène le système à déployer la règle de découverte dans toutes les zones de votre déploiement. (Si aucune zone n'est exclue, le système déploie la politique de découverte sur toutes les zones.)

Configuration des zones dans les règles de découverte de réseau

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Add Rule** (ajouter une règle).

Étape 3 Cliquez sur **Zones**.

Étape 4 Choisissez une zone ou des zones dans la liste **Zones disponibles**.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer vos modifications.

Prochaine étape

- Déployer les changements de configuration.

La source d'identité de détection basée sur le trafic

La détection basée sur le trafic est la seule source d'identité ne faisant pas autorité prise en charge par le système. Une fois configurés, les périphériques gérés détectent les connexions LDAP, AIM, POP3, IMAP, Oracle, SIP (VoIP), FTP, HTTP, MDNS et SMTP sur les réseaux que vous spécifiez. Les données obtenues grâce à la détection basée sur le trafic ne peuvent être utilisées que pour la sensibilisation des utilisateurs. Contrairement aux sources d'identité autorisées, vous configurez la détection basée sur le trafic dans votre politique de découverte de réseau comme décrit dans Configuration de la détection d'utilisateurs basée sur le trafic, à la page 13.

Notez les limites suivantes :

- La détection basée sur le trafic interprète uniquement les connexions Kerberos pour les connexions LDAP comme des authentifications LDAP. Les périphériques gérés ne peuvent pas détecter les authentifications LDAP chiffrées à l'aide de protocoles tels que SSL ou TLS.
- La détection basée sur le trafic détecte les connexions AIM à l'aide du protocole OSCAR uniquement. Ils ne peuvent pas détecter les connexions AIM à l'aide de TOC2.

- La détection basée sur le trafic ne peut pas restreindre la journalisation SMTP. En effet, les utilisateurs ne sont pas ajoutés à la base de données en fonction des connexions SMTP; bien que le système détecte les connexions SMTP, les connexions ne sont pas enregistrées, sauf s'il existe déjà un utilisateur avec une adresse de courriel correspondante dans la base de données.

La détection basée sur le trafic enregistre également les tentatives de connexion échouées. Un échec de tentative de connexion n'ajoute pas de nouvel utilisateur à la liste des utilisateurs dans la base de données. Le type d'activité de l'utilisateur pour les échecs de connexion détectés par la détection basée sur le trafic est **Failed User Login** (Échec de la connexion de l'utilisateur).

Remarque Le système ne peut pas faire la distinction entre les échecs de connexions HTTP et les connexions HTTP réussies. Pour afficher les informations de l'utilisateur HTTP, vous devez activer la **capture des échecs de connexion** dans la configuration de détection basée sur le trafic.

Mise en garde Activation ou désactivation de la détection d'utilisateurs non autorisés, basée sur le trafic, via les protocoles HTTP, FTP ou MDNS, à l'aide de la politique de découverte du réseau redémarre le processus Snort lorsque vous déployez des modifications de configuration, interrompant temporairement l'inspection du trafic. 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.

Données de détection basées sur le trafic

Lorsqu'un périphérique détecte une connexion à l'aide de la détection basée sur le trafic, il envoie les informations suivantes au centre de gestion pour qu'elles soient consignées comme activité de l'utilisateur :

- le nom d'utilisateur identifié dans le champ de connexion
- l'heure de la connexion
- l'adresse IP impliquée dans la connexion, qui peut être l'adresse IP de l'hôte de l'utilisateur (pour les connexions LDAP, POP3, IMAP et AIM), du serveur (pour les connexions HTTP, MDNS, FTP, SMTP et Oracle) ou de la session créateur (pour les connexions SIP)
- l'adresse courriel de l'utilisateur (pour les connexions POP3, IMAP et SMTP)
- le nom du périphérique qui a détecté la connexion

Si l'utilisateur a été détecté précédemment, centre de gestion met à jour l'historique de connexion de cet utilisateur. Notez que centre de gestion peut utiliser les adresses courriel dans les connexions POP3 et IMAP pour établir une corrélation avec les utilisateurs LDAP. Cela signifie que, par exemple, si le centre de gestion détecte une nouvelle connexion IMAP et que l'adresse courriel de la connexion IMAP correspond à celle d'un utilisateur LDAP existant, la connexion IMAP ne crée pas un nouvel utilisateur; il met plutôt à jour l'historique de l'utilisateur LDAP.

Si l'utilisateur n''a pas été détecté auparavant, le centre de gestion l'ajoute à la base de données des utilisateurs. Les connexions AIM, SIP et Oracle uniques créent toujours de nouveaux enregistrements d'utilisateur, car il n'y a aucune donnée dans ces événements de connexion que le centre de gestion peut corréler avec d'autres types de connexion.

Le centre de gestion n'enregistre **pas** l'activité ou l'identité des utilisateurs dans les cas suivants :

- si vous avez configuré la politique de découverte de réseau pour ignorer ce type de connexion
- si un périphérique géré détecte une connexion SMTP, mais que la base de données des utilisateurs ne contient pas d'utilisateur LDAP, POP3 ou IMAP détecté précédemment avec l'adresse courriel correspondante

Les données de l'utilisateur sont ajoutées au tableau Users (utilisateurs).

Politiques de détection basées sur le trafic

Vous pouvez restreindre les protocoles dans lesquels l'activité des utilisateurs est découverte afin de réduire le nombre total d'utilisateurs détectés. Ainsi, vous pouvez vous concentrer sur les utilisateurs susceptibles de fournir les informations les plus complètes sur l'utilisateur. Le fait de limiter la détection des protocoles permet de minimiser l'encombrement par les noms d'utilisateur et de préserver l'espace de stockage sur votre centre de gestion.

Tenez compte des éléments suivants lors de la sélection des protocoles de détection basées sur le trafic :

- L'obtention de noms d'utilisateur par le biais de protocoles tels qu'AIM, POP3 et IMAP peut introduire des noms d'utilisateur non pertinents pour votre organisation en raison de l'accès au réseau par les sous-traitants, les visiteurs et d'autres invités.
- Les connexions AIM, Oracle et SIP peuvent créer des enregistrements d'utilisateur superflus. Cela se produit parce que ces types de connexion ne sont associés à aucune des métadonnées d'utilisateur que le système obtient d'un serveur LDAP ni aux informations contenues dans les autres types de connexion détectés par vos périphériques gérés. Par conséquent, centre de gestion ne peut pas corréler ces utilisateurs avec d'autres types d'utilisateurs.

Configuration de la détection d'utilisateurs basée sur le trafic

Lorsque vous activez la détection d'utilisateurs basée sur le trafic dans une règle de découverte de réseau, la découverte d'hôte est automatiquement activée. Pour en savoir plus sur la détection basée sur le trafic, consultez La source d'identité de détection basée sur le trafic, à la page 11.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Users** (Utilisateurs).

Étape 3 Cliquez sur **Edit** ( ).

Étape 4 Cochez les cases des protocoles sur lesquels vous souhaitez détecter les connexions ou décochez les cases des protocoles sur lesquels vous ne souhaitez pas détecter les connexions.

Étape 5 Cochez la case **Capture Failed Login Attempts** (Enregistrer les tentatives de connexion qui ont échoué) pour enregistrer les tentatives de connexion échouées détectées dans le trafic LDAP, POP3, FTP ou IMAP, ou pour capturer les informations des utilisateurs pour les connexions HTTP.

Étape 6 Cliquez sur **Save** (enregistrer).

Prochaine étape

Mise en garde Activation ou désactivation de la détection d'utilisateurs non autorisés, basée sur le trafic, via les protocoles HTTP, FTP ou MDNS, à l'aide de la politique de découverte du réseau redémarre le processus Snort lorsque vous déployez des modifications de configuration, interrompant temporairement l'inspection du trafic. 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.

- Configurez les règles de découverte de réseau pour découvrir les utilisateurs, comme décrit dans Configuration des règles de découverte du réseau, à la page 4.
- Déployer les changements de configuration.

Configuration des options de découverte de réseau avancée

L'option Avancé de la politique de découverte de réseau vous permet de configurer les paramètres à l'échelle de la politique pour les événements détectés, la durée de conservation des données de découverte et la fréquence de mise à jour, les mappages de vulnérabilité utilisés pour la corrélation des impacts et le fonctionnement de l'identité du système d'exploitation et du serveur. les conflits sont résolus. En outre, vous pouvez ajouter des sources d'entrée d'hôte et des exportateurs NetFlow pour permettre l'importation de données provenant d'autres sources.

Remarque Les limites d'événements de la base de données pour les événements de découverte et d'activités des utilisateurs sont définies dans la configuration du système.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Advanced** (Avancé).

Étape 3 Cliquez sur **Edit** ( ) ou **Ajouter** ( ) à côté du paramètre que vous souhaitez modifier :

- Paramètres de stockage de données : mettez à jour les paramètres comme décrit dans Configuration du stockage des données de découverte de réseau, à la page 22.
- Paramètres de journalisation des événements : mettez à jour les paramètres comme décrit dans Configuration de la journalisation des événements de découverte du réseau, à la page 22.

- Paramètres généraux : mettez à jour les paramètres comme décrit dans Configuration des paramètres généraux de la découverte de réseau, à la page 15.
- Paramètres de conflit d'identité : mettez à jour les paramètres comme décrit dans Configuration de la résolution des conflits d'identité de découverte de réseau, à la page 17.
- Indications de compromission des paramètres : mettez à jour les paramètres comme décrit dans Activation des règles d'indication de compromission, à la page 19.
- Exportateurs NetFlow : mettez à jour les paramètres comme décrit dans Ajout de programmes d'exportation NetFlow à une politique de découverte de réseau, à la page 19.
- Sources d'identité du système d'exploitation et du serveur : mettez à jour les paramètres comme décrit dans Ajout de sources d'identité du système d'exploitation et du serveur de découverte de réseau, à la page 23.
- Vulnérabilités à utiliser pour l'évaluation d'impact : mettez à jour les paramètres comme décrit dans le Activation de l'évaluation de l'incidence de la vulnérabilité de la découverte de réseau, à la page 18.

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Paramètres généraux de la découverte de réseau

Les paramètres généraux contrôlent la fréquence à laquelle le système met à jour les cartes du réseau et si les bannières de serveur sont capturées lors de la découverte.

Capturer les bannières

Activez cette case à cocher si vous souhaitez que le système stocke les informations d'en-tête du trafic réseau qui annoncent les fournisseurs et les versions de serveur (« bannières »). Ces renseignements peuvent fournir un contexte supplémentaire aux renseignements recueillis. Vous pouvez accéder aux bannières de serveur collectées pour les hôtes en accédant aux détails du serveur.

Intervalle des mises à jour

L'intervalle auquel le système met à jour les informations (par exemple, quand les adresses IP d'un hôte ont été vues pour la dernière fois, quand une application a été utilisée ou le nombre de résultats pour une application). Le paramètre par défaut est de 3600 secondes.

Notez que la définition d'un intervalle inférieur pour les délais de mise à jour fournit des informations plus précises dans l'affichage de l'hôte, mais génère plus d'événements de réseau.

Configuration des paramètres généraux de la découverte de réseau

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Advanced** (Avancé).

Étape 3 Cliquez sur **Edit** (✎) à côté de **Paramètres généraux**.

Étape 4 Mettez à jour les paramètres comme décrit dans Paramètres généraux de la découverte de réseau, à la page 15.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer les paramètres généraux.

Prochaine étape

- Déployer les changements de configuration.

Paramètres des conflits d'identité de la découverte de réseau

Le système détermine quel système d'exploitation et quelles applications s'exécutent sur un hôte en faisant correspondre les empreintes des systèmes d'exploitation et des serveurs avec les schémas du trafic. Pour fournir les informations les plus fiables qui soient sur le système d'exploitation et l'identité du serveur, le système collecte les informations sur les empreintes digitales provenant de plusieurs sources.

Le système utilise toutes les données passives pour dériver les identités du système d'exploitation et attribuer une valeur de confiance.

Par défaut, sauf en cas de conflit d'identité, les données d'identité ajoutées par un analyseur ou une application tierce remplacent les données d'identité détectées par le système Firepower. Vous pouvez utiliser les paramètres Sources d'identité pour classer par priorité les sources d'empreintes d'analyseurs et d'applications tierces. Le système conserve une identité pour chaque source, mais seules les données de l'application tierce ou de la source d'analyseur ayant la priorité la plus élevée sont utilisées comme identité actuelle. Notez, cependant, que les données d'entrée de l'utilisateur prévalent sur les données de l'analyseur et des applications tierces, quelle que soit la priorité.

Un conflit d'identité se produit lorsque le système détecte une identité qui entre en conflit avec une identité existante provenant de l'analyseur actif ou de sources d'application tierce répertoriées dans les paramètres de Sources d'identité, ou d'un utilisateur du système Firepower. Par défaut, les conflits d'identité ne sont pas résolus automatiquement et vous devez les résoudre via le profil d'hôte ou en analysant de nouveau l'hôte ou en rajoutant de nouvelles données d'identité pour remplacer l'identité passive. Cependant, vous pouvez configurer votre système pour résoudre automatiquement le conflit en conservant l'identité passive ou l'identité active.

Générer un conflit d'identité

Spécifie si le système génère un événement lorsqu'un conflit d'identité se produit.

Résoudre automatiquement les conflits

Dans la liste déroulante **Automatically Resolve Conflicts (résolution automatique des conflits**), sélectionnez l'une des options suivantes :

- **Désactivé** si vous souhaitez forcer la résolution manuelle des conflits d'identité
- **Identité** si vous souhaitez que le système utilise l'empreinte passive en cas de conflit d'identité

- **Maintenir actif** si vous souhaitez que le système utilise l'identité actuelle de la source active ayant la priorité la plus élevée lorsqu'un conflit d'identité se produit

Configuration de la résolution des conflits d'identité de découverte de réseau

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Advanced** (Avancé).

Étape 3 Cliquez sur **Edit** (✎) à côté de **Paramètres de conflit d'identité**.

Étape 4 Mettez à jour les paramètres dans la fenêtre contextuelle de modification des paramètres de conflit d'identité comme décrit dans Paramètres des conflits d'identité de la découverte de réseau, à la page 16.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer les paramètres de conflit d'identité.

Prochaine étape

- Déployer les changements de configuration.

Options d'évaluation de l'incidence de la vulnérabilité de la découverte de réseau

Vous pouvez configurer la façon dont le système effectue la corrélation d'impact avec les incidents d'intrusion. Voici les différents choix proposés :

- Cochez la case **Use Network Discovery Vulnerability Mappings** (Utiliser les mappages de vulnérabilité de la découverte du réseau) si vous souhaitez utiliser les informations de vulnérabilité basées sur le système pour effectuer la corrélation d'impact.
- Cochez la case **Use Third-Party Vulnerability Mappings** (utiliser des mappages de vulnérabilités tiers) si vous souhaitez utiliser des références de vulnérabilité tierces pour effectuer la corrélation d'impact. Pour obtenir plus d'informations, reportez-vous à la *Guide d'API des entrées d'hôte du système Firepower*.

Vous pouvez cocher l'une des cases ou les deux. Si le système génère un incident d'intrusion et que l'hôte impliqué dans l'événement possède des serveurs ou un système d'exploitation avec des vulnérabilités dans les ensembles de mappage de vulnérabilité sélectionnés, l'incident d'intrusion est marqué par l'icône d'incidence sur la vulnérabilité (niveau 1 : rouge). Pour les serveurs qui ne disposent pas d'informations sur le fournisseur ou la version, notez que vous devez activer le mappage des vulnérabilités dans la configuration centre de gestion.

Si vous décochez les deux cases, les incidents d'intrusion ne seront **jamais** signalés par l'icône d'impact de vulnérabilité (niveau 1 : rouge).

Sujets connexes

Cartographie des vulnérabilités tierces

Activation de l'évaluation de l'incidence de la vulnérabilité de la découverte de réseau

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Advanced** (Avancé).

Étape 3 Cliquez sur **Edit** (✎) à côté de **Vulnérabilités à utiliser pour l'évaluation d'incidence**.

Étape 4 Mettez à jour les paramètres dans la fenêtre contextuelle Edit Vulnerability Settings (Modifier les paramètres de vulnérabilité), comme décrit dans Options d'évaluation de l'incidence de la vulnérabilité de la découverte de réseau, à la page 17.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer les paramètres de vulnérabilité.

Prochaine étape

- Déployer les changements de configuration.

Indices de compromission (IoC)

Le système utilise les règles IOC de la politique de découverte de réseau pour identifier un hôte comme susceptible d'être compromis par des moyens malveillants. Lorsqu'un hôte répond aux conditions spécifiées dans ces règles fournies par le système, le système lui donne une *indication de compromission* (IOC). Les règles connexes sont appelées *règles IOC*. Chaque règle IOC correspond à un type de balise IOC. Les *balises IOC* précisent la nature de la compromission probable.

Le centre de gestion peut étiqueter l'hôte et l'utilisateur concernés lorsque l'une des situations suivantes se produit :

- Le système met en corrélation les données recueillies sur votre réseau surveillé et son trafic, à l'aide d'incidents d'intrusion, de connexion, de renseignements sur la sécurité, et de fichiers ou de programmes malveillants, et détermine qu'un IOC potentiel s'est produit.
- Le centre de gestion peut importer des données IOC de vos déploiements AMP pour les points terminaux via le nuage AMP. Comme ces données examinent l'activité sur un hôte lui-même - par exemple les actions entreprises par ou sur des programmes individuels - elles peuvent donner des indications sur les menaces éventuelles, ce que ne peuvent pas faire les données relatives au réseau uniquement. Pour votre commodité, centre de gestion obtient automatiquement toutes les nouvelles balises IOC que Cisco développe à partir du nuage AMP.

Pour configurer cette fonction, consultez Activation des règles d'indication de compromission, à la page 19.

Vous pouvez également écrire des règles de corrélation avec les données IOC des hôtes et les listes de conformité autoriser qui prennent en compte les hôtes marqués IOC.

Pour étudier et utiliser les IOC marqués de balises, consultez la section *Indications de compromission de données* et ses sous-sections dans Guide d'administration Cisco Secure Firewall Management Center.

Activation des règles d'indication de compromission

Pour que votre système puisse détecter et baliser des indications de compromission (IOC), vous devez d'abord activer au moins une règle IOC dans votre politique de découverte de réseau. Chaque règle IOC correspond à un type de balise IOC et toutes les règles IOC sont prédéfinies par Cisco. vous ne pouvez pas créer les règles d'origine. Vous pouvez activer une partie ou l'ensemble des règles, selon les besoins de votre réseau et de votre organisation. Par exemple, si les hôtes utilisant des logiciels comme Microsoft Excel ne s'affichent jamais sur votre réseau surveillé, vous pouvez décider de ne pas activer les balises IOC qui se rapportent aux menaces basées sur Excel.

Avant de commencer

Étant donné que les règles IOC se déclenchent en fonction des données fournies par d'autres composants du système et par AMP pour les points terminaux, ces composants doivent disposer de la licence et être configurés correctement pour que les règles IOC définissent des balises IOC. Activez les fonctionnalités du système associées aux règles IOC que vous souhaitez activer, telles que la détection et la prévention des intrusions (IPS) et la protection avancée contre les programmes malveillants (AMP). Si une fonctionnalité associée d'une règle IOC n'est pas activée, aucune donnée pertinente n'est collectée et la règle ne peut pas se déclencher.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Advanced** (Avancé).

Étape 3 Cliquez sur **Edit** ( ) à côté d'**Indications of Compromise Settings** (Paramètres des indicateurs de compromission).

Étape 4 Pour activer ou désactiver l'ensemble de la fonction IOC, cliquez sur le curseur à côté de **Enable IOC** (Activer IOC).

Étape 5 Pour activer ou désactiver globalement les règles IOC individuelles, cliquez sur le curseur dans la colonne **Enabled** (activé) de la règle.

Étape 6 Cliquez sur **Save** (Enregistrer) pour sauvegarder vos paramètres.

Prochaine étape

- Déployer les changements de configuration.

Ajout de programmes d'exportation NetFlow à une politique de découverte de réseau

Avant de commencer

- Configurez les exportateurs NetFlow que vous prévoyez utiliser comme décrit dans le Données NetFlow.

- Passez en revue les autres conditions préalables à NetFlow décrites dans les Exigences relatives à l'utilisation des données NetFlow.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Advanced** (Avancé).

Étape 3 Cliquez sur **Ajouter** (+) à côté de **Périphériques NetFlow**.

Étape 4 Dans le champ **IP Address** (adresse IP), saisissez l'adresse IP du périphérique réseau à partir duquel vous souhaitez que le périphérique géré collecte des données NetFlow.

Étape 5 De manière facultative :

- Répétez les deux étapes précédentes pour ajouter des exportateurs NetFlow supplémentaires.
- Supprimez un exportateur NetFlow en cliquant sur **Supprimer** (🗑). Gardez à l'esprit que si vous utilisez un exportateur NetFlow dans une règle de découverte, vous devez supprimer la règle avant de pouvoir supprimer le périphérique à partir de la page Avancé.

Étape 6 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Configurez une règle de découverte de réseau pour surveiller le trafic NetFlow, comme décrit dans Configuration des règles de découverte du réseau, à la page 4.
- Déployer les changements de configuration.

Paramètres pour le stockage des données de Découverte du réseau

Les paramètres de stockage des données de découverte comprennent les paramètres de limite d'hôte et de délai d'expiration.

Lorsque la limite d'hôtes est atteinte

Le nombre d'hôtes que Cisco Secure Firewall Management Center peut surveiller et donc stocker dans des cartes réseau dépend de son modèle. L' option **When Host Limit Reached** (Lorsque la limite de l'hôte est atteinte) contrôle ce qui se passe lorsque vous détectez un nouvel hôte après avoir atteint la limite d'hôte. Vous pouvez réaliser les actions suivantes :

Supprimer les hôtes

Le système abandonne l'hôte qui est rester inactif le plus longtemps, puis ajoute le nouvel hôte. Il s'agit du paramètre par défaut.

Ne pas insérer de nouveaux hôtes

Le système ne suit pas les hôtes nouvellement découverts. Le système assure le suivi des nouveaux hôtes uniquement lorsque le nombre d'hôtes descend sous la limite, par exemple après qu'un administrateur ait augmenté la limite d'hôte du domaine ou supprimé manuellement des hôtes de la cartographie du réseau, ou si le système identifie des hôtes comme ayant expiré en raison d'une inactivité.

Dans un déploiement multidomaine, les domaines enfants partagent l'ensemble disponible d'hôtes surveillés. Pour vous assurer que chaque domaine enfant peut remplir sa carte réseau, vous pouvez définir des limites d'hôte à chaque niveau de sous-domaine dans les propriétés du domaine. Étant donné que chaque domaine enfant possède sa propre politique de découverte du réseau, chaque domaine enfant régit son propre comportement lorsque le système découvre un nouvel hôte, comme décrit dans le tableau suivant.

Tableau 2 : Atteinte de la limite d'hôte avec l'architecture multi-détenteur

Paramètres	La limite d'hôte de domaine a-t-elle été définie?	Limite d'hôte de domaine atteinte	Limite d'hôte du domaine ancêtre atteinte
Supprimer les hôtes	oui	Abandon de l'hôte le plus ancien du domaine contraint.	Supprime l'hôte le plus ancien parmi tous les domaines feuilles descendants configurés pour abandonner des hôtes. Si aucun hôte ne peut être supprimé, n'ajoute pas l'hôte.
	non	S.O.	Supprime l'hôte le plus ancien parmi tous les domaines descendants configurés pour abandonner les hôtes et qui partagent l'ensemble général.
N'insère pas de nouveaux hôtes	oui ou non	N'ajoute pas l'hôte.	N'ajoute pas l'hôte.

Expiration du délai de l'hôte

Le temps qui s'écoule, en minutes, avant que le système ne supprime un hôte de la cartographie du réseau pour cause d'inactivité. Le paramètre par défaut est 10080 minutes (une semaine). Les adresses MAC et IP d'hôte peuvent expirer individuellement, mais un hôte ne disparaît pas de la cartographie du réseau, sauf si toutes ses adresses associées expirent.

Pour éviter l'expiration prématurée des hôtes, vérifiez que la valeur du délai d'expiration de l'hôte est supérieure à l'intervalle de mise à jour dans les paramètres généraux de la politique de découverte de réseau.

Expiration du serveur

Le temps qui s'écoule, en minutes, avant que le système ne supprime un serveur de la cartographie du réseau pour cause d'inactivité. Le paramètre par défaut est 10080 minutes (une semaine).

Pour éviter l'expiration prématurée des serveurs, vérifiez que la valeur du délai d'expiration du service est plus longue que l'intervalle de mise à jour dans les paramètres généraux de la politique de découverte de réseau.

Délai d'expiration de l'application client

Le temps qui s'écoule, en minutes, avant que le système ne supprime un client de la cartographie du réseau pour cause d'inactivité. Le paramètre par défaut est 10080 minutes (une semaine).

Assurez-vous que la valeur du délai d'expiration du client est supérieure à l'intervalle de mise à jour dans les paramètres généraux de la politique de découverte de réseau.

Sujets connexes

Limite d'hôte du système Firepower

Configuration du stockage des données de découverte de réseau

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Advanced** (Avancé).

Étape 3 Cliquez sur **Edit** (✎) à côté des **Paramètres de stockage des données de découverte du réseau**.

Étape 4 Mettez à jour les paramètres dans la boîte de dialogue des paramètres de stockage de données comme décrit dans Paramètres pour le stockage des données de Découverte du réseau, à la page 20.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer les paramètres de stockage de données.

Prochaine étape

- Déployer les changements de configuration.

Configuration de la journalisation des événements de découverte du réseau

Les paramètres de journalisation des événements contrôlent si les événements de découverte et d'entrée de l'hôte sont enregistrés. Si vous ne consignez pas un événement, vous ne pouvez pas le récupérer dans les vues d'événements ou l'utiliser pour déclencher des règles de corrélation.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Advanced** (Avancé).

Étape 3 Cliquez sur **Edit** (✎) à côté des **Paramètres de la journalisation des événements**.

Étape 4 Cochez ou décochez les cases des types d'événements de découverte et d'entrée d'hôte que vous souhaitez consigner dans la base de données .

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer les paramètres de journalisation des événements.

Prochaine étape

- Déployer les changements de configuration.

Ajout de sources d'identité du système d'exploitation et du serveur de découverte de réseau

Dans la zone Advanced (Avancé) de la politique de découverte de réseau, vous pouvez ajouter de nouvelles sources actives ou modifier les paramètres de priorité ou de délai d'expiration des sources existantes.

L'ajout d'un analyseur à cette page n'ajoute pas les capacités d'intégration complètes qui existent pour les analyseurs Nmap, mais permet l'intégration d'applications tierces importées ou de résultats d'analyse.

Si vous importez des données d'une application ou d'un analyseur tiers, veillez à faire correspondre les vulnérabilités de la source avec les vulnérabilités détectées dans votre réseau.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Advanced** (Avancé).

Étape 3 Cliquez sur **Edit** ( ) à côté de **Sources d'identité du système d'exploitation et du serveur**.

Étape 4 Pour ajouter une nouvelle source, cliquez sur **Add Source** (Ajouter une source).

Étape 5 Saisissez un **Nom**.

Étape 6 Choisissez le **type** de source d'entrée dans la liste déroulante :

- Choisissez **Scanner** (Analyseur) si vous prévoyez importer les résultats d'analyse à l'aide de la fonction AddScanResult.
- Choisissez **Application** si vous ne prévoyez pas importer les résultats d'analyse.

Étape 7 Pour indiquer la durée qui doit s'exécuter entre l'ajout d'une identité à la cartographie du réseau par cette source et la suppression de cette identité, choisissez **Hours**, **Days** ou **Weeks** (Heures, jours ou semaines) dans la liste déroulante **Timeout** (délai d'expiration) et saisissez la durée appropriée.

Étape 8 De manière facultative :

- Pour promouvoir une source et faire en sorte que le système d'exploitation et les identités d'application soient utilisées en faveur des sources situées en dessous d'elle dans la liste, choisissez la source et cliquez sur la flèche vers le haut.
- Pour rétrograder une source et permettre l'utilisation des identités du système d'exploitation et des applications uniquement si aucune identité n'est fournie par les sources au-dessus dans la liste, choisissez la source et cliquez sur la flèche vers le bas.
- Pour supprimer une source, cliquez sur **Supprimer** ( ) à côté de la source.

Étape 9 Cliquez sur **Save** (Enregistrer) pour enregistrer les paramètres de la source d'identité.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Cartographie des vulnérabilités tierces

Dépannage de la politique de découverte de réseau

Avant d'apporter des modifications aux capacités de détection par défaut du système, vous devez analyser les hôtes qui ne sont pas identifiés correctement et les raisons pour lesquelles vous pouvez décider de la solution à mettre en œuvre.

Vos périphériques gérés sont-ils correctement placés?

Si des périphériques réseau tels que des équilibreurs de charge, des serveurs proxy ou des périphériques NAT se trouvent entre le périphérique géré et l'hôte non identifié ou mal identifié, placez un périphérique géré plus près de l'hôte mal identifié plutôt que d'utiliser la prise d'empreinte personnalisée. Cisco ne recommande pas l'utilisation de la prise d'empreinte personnalisée dans ce scénario.

Les systèmes d'exploitation non identifiés ont-ils une pile TCP unique?

Si le système fait une erreur dans l'identification d'un hôte, vous devez rechercher pourquoi l'hôte est mal identifié afin de vous aider à décider entre créer et activer une empreinte personnalisée ou remplacer les données d'entrée de Nmap ou de l'hôte par les données de découverte.

⚠

Mise en garde Si vous rencontrez des hôtes mal identifiés, contactez votre représentant du soutien avant de créer des empreintes personnalisées.

Si un hôte exécute un système d'exploitation qui n'est pas détecté par le système par défaut et ne partage pas les caractéristiques d'identification de la pile TCP avec les systèmes d'exploitation existants détectés, vous devez créer une empreinte personnalisée.

Par exemple, si vous avez une version personnalisée de Linux avec une pile TCP unique que le système ne peut pas identifier, vous auriez avantage à créer une empreinte personnalisée, qui permet au système d'identifier l'hôte et de continuer au surveiller, plutôt que d'utiliser les résultats d'analyse ou données de tiers, ce qui nécessite une mise à jour active et continue des données.

Notez que de nombreuses distributions Linux à code source libre utilisent le même noyau et que, par conséquent, le système les identifie à l'aide du nom du noyau Linux. Si vous créez une empreinte personnalisée pour un système Red Hat Linux, il se peut que d'autres systèmes d'exploitation (tels que Debian Linux, Mandrake Linux, Knoppix, etc.) soient identifiés comme étant Red Hat Linux, car la même empreinte correspond à plusieurs distributions Linux.

Vous ne devriez pas utiliser une empreinte dans toutes les situations. Par exemple, une modification peut avoir été apportée à la pile TCP d'un hôte de sorte qu'elle ressemble ou soit identique à un autre système d'exploitation. Par exemple, un hôte Apple Mac OS X est modifié, rendant son empreinte identique à celle

d'un hôte Linux 2.4, ce qui fait que le système l'identifie comme Linux 2.4 au lieu de Mac OS X. Si vous créez une empreinte personnalisée pour l'hôte Mac OS X, cela peut entraîner l'identification à erreur de tous les hôtes Linux 2.4 légitimes comme des hôtes Mac OS X. Dans ce cas, si Nmap identifie correctement l'hôte, vous pouvez planifier des analyses Nmap régulières pour cet hôte.

Si vous importez des données d'un système tiers à l'aide de l'entrée de l'hôte, vous devez mapper les chaînes de fournisseur, de produit et de version que le tiers utilise pour décrire les serveurs et les protocoles d'application aux définitions Cisco pour ces produits. Notez que même si vous mappez des données d'application avec le fournisseur et les définitions de version du système Firepower, les vulnérabilités tierces importées ne sont pas utilisées pour l'évaluation d'impact pour les clients ou les applications Web.

Le système peut concilier des données provenant de plusieurs sources afin de déterminer l'identité actuelle pour un système d'exploitation ou une application.

Pour les données Nmap, vous pouvez planifier des analyses Nmap régulières. Pour les données d'entrée de l'hôte, vous pouvez exécuter régulièrement le script Perl pour l'importation ou l'utilitaire de ligne de commande. Cependant, notez que les données d'analyse active et les données d'entrée de l'hôte peuvent ne pas être mises à jour avec la fréquence des données de découverte.

Le système Firepower peut-il identifier toutes les applications?

Si un hôte est correctement identifié par le système, mais qu'il comporte des applications non identifiées, vous pouvez créer un détecteur défini par l'utilisateur pour fournir au système des informations de correspondance de port et de modèle afin d'aider à identifier l'application.

avez-vous appliqué des correctifs qui corrigent des vulnérabilités?

Si le système identifie correctement un hôte mais ne reflète pas les correctifs appliqués, vous pouvez utiliser la fonction de saisie de l'hôte pour importer les informations sur le correctif. Lorsque vous importez des informations sur un correctif, vous devez mapper le nom du correctif avec un correctif dans la base de données.

Voulez-vous suivre les vulnérabilités des tiers?

Si vous avez des informations de vulnérabilité provenant d'un système tiers que vous souhaitez utiliser pour la corrélation de l'incidence, vous pouvez faire correspondre les identifiants de vulnérabilité tiers pour les serveurs et les protocoles d'application aux identifiants de vulnérabilité dans la base de données Cisco, puis importer les vulnérabilités à l'aide de la fonction saisie de l'hôte. Pour en savoir plus sur l'utilisation de la fonction de saisie de l'hôte, consultez *Guide d'API des entrées d'hôte du système Firepower*. Notez que même si vous mappez des données d'application avec le fournisseur et les définitions de version du système Firepower, les vulnérabilités tierces importées ne sont pas utilisées pour l'évaluation d'impact pour les clients ou les applications Web.

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.