Un aperçu de l'analyse de réseau et de la politique de prévention des intrusions

Le moteur d'inspection Snort fait partie intégrante du périphérique Cisco Secure Firewall Threat Defense (anciennement Firepower Threat Defense). Ce chapitre fournit une présentation de Snort 3 et de l'analyse de réseau et des politiques de prévention des intrusions. Il fournit également un aperçu des politiques d'analyse de réseau et de prévention des intrusions fournies et personnalisées par le système.

À propos des politiques d'analyse de réseau et de prévention des intrusions

Les politiques d'analyse de réseau et de prévention des intrusions fonctionnent ensemble dans le cadre de la fonction de détection et de prévention des intrusions.

- L'expression *détection des intrusions* fait généralement référence au processus de surveillance et d'analyse passives du trafic réseau à la recherche des intrusions potentielles et de stockage des données d'attaque pour l'analyse de la sécurité. C'est ce que l'on appelle parfois « IDS ».
- Le terme *prévention des intrusions* comprend le concept de détection des intrusions, mais ajoute la possibilité de bloquer ou de modifier le trafic malveillant lorsqu'il traverse votre réseau. C'est ce que l'on appelle parfois « IPS ».

Dans un déploiement de prévention des intrusions, lorsque le système examine les paquets :

- Une **politique d'analyse de réseau** régit la façon dont le trafic est *décodé* et *prétraité* afin qu'il puisse être évalué de manière plus approfondie, en particulier pour détecter un trafic anormal qui pourrait signaler une tentative d'intrusion.

- Une **politique** de prévention des intrusions utilise des règles d'*intrusion et de préprocesseur* (parfois appelées collectivement *règles de prévention des intrusions*) pour examiner les paquets décodés à la recherche d'attaques basées sur des modèles. Les politiques de prévention des intrusions sont associées à *des ensembles de variables*, ce qui vous permet d'utiliser des valeurs nommées pour refléter avec précision votre environnement réseau.

Les politiques d'analyse de réseau et de prévention des intrusions sont toutes deux appelées par une politique de contrôle d'accès parente, mais à des moments différents. Pendant que le système analyse le trafic, la phase d'analyse de réseau (décodage et prétraitement) se produit avant et séparément de la phase de prévention des intrusions (prétraitement et règles de prévention des intrusions supplémentaires). Ensemble, les politiques d'analyse de réseau et de prévention des intrusions permettent une inspection large et approfondie des paquets. Elles peuvent vous aider à détecter le trafic réseau, à vous alerter et à vous protéger contre le trafic réseau qui pourrait menacer la disponibilité, l'intégrité et la confidentialité des hôtes et de leurs données.

Le système est livré avec plusieurs politiques d'analyse de réseau et de prévention des intrusions du même nom (par exemple, Sécurité et connectivité équilibrées) qui se complètent et fonctionnent ensemble. En utilisant des politiques fournies par le système, vous pouvez profiter de l'expérience de Cisco Talos Intelligence Group (Talos). Pour ces politiques, Talos définit les états des règles de prévention des intrusions et des inspecteurs, et fournit les configurations initiales pour les inspecteurs et d'autres paramètres avancés.

Vous pouvez également créer des politiques personnalisées d'analyse de réseau et de prévention des intrusions. Vous pouvez ajuster les paramètres des politiques personnalisées pour inspecter le trafic de la manière qui vous semble la plus importante, afin d'améliorer à la fois les performances de vos périphériques gérés et votre capacité à répondre efficacement aux événements qu'ils génèrent.

Vous créez, modifiez, enregistrez et gérez les politiques d'analyse de réseau et de prévention des intrusions à l'aide d'éditeurs de politiques similaires dans l'interface Web. Lorsque vous modifiez l'un ou l'autre de ces types de politique, un panneau de navigation s'affiche sur le côté gauche de l'interface Web; le côté droit affiche diverses pages de configuration.

Reportez-vous aux vidéos pour obtenir de l'aide et des renseignements supplémentaires :

- Présentation condensée de Snort 3
- Présentation étendue de Snort 3

Plateforme d'inspection Snort

La plateforme d'inspection Snort fait partie intégrante du périphérique Cisco Secure Firewall Threat Defense (anciennement Firepower Threat Defense). La plateforme d'inspection analyse le trafic en temps réel pour fournir une inspection approfondie des paquets. Les politiques d'analyse de réseau et de prévention des intrusions utilisent les capacités de la plateforme d'inspection Snort pour détecter les intrusions et en protéger le système.

Snort 3

Snort 3 est la dernière version du moteur d'inspection de Snort, qui présente de grandes améliorations par rapport à la version antérieure de ce dernier. L'ancienne version de Snort est Snort 2. Snort 3 est plus efficace, et offre de meilleures performances et une meilleure évolutivité.

L’architecture de Snort 3 a été repensée pour inspecter plus de trafic avec des ressources équivalentes par rapport à Snort 2. Snort 3 permet une insertion simplifiée et flexible des analyseurs de trafic. Snort 3 fournit également une nouvelle syntaxe de règles qui facilite l’écriture de règles et rend visibles les équivalents des règles d’objets partagés.

Les autres changements importants concernant Snort 3 sont les suivants :

- Contrairement à Snort 2, qui utilise plusieurs instances de Snort, Snort 3 associe plusieurs threads à une seule instance de Snort. Cela utilise moins de mémoire, améliore les temps de rechargement Snort, prend en charge un plus grand nombre de règles de prévention des intrusions ainsi qu’une cartographie du réseau plus vaste. Le nombre de threads Snort varie selon la plateforme et est identique au nombre d’instances de Snort 2 pour chaque plateforme. L’utilisation est pratiquement transparente.
- Version Snort par Threat Defense : le moteur d’inspection Snort est spécifique à Threat Defense et non au Cisco Secure Firewall Management Center (anciennement le centre de gestion Cisco Firepower Management Center). Centre de gestion peut gérer plusieurs Threat Defense, chacun avec l’une ou l’autre des versions de Snort (Snort 2 et Snort 3). Bien que les politiques de prévention des intrusions de centre de gestionsoient uniques, le système applique la version Snort 2 ou Snort 3 d’une politique de prévention des intrusions pour la protection contre les intrusions en fonction du moteur d’inspection sélectionné du périphérique.
- Règles de décodeur : les règles de décodeur de paquets se déclenchent uniquement dans la politique de prévention des intrusions par défaut. Le système ignore les règles de décodeur que vous activez dans d’autres politiques.
- Règles d’objet partagé : Snort 3 prend en charge certaines des règles de prévention des intrusions d’objet partagé (SO), mais pas toutes (règles avec un ID de générateur (GID) égal à 3). Les règles d’objet partagé activées qui ne sont pas prises en charge ne se déclenchent pas.
- Inspection multicouche pour les renseignements sur la sécurité – Snort 3 détecte l’adresse IP la plus à l’intérieur, quelle que soit la couche.
- Prise en charge des plateformes : Snort 3 nécessite Threat Defense 7.0 ou une version ultérieure. Elle n’est pas prise en charge par ASA FirePOWER ou NGIPSv.
- Périphériques gérés : un centre de gestionThreat Defenseavec la version 7.0 peut prendre en charge simultanément les versions 6.4, 6.5, 6.6, 6.7 et 7.0 de Snort 2 et la version 7.0 de Snort 3 Threat Defense.
- Interruption de trafic lors du changement de version Snort : le changement de version Snort interrompt l’inspection du trafic et quelques paquets peuvent être abandonnés pendant le déploiement.
- Politiques unifiées : quelle que soit la version du moteur Snort sous-jacent qui est activée dans les Threat Defense gérés, les politiques de contrôle d’accès, les politiques de prévention des intrusions et les politiques d’analyse de réseau configurées dans les centre de gestion fonctionnent de manière transparente lors de l’application des politiques. Toutes les politiques de prévention des intrusions dans les versions 7.0 et ultérieures de centre de gestion comportent deux versions, la version Snort 2 et la version Snort 3. La politique de prévention des intrusions est unifiée, ce qui signifie qu’elle a un nom, une politique de base et un mode d’inspection communs, bien qu’il existe deux versions de la politique (version Snort 2 et version Snort 3). Les versions Snort 2 et Snort 3 de la politique de prévention des intrusions peuvent être différentes en termes de paramètres de règles. Cependant, lorsque la politique de prévention des intrusions est appliquée à un périphérique, le système identifie automatiquement la version Snort activée sur le périphérique et applique les paramètres de règle configurés pour cette version.
- Lightweight Security Package (LSP) (Paquet de sécurité léger) : remplace les mises à jour des règles Snort (SRU) par les mises à jour des règles de prévention des intrusions et de configuration de nouvelle

génération de Snort 3. Le téléchargement de mises à jour télécharge à la fois le LSP Snort 3 et la SRU Snort 2.

Les mises à jour LSP fournissent des règles de prévention des intrusions et des règles d'inspecteurs nouvelles et mises à jour, des états modifiés pour les règles existantes et des paramètres de politique de prévention des intrusions par défaut modifiés pour centre de gestion et Threat Defense version 7.0 ou supérieure. Lorsque vous mettez à niveau un centre de gestion de la version 6.7 ou antérieure à la version 7.0, il prend en charge les LSP et les SRU. Les mises à jour de règles peuvent également supprimer des règles, fournir de nouvelles catégories de règles et variables par défaut, et modifier les valeurs des variables par défaut. Pour en savoir plus sur les mises à jour des LSP, consultez la rubrique *Mettre à jour les règles de prévention des intrusions* dans la dernière version du *Guide de configuration du centre de gestion Cisco Firepower Management Center*.

- Mappage des règles et des présélections Snort 2 et Snort 3 : les règles Snort 2 et Snort 3 sont mappées et le mappage est fourni par le système. Cependant, il ne s'agit pas d'un mappage un à un. Les politiques de base en matière de prévention des intrusions fournies par le système sont préconfigurées pour Snort 2 et Snort 3 et fournissent la même prévention des intrusions, bien qu'avec des ensembles de règles différents. Les politiques de base fournies par le système pour Snort 2 et Snort 3 sont mappées entre elles pour les mêmes paramètres de prévention des intrusions.Pour plus de renseignements, consultez Afficher le mappage de politique de base Snort 2 et Snort 3.
- Annulation des règles de remplacement Snort 2 et Snort 3 : lorsqu'un Threat Defense est mis à niveau vers la version 7.0, vous pouvez mettre à niveau la plateforme d'inspection de Threat Defense vers la version Snort 3. Centre de gestion met en correspondance tous les remplacements dans les règles existantes de la version Snort 2 des politiques de prévention des intrusions avec les règles Snort 3 correspondantes en utilisant le mappage fourni par Talos. Cependant, si des remplacements supplémentaires sont effectués après la mise à niveau ou si vous avez installé un nouveau Threat Defense à la version 7.0, ils doivent être synchronisés manuellement. Pour en savoir plus, consultez Synchroniser les règles de Snort 2 avec celles de Snort 3.
- Règles de prévention des intrusions personnalisées : vous pouvez créer des règles de prévention des intrusions personnalisées dans Snort 3. Vous pouvez également importer les règles de prévention des intrusions personnalisées qui existent pour Snort 2 dans Snort 3. Pour en savoir plus, consultez Règles personnalisées dans Snort 3.
- Groupes de règles : centre de gestion regroupe toutes les règles de Snort 3 en groupes de règles. Les groupes de règles sont des groupes logiques de règles qui fournissent une interface de gestion simple pour améliorer l'accessibilité des règles, la navigation dans les règles et un meilleur contrôle sur le niveau de sécurité des groupes de règles.

  À partir de centre de gestion 7.3.0, la navigation par les règles est prise en charge pour plusieurs niveaux de groupes de règles, ce qui offre plus de flexibilité et un ensemble logique des règles. Le cadre MITRE est ajouté et vous permet de naviguer dans les règles à l'aide du cadre MITRE. MITRE n'est qu'une autre catégorie de groupes de règles et fait partie des groupes de règles Talos.

Remarque Consultez https://attack.mitre.org pour obtenir des renseignements sur MITRE.

Une règle peut faire partie de plusieurs groupes de règles, p. ex., plusieurs groupes de règles MITRE ATT&CK, un groupe de règles de catégorie de règles, plusieurs groupes de règles de « type de ressource », une campagne contre des programmes malveillants, etc. Les groupes de règles disponibles sont répertoriés dans l'éditeur de politiques de prévention des intrusions et peuvent être sélectionnés pour améliorer les politiques.

Grâce à cette structure hiérarchique à plusieurs niveaux, vous pouvez parcourir jusqu'au dernier élément, qui est le « groupe de règles descendant ». Ces groupes de règles contiennent des ensembles de règles liées les unes aux autres, comme un type de vulnérabilité spécifique, un système cible similaire ou une catégorie de menace similaire. Les groupes de règles sont associés à quatre niveaux de sécurité. Vous pouvez modifier le niveau de sécurité, ajouter ou supprimer des groupes de règles, et vous pouvez modifier l'action découlant d'une règle pour les règles qui correspondent au trafic observé sur le réseau. Cela est fait pour apporter un équilibre satisfaisant entre la sécurité, les performances et la résistance aux faux positifs.

Pour modifier une politique de prévention des intrusions Snort 3, consultez Modification des politiques de prévention des intrusions Snort 3.

Pour les rapports de groupes de règles dans les incidents d'intrusion, consultez Rapport de groupe de règles.

- Commutation entre les moteurs Snort 2 et Snort 3 : les Threat Defense qui prennent en charge Snort 3 peuvent également prendre en charge Snort 2. Le passage de Snort 3 à Snort 2 n'est pas recommandé du point de vue de l'efficacité.

Important Bien que vous puissiez changer de version Snort librement, les modifications de règles de prévention des intrusions dans une version de Snort ne seront pas mises à jour automatiquement dans l'autre version. Si vous modifiez l'action de règle pour une règle d'une version Snort, assurez-vous de reproduire la modification dans l'autre version avant de changer de version Snort. L'option de synchronisation fournie par le système synchronise uniquement les modifications de la version Snort 2 de la politique de prévention des intrusions avec la version Snort 3, et non l'inverse.

Lignes directrices et limites relatives aux politiques d'analyse de réseau et de prévention des intrusions

- Un pourcentage élevé de trafic composé de petits paquets diminue les performances de Snort. Ce comportement est observé même lorsque tous les préprocesseurs sont désactivés.
- Lorsque vous tentez de déployer une modification de configuration sur un périphérique Threat Defense avec une mémoire faible, le déploiement de Snort est également déclenché. Il en résulte une utilisation élevée de la mémoire RSS. L'utilisation de la mémoire Snort est également affectée si vous déployez des configurations importantes sur le périphérique, telles que plusieurs politiques IPS contenant un grand nombre de règles IPS Snort, d'objets de réseau et de listes de contrôle d'accès. Vous pouvez atténuer ces problèmes de mémoire en optimisant la configuration. Pour connaître les bonnes pratiques en matière de configuration des règles de contrôle d'accès afin d'optimiser la configuration, consultez Bonnes pratiques pour les règles de contrôle d'accès.
- Si vous augmentez la mémoire d'une instance Threat Defense Virtual, vous devez redéployer la configuration pour Snort 3 afin d'utiliser la mémoire supplémentaire.

Remarque L'allocation de mémoire Snort 3 n'est pas automatiquement ajustée lorsque vous augmentez la mémoire de l'instance Threat Defense Virtual. Vous devez redéployer la configuration pour régénérer les fichiers de configuration pertinents, tels que `memory_allocation.lua`, qui appliquent les limites de ressources mises à jour à Snort 3.

Limites de la fonctionnalité Snort 3 pour Threat Defense géré par Centre de gestion

Le tableau suivant répertorie les fonctions prises en charge sur Snort 2 mais non sur Snort 3 pour les périphériques Threat Defense gérés par centre de gestion.

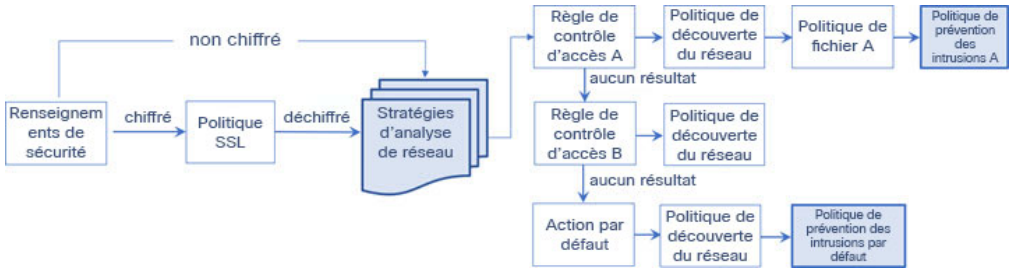
Tableau 1 : Limites des fonctionnalités de Snort 3

Politique/domaine	Fonctionnalités non prises en charge
Politique de contrôle d'accès	Les paramètres de l'application suivants : • Recherche sécuritaire • YouTube EDU
Politique de prévention des intrusions	• Seuil de règle globale • Configuration de la journalisation : • SNMP • Mises à jour des règles SRU car Snort 3 prend uniquement en charge les mises à jour des règles LSP
Autres fonctionnalités	Journalisation des événements avec noms de domaines complets

Comment les politiques examinent le trafic à la recherche d'intrusions

Lorsque le système analyse le trafic dans le cadre de votre déploiement de contrôle d'accès, la phase d'analyse de réseau (décodage et prétraitement) se produit avant et séparément de la phase de prévention des intrusions (règles de prévention des intrusions et paramètres avancés).

Le diagramme suivant montre, de manière simplifiée, l'ordre d'analyse du trafic dans un déploiement en ligne de la prévention des intrusions et d'AMP for Networks. Il montre comment la politique de contrôle d'accès fait appel à d'autres politiques pour examiner le trafic et dans quel ordre ces politiques sont appelées. Les phases d'analyse de réseau et de sélection de la politique de prévention des intrusions sont mises en surbrillance.



Dans un déploiement en ligne (c'est-à-dire lorsque les configurations pertinentes sont déployées sur des périphériques utilisant des interfaces routées, commutées ou transparentes, ou des paires d'interfaces en ligne), le système peut bloquer le trafic sans autre inspection, à presque toutes les étapes du processus illustré. La solution Security Intelligence, la politique SSL, les politiques d'analyse de réseau, les politiques de fichiers et les politiques de prévention des intrusions peuvent toutes supprimer ou modifier le trafic. Seule la politique de découverte de réseau, qui inspecte passivement les paquets, ne peut pas affecter le flux de trafic.

De même, à chaque étape du processus, un paquet peut entraîner la génération d'un événement par le système. Les intrusions et les événements de préprocesseur (parfois appelés collectivement *incidents d'intrusion*) sont des indications qu'un paquet ou son contenu peuvent présenter un risque pour la sécurité.

Astuces Le diagramme ne reflète pas le fait que les règles de contrôle d'accès traitent le trafic chiffré lorsque votre configuration d'inspection SSL le laisse passer, ou si vous ne configurez pas l'inspection SSL. Par défaut, le système désactive la prévention des intrusions et l'inspection des fichiers des charges utiles chiffrées. Cela permet de réduire les faux positifs et d'améliorer les performances lorsqu'une connexion chiffrée correspond à une règle de contrôle d'accès qui a configuré l'inspection des intrusions et des fichiers.

Notez que pour une connexion unique, bien que le système sélectionne une politique d'analyse de réseau avant une règle de contrôle d'accès comme le montre le diagramme, un certain prétraitement (notamment un prétraitement de la couche applicative) a lieu après la sélection de la règle de contrôle d'accès. Cela n'affecte **pas** la façon dont vous configurez le prétraitement dans les politiques d'analyse de réseau personnalisées.

Décodage, normalisation et prétraitement : politiques d'analyse de réseau

Sans décodage et prétraitement, le système ne pourrait pas évaluer correctement le trafic pour détecter les intrusions, car les différences de protocole rendraient impossible la mise en correspondance de modèles. Les politiques d'analyse de réseau régissent ces tâches de gestion du trafic :

- une **fois** le trafic filtré par Security Intelligence
- une **fois** le trafic chiffré déchiffré par une politique SSL facultative
- **avant que** le trafic puisse être inspecté par des politiques de fichiers ou de prévention des intrusions

Une politique d'analyse de réseau régit le traitement des paquets par phases. Tout d'abord, le système décode les paquets qui passent par les trois premières couches TCP/IP, puis poursuit la normalisation, le prétraitement et la détection des anomalies de protocole :

- Le décodeur de paquets convertit les en-têtes de paquets et les charges utiles dans un format qui peut être facilement utilisé par les inspecteurs et, ultérieurement, par les règles de prévention des intrusions. Chaque couche de la pile TCP/IP est décodée tour à tour, en commençant par la couche de liaison de

données jusqu'aux couches de réseau et de transport. Le décodeur de paquets détecte également divers comportements anormaux dans les en-têtes de paquets.

- Dans les déploiements en ligne, le préprocesseur de normalisation en ligne formate (normalise) le trafic pour minimiser les risques que les attaquants échappant à la détection. Il prépare les paquets pour l'examen par d'autres inspecteurs et prépare les règles de prévention des intrusions, et veille à ce que les paquets traités par le système soient les mêmes que les paquets reçus par les hôtes de votre réseau.
- Divers inspecteurs des couches de réseau et de transport détectent les attaques qui exploitent la fragmentation IP, effectuent la validation de la somme de contrôle et le prétraitement de la session TCP et UDP.

  Notez que certains paramètres avancés de transport et de réseau de l'inspecteur s'appliquent globalement à tout le trafic géré par les périphériques cibles d'une politique de contrôle d'accès. Vous les configurez dans la politique de contrôle d'accès plutôt que dans une politique d'analyse de réseau.
- Divers décodeurs de protocole de la couche d'application normalisent des types spécifiques de données de paquets dans des formats que le moteur de règles de prévention des intrusions peut analyser. La normalisation des codages de protocoles de la couche d'application permet au système d'appliquer efficacement les mêmes règles de prévention des intrusions liées au contenu aux paquets dont les données sont présentées différemment et d'obtenir des résultats significatifs.
- Les inspecteurs Modbus, DNP3, CIP et SCADA s7commplus détectent les anomalies de trafic et fournissent des données aux règles de prévention des intrusions. Les protocoles de supervision, de contrôle et d'acquisition de données (SCADA) surveillent, contrôlent et acquièrent des données des processus industriels, des processus d'infrastructure et d'installation tels que la fabrication, la production, le traitement de l'eau, la distribution d'énergie électrique, les systèmes aéroportuaires et d'expédition, et ainsi de suite.
- Plusieurs inspecteurs vous permettent de détecter des menaces spécifiques, comme l'ouverture arrière, les analyses de ports, les inondations SYN et d'autres attaques basées sur le débit.

  Notez que vous configurez l'inspecteur de données sensibles, qui détecte les données sensibles telles que les numéros de carte de crédit et les numéros de sécurité sociale en texte ASCII, dans les politiques de prévention des intrusions.

Remarque Lorsque l'identité du serveur TLS est désactivée, Snort 3 n'effectue pas de détection de non-concordance SNI. Il évalue uniquement le SNI dans le paquet Client Hello et contourne la validation du nom commun (CN) du certificat dans le paquet Server Hello.

Dans une politique de contrôle d'accès nouvellement créée, une politique d'analyse de réseau par défaut régit le prétraitement de *tout* le trafic pour *toutes* les politiques de prévention des intrusions appelées par la même politique parente de contrôle d'accès. Au départ, le système utilise la politique d'analyse de réseau Sécurité et connectivité équilibrées par défaut, mais vous pouvez la remplacer par une autre politique d'analyse de réseau fournie par le système ou personnalisée. Dans un déploiement plus complexe, les utilisateurs avancés peuvent adapter les options de prétraitement du trafic à des zones de sécurité, à des réseaux et à des VLAN spécifiques en attribuant différentes politiques d'analyse de réseau personnalisées pour prétraiter le trafic correspondant.

Remarque Pour une stratégie de contrôle d'accès avec une action découlant d'une règle définie sur **Trust** et une règle de préfiltre avec une action définie sur **Fastpath** avec les options de journalisation désactivées, vous remarquerez que les événements de fin de flux sont toujours générés dans le système. Les événements ne sont pas visibles sur les pages des événements du centre de gestion.

Règles de contrôle d'accès : sélection de la politique de prévention des intrusions

Après le prétraitement initial, les règles de contrôle d'accès (le cas échéant) évaluent le trafic. Dans la plupart des cas, la première règle de contrôle d'accès à laquelle un paquet correspond est la règle qui gère ce trafic; vous pouvez surveiller, faire confiance, bloquer ou autoriser le trafic correspondant.

Lorsque vous autorisez le trafic avec une règle de contrôle d'accès, le système peut inspecter le trafic à la recherche de données de découverte, de programmes malveillants, de fichiers interdits et d'intrusions, dans cet ordre. Le trafic ne correspondant à aucune règle de contrôle d'accès est géré par l'action par défaut de la politique de contrôle d'accès, qui peut également inspecter les données de découverte et les intrusions.

Remarque Tous les paquets, **quelle que soit** la politique d'analyse de réseau qui les prétraite, correspondent aux règles de contrôle d'accès configurées et sont donc potentiellement sujets à une inspection par les politiques de prévention des intrusions, dans l'ordre descendant.

Le diagramme en Comment les politiques examinent le trafic à la recherche d'intrusions, à la page 6 montre le flux du trafic dans un périphérique dans un déploiement en ligne de la prévention des intrusions et de AMP for Networks, comme suit :

- La règle de contrôle d'accès A permet au trafic correspondant de se poursuivre. La politique de découverte du réseau inspecte ensuite le trafic pour identifier des données de découverte, afin de détecter les fichiers interdits et les programmes malveillants par la politique A de fichiers, puis les intrusions sont repérées par la politique de prévention des intrusions A.
- La règle de contrôle d'accès B permet également de mettre en correspondance le trafic. Cependant, dans ce scénario, le trafic n'est pas inspecté pour détecter les intrusions (ou les fichiers ou les programmes malveillants), donc aucune politique de prévention des intrusions ou de fichier n'est associée à la règle. Notez que par défaut, le trafic que vous autorisez la poursuite est inspecté par la politique de découverte de réseau; vous n'avez pas besoin de configurer cela.
- Dans ce scénario, l'action par défaut de la politique de contrôle d'accès permet une mise en correspondance du trafic. Le trafic est ensuite inspecté par la politique de découverte de réseau, puis par une politique de prévention des intrusions. Vous pouvez (sans y être obligé) utiliser une politique de prévention des intrusions différente lorsque vous associez des politiques de prévention des intrusions aux règles de contrôle d'accès ou à l'action par défaut.

L'exemple du diagramme n'inclut aucune règle de blocage ou d'approbation, car le système n'inspecte pas le trafic bloqué ou de confiance.

Inspection d'intrusion : politiques, règles et ensembles de variables de prévention d'intrusion

De même, vous pouvez utiliser une politique IPS comme dernière ligne de défense du système avant que le trafic ne soit autorisé à se rendre à destination. Les politiques d'intrusion régissent la manière dont le système inspecte le trafic à la recherche de violations de la sécurité et, dans les déploiements en ligne, peuvent bloquer ou modifier le trafic malveillant. La fonction principale des politiques de prévention des intrusions est de gérer les règles de prévention des intrusions et de préprocesseur activées et la façon dont elles sont configurées.

Règles de prévention des intrusions et de l'inspecteur

Une règle de prévention des intrusions est un ensemble précis de mots-clés et d'arguments qui détectent les tentatives d'exploitation des vulnérabilités de votre réseau. le système utilise une règle de prévention des intrusions pour analyser le trafic réseau et vérifier s'il correspond aux critères de la règle. Le système compare les paquets aux conditions spécifiées dans chaque règle et, si les données du paquet correspondent à toutes les conditions spécifiées dans une règle, la règle se déclenche.

Le système comprend les types de règles suivants, créées par Cisco Talos Intelligence Group (Talos) :

- *les règles de prévention des intrusions d'objets partagés*, qui sont compilées et ne peuvent pas être modifiées (à l'exception des informations d'en-tête de règle telles que les ports source et de destination et les adresses IP)
- *les règles de prévention des intrusions en texte standard*, qui peuvent être enregistrées et modifiées en tant que nouvelles instances personnalisées de la règle.
- *les règles de préprocesseur*, qui sont des règles associées aux inspecteurs et aux options de détection des décodeurs de paquets dans la politique d'analyse de réseau. Vous ne pouvez pas copier ou modifier les règles de l'inspecteur. La plupart des règles de l'inspecteur sont désactivées par défaut; vous devez leur permettre d'utiliser les inspecteurs pour générer des événements et, dans un déploiement en ligne, abandonner les paquets fautifs.

Lorsque le système traite les paquets conformément à une politique de prévention des intrusions, un optimiseur de règles classe d'abord toutes les règles activées en sous-ensembles en fonction de critères tels que la couche de transport, le protocole d'application, la direction vers ou à partir du réseau protégé, etc. Ensuite, le moteur de règles de prévention des intrusions sélectionne les sous-ensembles de règles appropriés à appliquer à chaque paquet. Enfin, un moteur de recherche à règles multiples effectue trois types de recherches différents pour déterminer si le trafic correspond à la règle :

- La recherche de champ de protocole recherche les correspondances dans des champs particuliers d'un protocole d'application.
- La recherche de contenu générique recherche les correspondances d'octets ASCII ou binaires dans les données utiles du paquet.
- La recherche d'anomalies de paquet recherche les en-têtes de paquet et les charges utiles qui, plutôt que de contenir un contenu spécifique, enfreignent des protocoles bien établis.

Dans une politique de prévention des intrusions personnalisée, vous pouvez ajuster la détection en activant et en désactivant les règles, ainsi qu'en écrivant et en ajoutant vos propres règles de texte standard. Vous pouvez également utiliser les recommandations de Cisco pour associer les systèmes d'exploitation, les serveurs et les protocoles d'applications clientes détectés sur votre réseau à des règles spécifiquement écrites pour protéger ces ressources.

Remarque Lorsqu'il y a suffisamment de paquets pour traiter un trafic spécifique selon une règle de blocage, le système continue d'évaluer le trafic restant en fonction d'autres règles. Si du trafic restant correspond à une règle définie pour bloquer, la session est bloquée. Cependant, si le système analyse le trafic restant à transmettre, l'état du trafic indique en attente pour la règle qui est bloquée faute de paquets complets.

Ensembles de variables

Chaque fois que le système utilise une politique de prévention des intrusions pour évaluer le trafic, il utilise un *ensemble de variables* associé. La plupart des variables d'un ensemble représentent des valeurs couramment utilisées dans les règles d'intrusion pour identifier les adresses IP et les ports source et destination. Vous pouvez également utiliser des variables dans les politiques de prévention des intrusions pour représenter les adresses IP dans les états de suppressions de règles et de règles dynamiques.

Le système fournit un seul ensemble de variables par défaut, qui comprend des variables par défaut prédéfinies. La plupart des règles d'objet partagé et des règles de texte standard fournies par le système utilisent ces variables par défaut prédéfinies pour définir les réseaux et les numéros de port. Par exemple, la majorité des règles utilisent la variable `$HOME_NET` pour préciser le réseau protégé et la variable `$EXTERNAL_NET`pour préciser le réseau non protégé (ou externe). En outre, les règles spécialisées utilisent souvent d'autres variables prédéfinies. Par exemple, les règles qui détectent les exploits contre les serveurs Web utilisent les variables `$HTTP_SERVERS` et `$HTTP_PORTS`.

Astuces Même si vous utilisez les politiques de prévention des intrusions fournies par le système, Cisco vous recommande **fortement** de modifier les variables clés par défaut de l'ensemble par défaut. Lorsque vous utilisez des variables qui reflètent avec précision votre environnement réseau, le traitement est optimisé et le système peut surveiller les systèmes concernés pour détecter toute activité suspecte. Les utilisateurs avancés peuvent créer et utiliser des ensembles de variables personnalisés pour les jumeler avec une ou plusieurs politiques de prévention des intrusions personnalisées.

Important Si vous créez un ensemble de variables personnalisé, n'utilisez pas de chiffre comme premier caractère dans le nom d'un ensemble de variables personnalisées (par exemple, 3Snort). Cela entraînera l'échec de la validation du Snort 3 lorsque vous déployez une configuration sur le pare-feu Threat Defense sur centre de gestion.

Génération d'incidents d'intrusion

Lorsque le système détecte une intrusion possible, il génère un événement d' *intrusion ou de préprocesseur* (parfois appelés collectivement *incidents d'intrusion*). Les périphériques gérés transmettent leurs événements à centre de gestion, où vous pouvez afficher les données agrégées et acquérir une meilleure compréhension des attaques contre les ressources de votre réseau. Dans un déploiement en ligne, les périphériques gérés peuvent également abandonner ou remplacer des paquets que vous savez être dangereux.

Chaque incident d'intrusion dans la base de données comprend un en-tête d'événement et contient des informations sur le nom et la classification de l'événement; les adresses IP de source et de destination; les ports; le processus qui a généré l'événement; et la date et l'heure de l'événement, ainsi que des informations contextuelles sur la source de l'attaque et sa cible. Pour les événements par paquets, le système enregistre

également une copie de l'en-tête du paquet décodé et de la charge utile du ou des paquets qui ont déclenché l'événement.

Le décodeur de paquets, les préprocesseurs et le moteur de règles de prévention des intrusions peuvent tous forcer le système à générer un événement. Par exemple :

- Si le décodeur de paquets (configuré dans la politique d'analyse de réseau) reçoit un paquet IP de moins de 20 octets, soit la taille d'un datagramme IP sans option ni charge utile, le décodeur interprète cela comme un trafic anormal. Si, ultérieurement, la règle de décodeur associée dans la politique de prévention des intrusions qui examine le paquet est activée, le système génère un événement d'inspection.
- Si le préprocesseur de défragmentation IP rencontre une série de fragments IP qui se chevauchent, l'inspecteur interprète cela comme une attaque possible et, lorsque la règle d'inspecteur associée est activée, le système génère un événement d'inspecteur.
- Dans le moteur de règles de prévention des intrusions, la plupart des règles de texte standard et des règles d'objets partagés sont écrites de manière à générer des incidents d'intrusion lorsqu'elles sont déclenchées par des paquets.

Au fur et à mesure que la base de données accumule les incidents d'intrusion, vous pouvez commencer votre analyse des attaques potentielles. Le système vous fournit les outils dont vous avez besoin pour passer en revue les incidents d'intrusion et évaluer s'ils sont importants dans le contexte de votre environnement réseau et de vos politiques de sécurité.

Politiques d'analyse de réseau et de prévention des intrusions fournies par le système et personnalisées

La création d'une nouvelle politique de contrôle d'accès est l'une des premières étapes de la gestion du flux de trafic à l'aide du système. Par défaut, une politique de contrôle d'accès nouvellement créée fait appel aux politiques d'analyse de réseau et de prévention des intrusions fournies par le système pour examiner le trafic.

Le diagramme suivant montre comment une nouvelle politique de contrôle d'accès dans un déploiement de prévention des intrusions en ligne gère initialement le trafic. Les phases de prétraitement et de prévention des intrusions sont mises en surbrillance.

Remarquez comment :

- Une politique d'analyse de réseau par défaut régit le prétraitement de *tout* le trafic géré par la politique de contrôle d'accès. Au départ, la *politique d'analyse du réseau de sécurité et de connectivité équilibrée* fournie par le système est la politique par défaut.
- L'action par défaut de la politique de contrôle d'accès autorise tout le trafic non malveillant, comme déterminé par la *politique de prévention des intrusions, de sécurité et connectivité équilibrées* fournie par le système. Comme l'action par défaut laisse passer le trafic, la fonction de découverte peut l'examiner à la recherche de données relatives à l'hôte, à l'application et à l'utilisateur avant que la politique de prévention des intrusions ne puisse examiner et éventuellement bloquer le trafic malveillant.
- La politique utilise les options Security Intelligence par défaut (listes globales de blocage et Ne pas bloquer uniquement), ne déchiffre pas le trafic chiffré avec une politique SSL et n'effectue pas de traitement spécial ni d'inspection du trafic réseau à l'aide des règles de contrôle d'accès.

Une mesure simple à prendre pour optimiser le déploiement de la prévention des intrusions consiste à utiliser par défaut un ensemble différent de politiques d'analyse du réseau et de prévention des intrusions fournies par le système. Cisco fournit plusieurs paires de ces politiques avec le système.

Vous pouvez aussi adapter votre déploiement de prévention des intrusions en créant et en utilisant des politiques personnalisées. Vous constaterez peut-être que les options de l'inspecteur, la règle de prévention des intrusions et d'autres paramètres avancés configurés dans ces politiques ne répondent pas aux besoins de sécurité de votre réseau. En ajustant vos politiques d'analyse de réseau et de prévention des intrusions, vous pouvez configurer, à un niveau très fin, la façon dont le système traite et inspecte le trafic sur votre réseau pour détecter les intrusions.

Politiques d'analyse de réseau et de prévention des intrusions fournies par le système et personnalisées

Cisco fournit les politiques d'analyse de réseau et de prévention des intrusions suivantes avec le système : En utilisant les politiques d'analyse de réseau et de prévention des intrusions fournies par le système, vous pouvez profiter de l'expérience de Cisco Talos Intelligence Group (Talos). Pour ces politiques, Talos fournit des états des règles de prévention des intrusions et d'inspecteur, ainsi que des configurations initiales pour les inspecteurs et d'autres paramètres avancés.

Aucune politique fournie par le système ne couvre tous les profils de réseau, toutes les combinaisons de trafic ou toutes les postures défensives. Chacune couvre des cas et des configurations réseau courants qui fournissent un point de départ pour une politique défensive bien réglée. Bien que vous puissiez utiliser les politiques fournies par le système telles quelles, Cisco vous recommande fortement de les utiliser comme base pour des politiques personnalisées que vous ajusterez en fonction de votre réseau.

Astuces Même si vous utilisez les politiques d'analyse de réseau et de prévention des intrusions fournies par le système, vous devez configurer les variables de prévention des intrusions du système pour refléter avec précision votre environnement réseau. Modifiez au minimum les variables par défaut clés dans l'ensemble par défaut.

À mesure que de nouvelles vulnérabilités sont connues, Talos publie des mises à jour des règles de prévention des intrusions, également appelées *Paquet léger de sécurité* (LSP). Ces mises à jour de règles peuvent modifier toute analyse de réseau ou politique de prévention des intrusions fournie par le système, ainsi que des règles de prévention des intrusions et d'inspecteur nouvelles ou mises à jour, des états modifiés pour les règles existantes et des paramètres de politique par défaut modifiés. Les mises à jour de règles peuvent également supprimer des règles des politiques fournies par le système et fournir de nouvelles catégories de règles, ainsi que modifier l'ensemble de variables par défaut.

Si la mise à jour d'une règle affecte votre déploiement, l'interface Web marque comme obsolètes les politiques d'analyse de réseau et de prévention des intrusions affectées, ainsi que leurs politiques parentes de contrôle d'accès. Vous devez redéployer une politique mise à jour pour que ses modifications prennent effet.

Pour plus de commodité, vous pouvez configurer des mises à jour de règles pour qu'elles redéploient automatiquement les politiques de prévention des intrusions touchées, seules ou en combinaison avec les politiques de contrôle d'accès concernées. Cela vous permet de garder facilement et automatiquement votre déploiement à jour pour vous protéger contre les intrusions et les exploits découverts récemment.

Pour garantir la mise à jour des paramètres de prétraitement, vous **devez** redéployer les politiques de contrôle d'accès, qui déploient également tout SSL associé, ainsi que les politiques d'analyse de réseau et de fichiers différentes de celles en cours d'exécution, et peuvent également mettre à jour les valeurs par défaut pour le prétraitement avancé. et les options de performance.

Cisco fournit les politiques d'analyse de réseau et de prévention des intrusions suivantes avec le système :

Politiques d'analyse des intrusions et de sécurité et de connectivité équilibrées

Ces politiques sont conçues pour la vitesse et la détection. Utilisés ensemble, ils constituent un bon point de départ pour la plupart des organisations et des types de déploiement. Le système utilise les politiques et les paramètres de sécurité et de connectivité équilibrées par défaut dans la plupart des cas.

Politiques en matière d'analyse de réseau et de prévention des intrusions La connectivité avant la sécurité

Ces politiques sont conçues pour les organisations où la connectivité (permission d'accéder à toutes les ressources) prime sur la sécurité de l'infrastructure réseau. La politique de prévention des intrusions active beaucoup moins de règles que celles activées dans la politique de sécurité avant la connectivité. Seules les règles les plus critiques qui bloquent le trafic sont activées.

Politiques en matière d'analyse de réseau et de prévention des intrusions La connectivité avant la sécurité

Ces politiques sont conçues pour les entreprises où la sécurité de l'infrastructure réseau prime sur la commodité pour l'utilisateur. La politique de prévention des intrusions permet d'appliquer de nombreuses règles de prévention des anomalies du réseau qui peuvent alerter sur le trafic légitime ou l'interrompre.

Politiques d'analyse de réseau et de prévention des intrusions

Ces politiques sont conçues pour les organisations où la sécurité de l'infrastructure du réseau est encore plus importante que celle des politiques de sécurité sur la connectivité, avec un potentiel d'impact opérationnel encore plus grand. Par exemple, la politique de prévention des intrusions active des règles dans un grand nombre de catégories de menaces, y compris les programmes malveillants, les trousses d'exploit, les vulnérabilités anciennes et courantes, et les exploits connus et répandus.

Politique de prévention des intrusions Aucune règle active

Dans la politique de prévention des intrusions Aucune règle active, toutes les règles de prévention des intrusions et tous les paramètres avancés, à l'exception des seuils de règles de prévention des intrusions, sont désactivés. La présente politique fournit un point de départ si vous souhaitez créer votre propre politique de prévention des intrusions au lieu de la baser sur les règles activées dans l'une des autres politiques fournies par le système.

Remarque Selon la politique de base sélectionnée, fournie par le système, les paramètres de la politique varient. Pour afficher les paramètres de la politique, cliquez sur l'icône **Modifier** à côté de la politique, puis cliquez sur la liste déroulante **Base Policy** (politique de base).

Avantages de l'analyse personnalisée du réseau et des politiques de prévention des intrusions

Vous constaterez peut-être que les options de l'inspecteur, les règles de prévention des intrusions et d'autres paramètres avancés configurés dans les politiques d'analyse de réseau et de prévention des intrusions fournies par le système ne répondent pas entièrement aux besoins de sécurité de votre organisation.

L'élaboration de politiques personnalisées peut améliorer les performances du système dans votre environnement et fournir un aperçu précis du trafic malveillant et des violations de politiques qui se produisent sur votre réseau. La création et le réglage de politiques personnalisées vous permettent de configurer, à un niveau très fin, la façon dont le système traite et inspecte le trafic sur votre réseau pour détecter les intrusions.

Toutes les politiques personnalisées ont une politique de base, également appelée couche de base, qui définit les paramètres par défaut pour toutes les configurations de la politique. Une couche est un bloc de construction que vous pouvez utiliser pour gérer efficacement plusieurs politiques d'analyse de réseau ou de prévention des intrusions.

Dans la plupart des cas, vous fondez les politiques personnalisées sur les politiques fournies par le système, mais vous pouvez utiliser une autre politique personnalisée. Cependant, toutes les politiques personnalisées ont une politique fournie par le système comme base potentielle dans une chaîne de politiques. Étant donné que les mises à jour de règles peuvent modifier des politiques fournies par le système, l'importation d'une mise à jour de règle peut vous affecter même si vous utilisez une politique personnalisée comme base. Si la mise à jour d'une règle affecte votre déploiement, l'interface Web marque les politiques concernées comme obsolètes.

Avantages des politiques d'analyse de réseau personnalisées

Par défaut, une politique d'analyse de réseau prétraite tout le trafic non chiffré géré par la politique de contrôle d'accès. Cela signifie que tous les paquets sont décodés et prétraités en fonction des mêmes paramètres, quelle que soit la politique de prévention des intrusions (et, par conséquent, l'ensemble de règles de prévention des intrusions) qui les examinera ultérieurement.

Au départ, la politique d'analyse de réseau Sécurité et connectivité équilibrées fournie par le système est la politique par défaut. Un moyen simple de régler le prétraitement consiste à créer et à utiliser une politique d'analyse de réseau personnalisée par défaut.

Les options de réglage disponibles varient d'un inspecteur à l'autre, mais il est possible de régler les inspecteurs et les décodeurs de plusieurs façons :

- Vous pouvez désactiver les inspecteurs qui ne s'appliquent pas au trafic que vous surveillez. Par exemple, l'inspecteur HTTP Inspect normalise le trafic HTTP. Si vous êtes sûr que votre réseau n'inclut aucun serveur Web utilisant les services Internet Information Services (IIS de Microsoft), vous pouvez désactiver l'option de l'inspecteur qui recherche le trafic spécifique à IIS et ainsi réduire la surcharge de traitement du système.

Remarque Si vous désactivez un inspecteur dans une politique d'analyse de réseau personnalisée, mais que le système doit utiliser cet inspecteur pour évaluer ultérieurement les paquets par rapport à une règle de prévention des intrusions ou à une règle d'inspecteur activée, le système active et utilise automatiquement l'inspecteur, bien que l'inspecteur reste désactivé dans la politique d'analyse de réseau interface Web.

- Préciser les ports, le cas échéant, pour concentrer l'activité de certains inspecteurs. Par exemple, vous pouvez identifier des ports supplémentaires pour surveiller les réponses du serveur DNS ou les sessions SSL chiffrées, ou des ports sur lesquels vous décodez le trafic Telnet, HTTP et RPC.

Pour les utilisateurs avancés ayant des déploiements complexes, vous pouvez créer plusieurs politiques d'analyse du réseau, chacune étant conçue pour prétraiter le trafic différemment. Ensuite, vous pouvez configurer le système pour utiliser ces politiques et régir le prétraitement du trafic en utilisant différentes zones de sécurité, réseaux ou VLAN. (Notez que les modules ASA FirePOWER ne peuvent pas restreindre le prétraitement par VLAN.)

Remarque La personnalisation du prétraitement à l'aide de politiques d'analyse de réseau personnalisées, en particulier de plusieurs politiques d'analyse de réseau, est une tâche avancée. Le prétraitement et l'inspection de prévention des intrusions étant si étroitement liés, vous **devez** veiller à ne pas autoriser les politiques d'analyse de réseau et de prévention des intrusions examinant un seul paquet à se compléter.

Avantages des politiques de prévention des intrusions personnalisées

Dans une nouvelle politique de contrôle d'accès configurée initialement pour effectuer la prévention des intrusions, l'action par défaut autorise tout le trafic, mais en l'inspectant d'abord à l'aide de la politique de prévention des intrusions de sécurité et de connectivité équilibrées fournie par le système. À moins que vous ajoutiez des règles de contrôle d'accès ou changiez l'action par défaut, tout le trafic est inspecté par cette politique de prévention des intrusions.

Pour personnaliser votre déploiement de prévention des intrusions, vous pouvez créer plusieurs politiques à cet effet, chacune étant conçue pour inspecter le trafic différemment. Configurez ensuite une politique de contrôle d'accès avec des règles qui précisent quelle politique inspecte quel trafic. Les règles de contrôle d'accès peuvent être simples ou complexes : les correspondances et l'inspection du trafic se font en fonction de plusieurs critères, notamment la zone de sécurité, l'emplacement réseau ou géographique, le VLAN, le port, l'application, l'URL demandée ou l'utilisateur.

La principale fonction des politiques de prévention des intrusions est de gérer les règles de prévention des intrusions et d'inspection qui sont activées et la manière dont elles sont configurées, comme suit :

- Dans chaque politique de prévention des intrusions, vous devez vérifier que toutes les règles applicables à votre environnement sont activées et améliorer les performances en désactivant les règles qui ne sont pas applicables à ce dernier. Vous pouvez préciser les règles qui doivent abandonner ou modifier les paquets malveillants.
- Les recommandationsCisco vous permettent d'associer les systèmes d'exploitation, les serveurs et les protocoles d'applications clientes détectés sur votre réseau à des règles spécifiquement écrites pour protéger ces ressources.
- Vous pouvez modifier les règles existantes et écrire de nouvelles règles en texte standard au besoin pour détecter de nouveaux exploits ou appliquer vos politiques de sécurité.

Voici d'autres personnalisations que vous pourriez apporter à une politique de prévention des intrusions :

- Le préprocesseur des données sensibles détecte les données sensibles telles que les numéros de cartes de crédit et les numéros de sécurité sociale dans le texte ASCII. Notez que d'autres inspecteurs qui détectent des menaces spécifiques (attaques par orifice arrière, plusieurs types de balayage de ports et attaques basées sur le débit qui tentent de submerger votre réseau avec un trafic excessif) sont configurés dans les politiques d'analyse de réseau.
- Les seuils globaux obligent le système à générer des événements en fonction du nombre de fois que le trafic correspondant à une règle de prévention des intrusions provient d'une adresse ou d'une plage d'adresses spécifique au cours d'une période donnée ou est ciblé vers une adresse ou une plage d'adresses donnée. Cela permet d'éviter que le système ne soit submergé par un grand nombre d'événements.
- La suppression des notifications d'incidents d'intrusion et la définition de seuils pour des règles individuelles ou des politiques complètes de prévention des intrusions peuvent également éviter que le système ne soit submergé par un grand nombre d'événements.

- En plus des différents affichages des incidents d'intrusion dans l'interface Web, vous pouvez activer la journalisation dans les installations Syslog ou envoyer des données d'événements à un serveur de déroutement SNMP. Par politique, vous pouvez préciser les limites de notification d'incidents d'intrusion, configurer la notification d'incidents d'intrusion aux installations de journalisation externes et configurer les réponses externes aux incidents d'intrusion. Notez qu'en plus de ces configurations d'alertes par politique, vous pouvez activer ou désactiver globalement les alertes par courriel sur les incidents d'intrusion pour chaque règle ou groupe de règles. Les paramètres de vos alertes par courriel sont utilisés, quelles que soient la politique de prévention des intrusions qui traite un paquet.

Limites des politiques personnalisées

Le prétraitement et l'inspection de prévention des intrusions étant si étroitement liés, vous **devez** veiller à ce que votre configuration permette à l'analyse de réseau et à l'inspection de réseau, au traitement et à l'examen d'un seul paquet de se compléter.

Par défaut, le système utilise une politique d'analyse de réseau pour prétraiter tout le trafic géré par les périphériques gérés à l'aide d'une seule politique de contrôle d'accès. Le diagramme suivant montre comment une nouvelle politique de contrôle d'accès dans un déploiement de prévention des intrusions en ligne gère initialement le trafic. Les phases de prétraitement et de prévention des intrusions sont mises en surbrillance.

Remarquez comment une politique d'analyse de réseau par défaut régit le prétraitement de *tout* le trafic géré par la politique de contrôle d'accès. Au départ, la politique d'analyse de réseau Sécurité et connectivité équilibrées fournie par le système est la politique par défaut.

Un moyen simple de régler le prétraitement consiste à créer et à utiliser une politique d'analyse de réseau personnalisée par défaut. Toutefois, si vous désactivez un inspecteur dans une politique d'analyse de réseau personnalisée, mais que le système doit évaluer les paquets prétraités par rapport à une règle de prévention des intrusions ou d'inspecteur activée, le système active et utilise automatiquement l'inspecteur, même s'il reste désactivé dans l'interface Web de la politique d'analyse de réseau.

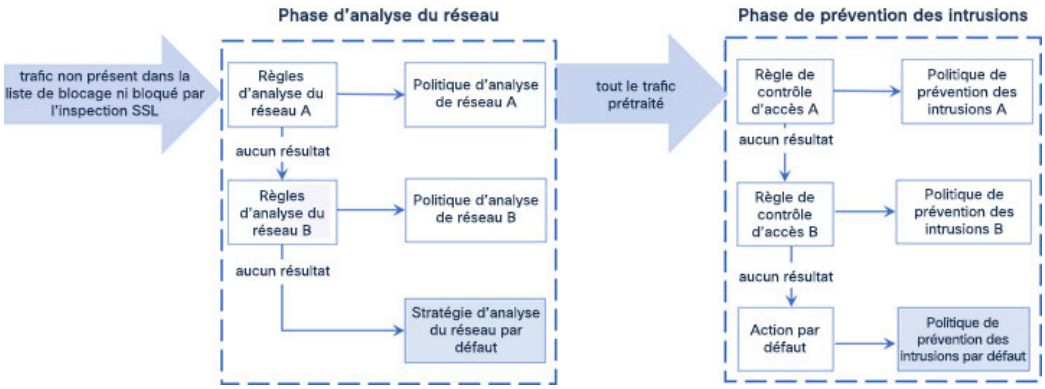
Remarque Afin de profiter des avantages liés à la désactivation d'un inspecteur en matière de performances, vous **devez** vous assurer qu'aucune de vos politiques de prévention des intrusions ne comporte de règles activées nécessitant cet inspecteur.

Un défi supplémentaire survient si vous utilisez plusieurs politiques d'analyse de réseau personnalisées. Pour les utilisateurs avancés avec des déploiements complexes, vous pouvez adapter le prétraitement à des zones de sécurité, à des réseaux et à des VLAN spécifiques en attribuant des politiques d'analyse de réseau personnalisées pour prétraiter le trafic correspondant. (Notez qu'ASA FirePOWER ne peut pas restreindre le prétraitement par VLAN.) Pour ce faire, ajoutez des *règles d'analyse de réseau* personnalisées à votre politique de contrôle d'accès. Chaque règle est associée à une politique d'analyse de réseau qui régit le prétraitement du trafic correspondant à la règle.

Astuces Vous configurez les règles d'analyse de réseau en tant que paramètre avancé dans une politique de contrôle d'accès. Contrairement à d'autres types de règles, les règles d'analyse de réseau font appel à des politiques d'analyse de réseau plutôt que d'être contenues par.

Le système fait correspondre les paquets à des règles d'analyse de réseau configurées en ordre descendant par numéro de règle. Le trafic qui ne correspond à aucune règle d'analyse de réseau est prétraité par la politique d'analyse de réseau par défaut. Bien que cela vous permette une grande souplesse dans le prétraitement du trafic, gardez à l'esprit que tous les paquets, **quelle que soit** la politique d'analyse de réseau qui les ont prétraités, sont par la suite mis en correspondance avec les règles de contrôle d'accès, et donc à l'inspection potentielle par les politiques de prévention des intrusions, dans leur propre processus. . En d'autres termes, le prétraitement d'un paquet avec une politique d'analyse de réseau particulière ne garantit **pas** que le paquet sera examiné avec une politique de prévention des intrusions particulière. Vous **devez** configurer avec soin votre politique de contrôle d'accès afin qu'elle fasse appel aux politiques d'analyse de réseau et de prévention des intrusions appropriées pour évaluer un paquet particulier.

Le diagramme suivant montre de manière très détaillée comment la phase de sélection de la politique d'analyse de réseau (prétraitement) se produit avant la phase de prévention des intrusions (règles) et séparément. Par souci de simplicité, le diagramme élimine les phases de découverte et d'inspection des fichiers et des programmes malveillants. Il met également en évidence les politiques d'analyse de réseau et d'action par défaut contre les intrusions par défaut.



Dans ce scénario, une politique de contrôle d'accès est configurée avec deux règles d'analyse de réseau et une politique d'analyse de réseau par défaut :

- La règle d'analyse de réseau A prétraite le trafic correspondant avec la politique d'analyse de réseau A. Vous souhaitez que ce trafic soit inspecté ultérieurement par la politique de prévention des intrusions A.
- La règle d'analyse de réseau B prétraite le trafic correspondant avec la politique d'analyse de réseau B. Vous souhaitez que ce trafic soit inspecté ultérieurement par la politique de prévention des intrusions B.
- Tout le trafic restant est prétraité avec la politique d'analyse de réseau par défaut. Plus tard, vous souhaitez que ce trafic soit inspecté par la politique de prévention des intrusions associée à l'action par défaut de la politique de contrôle d'accès.

Une fois que le système a prétraité le trafic, il peut examiner le trafic pour détecter des intrusions. Le diagramme montre une politique de contrôle d'accès avec deux règles de contrôle d'accès et une action par défaut :

- La règle de contrôle d'accès A permet la mise en correspondance du trafic. Le trafic est ensuite inspecté par la politique de prévention des intrusions A.
- La règle de contrôle d'accès B permet de mettre en correspondance le trafic. Le trafic est ensuite inspecté par la politique de prévention des intrusions B.
- L'action par défaut de la politique de contrôle d'accès permet une mise en correspondance du trafic. Le trafic est ensuite inspecté par la politique de prévention des intrusions de l'action par défaut.

Le traitement de chaque paquet est régi par une paire de politiques d'analyse de réseau et de politiques de prévention des intrusions, mais le système ne coordonne **pas** la paire pour vous. Voici un scénario dans lequel vous configurez mal votre politique de contrôle d'accès de sorte que la règle d'analyse de réseau A et la règle de contrôle d'accès A ne traitent pas le même trafic. Par exemple, vous pouvez vouloir que les politiques jumelées régissent le traitement du trafic sur une zone de sécurité particulière, mais vous utilisez par erreur des zones différentes dans les conditions des deux règles. Cela pourrait entraîner un prétraitement incorrect du trafic. Pour cette raison, la personnalisation du prétraitement à l'aide de règles d'analyse de réseau et de politiques personnalisées est une tâche **avancée**.

Veuillez noter que pour une connexion unique, bien que le système sélectionne une politique d'analyse de réseau avant une règle de contrôle d'accès, un certain prétraitement (notamment le prétraitement de la couche d'application) a lieu après la sélection de la règle de contrôle d'accès. Cela n'affecte **pas** la façon dont vous configurez le prétraitement dans les politiques d'analyse de réseau personnalisées.

Conditions préalables pour les politiques d'analyse de réseau et de prévention des intrusions

Pour permettre au moteur d'inspection Snort de traiter le trafic pour l'analyse des intrusions et des programmes malveillants, la licence IPS doit être activée pour le périphérique Threat Defense.

Vous devez être un utilisateur administrateur pour gérer l'analyse de réseau et les politiques de prévention des intrusions et effectuer les tâches de migration.

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.