Préprocesseurs de couche applicative

Les rubriques suivantes expliquent les préprocesseurs de la couche d'application et la façon de les configurer :

Introduction aux préprocesseurs de couche applicative

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Les protocoles de la couche d'application peuvent représenter les mêmes données de diverses manières. Le système Firepower fournit des décodeurs de protocole de la couche applicative qui normalisent des types spécifiques de paquets de données dans des formats que le moteur de règles de prévention des intrusions peut analyser. La normalisation des codages de protocole de la couche applicative permet au moteur de règles d'appliquer efficacement les mêmes règles liées au contenu aux paquets dont les données sont présentées différemment et d'obtenir des résultats significatifs.

Lorsqu'une règle de prévention des intrusions ou un arguments de règle nécessite un préprocesseur désactivé, le système l'utilise automatiquement avec sa configuration actuelle, même s'il reste désactivé dans l'interface Web de la politique d'analyse de réseau.

Notez que les préprocesseurs ne génèrent pas d'événements dans la plupart des cas, sauf si vous activez les règles de préprocesseur associées à une politique de prévention des intrusions.

Licences requises pour les préprocesseurs de la couche applicative

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables pour les préprocesseurs de la couche d'application

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'intrusion

Le préprocesseur DCE/RPC

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le protocole DCE/RPC permet aux processus se trouvant sur des hôtes réseau distincts de communiquer comme si les processus se trouvaient sur le même hôte. Ces communications interprocessus sont généralement transportées entre les hôtes sur TCP et UDP. Dans le transport TCP, DCE/RPC peut également être encapsulé dans le protocole SMB (Windows Server Message Block) ou SMB, une implémentation SMB à code source ouvert utilisée pour la communication interprocessus dans un environnement mixte Windows et UNIX ou des systèmes d'exploitation de type Linux. En outre, les serveurs Web Windows IIS de votre réseau peuvent

utiliser l'appel RPC IIS sur HTTP, qui fournit une communication distribuée par l'intermédiaire d'un pare-feu, pour constituer un proxy du trafic DCE/RPC transporté par TCP.

Notez que les descriptions des options et des fonctionnalités du préprocesseur DCE/RPC comprennent l'implémentation de Microsoft de DCE/RPC connue sous le nom de MSRPC; les descriptions des options et des fonctionnalités de SMB font référence à la fois à SMB et à Samba.

Bien que la plupart des exploits DCE/RPC se produisent dans les demandes des clients DCE/RPC ciblant les serveurs DCE/RPC, qui peuvent être pratiquement n'importe quel hôte de votre réseau qui exécute Windows ou Samba, des exploits peuvent également se produire dans les réponses des serveurs. Le préprocesseur DCE/RPC détecte les requêtes et les réponses DCE/RPC encapsulées dans des transports TCP, UDP et SMB, y compris DCE/RPC transporté par TCP à l'aide de la version 1 de l'appel RPC sur HTTP. Le préprocesseur analyse les flux de données DCE/RPC et détecte les comportements anormaux et les techniques de contournement dans le trafic DCE/RPC. Il analyse également les flux de données SMB et détecte le comportement anormal des SMB et les techniques de contournement.

Le préprocesseur DCE/RPC désegmente SMB et défragmente DCE/RPC en plus de la défragmentation IP fournie par le préprocesseur de défragmentation IP et le réassemblage de flux TCP assuré par le préprocesseur de flux TCP.

Enfin, le préprocesseur DCE/RPC normalise le trafic DCE/RPC pour le traitement par le moteur de règles.

Trafic DCE/RPC avec et sans connexion

Les messages DCE/RPC sont conformes à l'un des deux protocoles suivants : DCE/RPC Protocol Data Unit (PDU) :

protocole PDU DCE/RPC axé sur la connexion

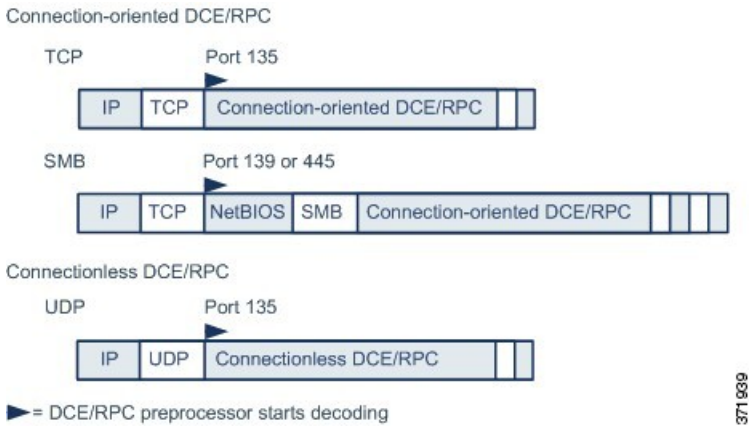
Le préprocesseur DCE/RPC détecte le DCE/RPC en mode connexion dans les transports TCP, SMB et RPC sur HTTP.

protocole PDU DCE/RPC sans connexion

Le préprocesseur DCE/RPC détecte le DCE/RPC sans connexion dans le transport UDP.

Les deux protocoles PDU DCE/RPC ont leurs propres en-têtes et caractéristiques de données. Par exemple, la longueur de l'en-tête DCE/RPC orienté connexion est généralement de 24 octets et la longueur d'en-tête DCE/RPC sans connexion est fixée à 80 octets. De plus, l'ordre correct des fragments d'un DCE/RPC fragmenté sans connexion ne peut pas être géré par un transport sans connexion et doit plutôt être garanti par des valeurs d'en-tête DCE/RPC sans connexion; en revanche, le protocole de transport garantit que l'ordre des fragments est correct pour l'ETCD ou l'RPC orienté connexion. Le préprocesseur DCE/RPC utilise ces caractéristiques et d'autres caractéristiques propres aux protocoles pour surveiller les anomalies et autres techniques de contournement des deux protocoles, et pour décoder et défragmenter le trafic avant de le transmettre au moteur de règles.

Le diagramme suivant illustre le moment où le préprocesseur DCE/RPC commence à traiter le trafic DCE/RPC pour les différents transports.



Notez les éléments suivants dans la figure :

- Le port TCP ou UDP bien connu 135 identifie le trafic DCE/RPC dans les transports TCP et UDP.
- La figure n'inclut pas l'appel RPC sur HTTP.

  Pour les appels RPC sur HTTP, le protocole ETCD/RPC orienté connexion est transporté directement sur TCP, comme le montre la figure, après une séquence de configuration initiale sur HTTP.
- Le préprocesseur DCE/RPC reçoit généralement le trafic SMB sur le port TCP bien connu 139 pour le service de session NetBIOS ou le port Windows bien connu 445 mis en œuvre de manière similaire.

  Étant donné que SMB remplit de nombreuses fonctions autres que le transport de DCE/RPC, le préprocesseur teste d'abord si le trafic SMB transporte du trafic DCE/RPC et arrête le traitement si ce n'est pas le cas ou poursuit le traitement dans le cas inverse.
- IP encapsule tous les transports DCE/RPC.
- TCP transporte tous les DCE/RPC en mode connexion.
- Le protocole UDP achemine ETCD/RPC sans connexion.

Politiques basées sur la cible DCE/RPC

Les implémentations de Windows et Samba DCE/RPC sont très différentes. Par exemple, toutes les versions de Windows utilisent l'ID de contexte DCE/RPC dans le premier fragment lors de la défragmentation du trafic DCE/RPC, et toutes les versions de Samba utilisent l'ID de contexte dans le dernier fragment. À titre d'autre exemple, Windows XP utilise le champ d'en-tête « opnum » (numéro d'opération) dans le premier fragment pour identifier un appel de fonction spécifique, et Samba et toutes les autres versions de Windows utilisent le champ « opnum » dans le dernier fragment.

Il existe également des différences importantes dans les implémentations de Windows et Samba SMB. Par exemple, Windows reconnaît les commandes SMB OPEN et READ lorsqu'il utilise des canaux nommés, mais Samba ne reconnaît pas ces commandes.

Lorsque vous activez le préprocesseur DCE/RPC, vous activez automatiquement une politique basée sur la cible par défaut. Vous pouvez également ajouter des politiques basées sur la cible qui ciblent d'autres hôtes exécutant différentes versions de Windows ou de Samba. La politique basée sur la cible par défaut s'applique à tout hôte non inclus dans une autre politique basée sur la cible.

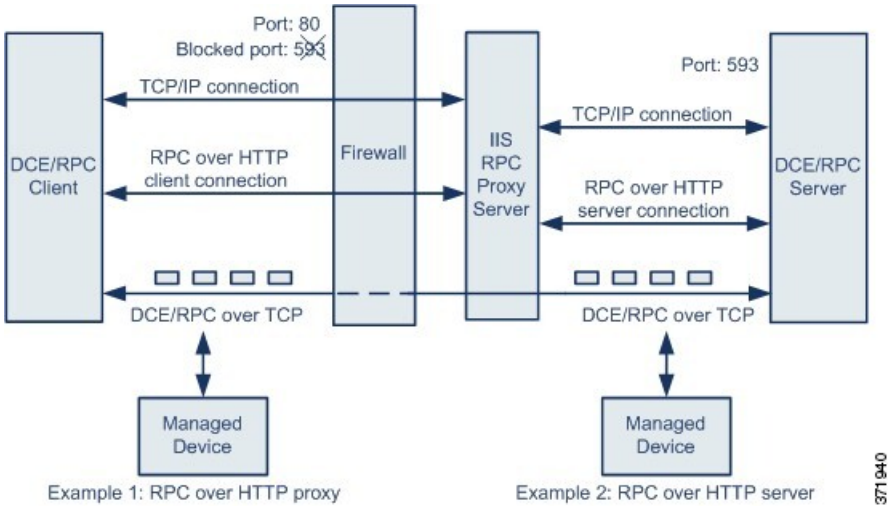
Dans chaque politique basée sur la cible, vous pouvez :

- activer un ou plusieurs transports et préciser les *ports de détection* pour chacun.
- activer et préciser *les ports à détection automatique*
- configurer le préprocesseur pour détecter une ou plusieurs tentatives de connexion à une ou plusieurs ressources SMB partagées que vous identifiez
- configurer le préprocesseur pour détecter les fichiers dans le trafic SMB et pour inspecter un nombre donné d'octets dans un fichier détecté
- modifier une option avancée qui ne doit être modifiée que par un utilisateur expert en protocole SMB; cette option vous permet de configurer le préprocesseur pour détecter quand un certain nombre de commandes SMB AndX en chaîne dépasse un nombre maximal spécifié

En plus d'activer la détection des fichiers de trafic SMB dans le préprocesseur DCE/RPC, vous pouvez configurer une politique de fichiers pour capturer et bloquer ces fichiers ou les soumettre au nuage Cisco AMP pour une analyse dynamique. Dans cette politique, vous devez créer une règle de fichier avec une **action** de **détecter les fichiers** ou de **bloquer les fichiers** et un **protocole d'application** sélectionné **Any** ou **NetBIOS-ssn (SMB)**.

Transport RPC sur HTTP

Microsoft RPC sur HTTP vous permet de canaliser le trafic DCE/RPC à travers un pare-feu, comme l'illustre le diagramme suivant. Le préprocesseur DCE/RPC détecte la version 1 de Microsoft RPC sur HTTP.



Le serveur mandataire Microsoft IIS et le serveur DCE/RPC peuvent se trouver sur le même hôte ou sur des hôtes différents. Des options de serveur mandataire et de serveur distincts permettent les deux cas. Notez les éléments suivants dans la figure :

- Le serveur DCE/RPC surveille le port 593 pour le trafic client DCE/RPC, mais le pare-feu bloque le port 593.

  Les pare-feu bloquent généralement le port 593 par défaut.
- RPC sur HTTP transporte DCE/RPC sur HTTP en utilisant le port HTTP 80 bien connu, ce que les pare-feu sont susceptibles de permettre.
- L'exemple 1 montre que vous choisiriez l'option de **proxy RPC sur HTTP** pour surveiller le trafic entre le client DCE/RPC et le serveur proxy RPC Microsoft IIS.

- L’exemple 2 montre que vous choisiriez l’option **de serveur RPC sur HTTP** lorsque le serveur mandataire RPC de Microsoft IIS et le serveur DCE/RPC sont situés sur des hôtes différents et le périphérique surveille le trafic entre les deux serveurs.
- Le trafic est composé uniquement d’un transfert DCE/RPC sur TCP en orienté connexion une fois que RPC sur HTTP a terminé la configuration par serveur mandataire entre le client et le serveur DCE/RPC.

Options globales DCE/RPC

Les options globales de préprocesseur DCE/RPC contrôlent le fonctionnement du préprocesseur. Notez qu’à l’exception des options **Mémoire maximale atteinte** et **Politique de détection automatique sur la session SMB**, la modification de ces options peut avoir un impact négatif sur les performances ou la capacité de détection. Vous ne devez pas les modifier à moins de maîtriser parfaitement le préprocesseur et l’interaction entre le préprocesseur et les règles DCE/RPC activées.

Si aucune règle de préprocesseur n’est mentionnée dans les descriptions suivantes, l’option n’est associée à aucune règle de préprocesseur.

Taille maximale de fragment

Lorsque l’option d’ **activation de la défragmentation** est sélectionnée, cette valeur précise la longueur maximale de fragment DCE/RPC autorisée. Le préprocesseur tronque les fragments plus volumineux à des fins de traitement à la taille spécifiée avant la défragmentation, mais ne modifie pas le paquet lui-même. Un champ vide désactive cette option.

Assurez-vous que l’option **Maximum Fragment Size** (Taille maximum de fragment) est supérieure ou égale à la profondeur à laquelle les règles doivent détecter.

Seuil de réassemblage

Lorsque l'option d'**activation de la défragmentation** est sélectionnée, la valeur 0 désactive cette option ou spécifie un nombre minimal d'octets DCE/RPC fragmentés et, le cas échéant, d'octets SMB segmentés à mettre en file d'attente avant d'envoyer un paquet réassemblé au moteur de règles. Une valeur faible augmente la probabilité d’une détection précoce, mais peut avoir un impact négatif sur les performances. Vous devez effectuer un test de l’impact sur les performances si vous activez cette option.

Vérifiez que l’option de **seuil de réassemblage** est supérieure ou égale à la profondeur à laquelle les règles doivent détecter.

Activer la défragmentation

Spécifie s’il faut défragmenter le trafic DCE/RPC fragmenté. Lorsqu’elle est désactivée, le préprocesseur détecte toujours les anomalies et envoie des données DCE/RPC au moteur de règles, mais au risque de rater des exploits dans les données DCE/RPC fragmentées.

Bien que cette option offre la possibilité de ne pas défragmenter le trafic DCE/RPC, la plupart des exploits DCE/RPC tentent de profiter de la fragmentation pour masquer l’exploitation. La désactivation de cette option contournerait la plupart des exploits connus, ce qui entraînerait un grand nombre de faux négatifs.

Mémoire maximale atteinte

Détecte lorsque la limite de mémoire maximale allouée au préprocesseur est atteinte ou dépassée. Lorsque la limite maximale de mémoire est atteinte ou dépassée, le préprocesseur libère toutes les données en attente associées à la session qui a provoqué l’événement de limite de mémoire et ignore le reste de cette session.

Vous pouvez activer la règle 133:1 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Politique de détection automatique sur session SMB

Détecte la version de Windows ou de Samba identifiée dans les demandes et réponses `AndX de configuration de session` SMB. Lorsque la version détectée est différente de la version de Windows ou Samba configurée pour l'option de configuration de la **politique**, la version détectée remplace la version configurée uniquement pour cette session.

Par exemple, si vous définissez **la politique** sur Windows XP et que le préprocesseur détecte Windows XP, le préprocesseur utilise une politique Windows XP pour cette session. Les autres paramètres restent en vigueur.

Lorsque le transport DCE/RPC n'est pas SMB (c'est-à-dire lorsque le transport est TCP ou UDP), la version ne peut pas être détectée et la politique ne peut pas être configurée automatiquement.

Pour activer cette option, choisissez l'une des options suivantes dans la liste déroulante :

- Choisissez **Client** pour inspecter le trafic de serveur à client pour le type de politique.
- Choisissez **Serveur** pour inspecter le trafic client-serveur pour le type de politique.
- Choisissez les **deux** pour inspecter le trafic serveur-client et client-serveur pour le type de politique.

Mode d'inspection du SMB hérité

Lorsque le **mode d'inspection SMB** existant est activé, le système applique les règles de prévention des intrusions SMB uniquement au trafic SMB version 1 et applique les règles de prévention des intrusions DCE/RPC au trafic DCE/RPC en utilisant SMB version 1 comme transport. Lorsque cette option est désactivée, le système applique les règles de prévention des intrusions SMB au trafic utilisant SMB versions 1, 2 et 3, mais applique les règles de prévention des intrusions DCE/RPC au trafic DCE/RPC en utilisant SMB comme transport uniquement pour la version SMB 1.

Sujets connexes

Arguments pour le contenu de base et le mot-clé protected_content
Présentation : mots-clés byte_jump et byte_test

Options de politique basées sur la cible DCE/RPC

Dans chaque politique basée sur la cible, vous pouvez activer un ou plusieurs des transports TCP, UDP, SMB et RPC sur HTTP. Lorsque vous activez un transport, vous devez également préciser un ou plusieurs *ports de détection*, c'est-à-dire des ports connus pour acheminer le trafic DCE/RPC.

Cisco vous recommande d'utiliser les ports de détection par défaut, qui sont soit des ports bien connus, soit des ports couramment utilisés pour chaque protocole. Vous devez ajouter des ports de détection uniquement si vous détectez le trafic DCE/RPC sur un port autre que celui par défaut.

Vous pouvez spécifier des ports pour un ou plusieurs transports dans n'importe quelle combinaison dans une politique basée sur une cible Windows afin de correspondre au trafic sur votre réseau, mais vous ne pouvez spécifier des ports que pour le transport SMB dans une politique basée sur une cible Samba.

Remarque Vous devez activer au moins un transport DCE/RPC dans la politique basée sur la cible par défaut, sauf lorsque vous avez ajouté une politique basée sur la cible DCE/RPC qui a au moins un transport activé. Par exemple, vous pourriez souhaiter préciser les hôtes pour toutes les implémentations DCE/RPC et ne pas faire en sorte que la politique basée sur la cible par défaut soit déployée vers des hôtes non spécifiés, auquel cas vous n'activez pas de transport pour la politique basée sur la cible par défaut.

Vous pouvez également activer et spécifier *des ports de détection automatique*, c'est-à-dire des ports que le préprocesseur teste d'abord pour déterminer s'ils acheminent le trafic DCE/RPC et qui poursuit le traitement uniquement lorsqu'il détecte du trafic DCE/RPC.

Lorsque vous activez les ports à détection automatique, assurez-vous qu'ils sont compris dans la plage de ports comprise entre 1 1024 et 65 535 afin de couvrir toute la plage de ports éphémères.

Notez que la détection automatique se produit uniquement pour les ports qui ne sont pas déjà identifiés par les ports de détection de transport.

Il est peu probable que vous activiez ou spécifiiez des ports de détection automatique pour l'option de détection automatique des ports par mandataire RPC sur HTTP ou l'option de détection automatique des ports SMB, car il est peu probable qu'un trafic se produise ou soit possible, sauf sur ports de détection par défaut précisés.

Chaque politique basée sur la cible vous permet de spécifier les différentes options ci-dessous. Si aucune règle de préprocesseur n'est mentionnée dans les descriptions suivantes, l'option n'est associée à aucune règle de préprocesseur.

Réseaux

Les adresses IP de l'hôte sur lequel vous souhaitez déployer la politique de serveur basée sur la cible DCE/RPC. Également nommé champ **Server Address** (adresse du serveur) dans la fenêtre contextuelle Add Target (ajouter une cible) lorsque vous ajoutez une politique basée sur la cible.

Vous pouvez spécifier une adresse IP unique, ou bloc d'adresses, ou une liste de ces deux éléments (séparés par des virgules) ou des deux. Vous pouvez configurer jusqu'à 255 profils au total, y compris la politique par défaut.

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Notez que le paramètre par `défaut` de la politique par défaut spécifie toutes les adresses IP de votre segment de réseau surveillé qui ne sont pas couvertes par une autre politique basée sur la cible. Par conséquent, vous ne pouvez pas et n'avez pas besoin de spécifier une adresse IP ou une longueur de bloc ou de préfixe CIDR pour la politique par défaut, et vous ne pouvez pas laisser ce paramètre vide dans une autre politique ou utiliser la notation de l'adresse pour représenter `toute` (par exemple, 0.0.0.0/0 ou:/0).

Politique

L'implémentation de Windows ou Samba DCE/RPC utilisée par l'hôte ou les hôtes ciblés sur votre segment de réseau surveillé.

Notez que vous pouvez activer l'option globale **de politique de détection automatique lors de la session SMB** pour remplacer automatiquement le paramètre de cette option sur une base par session lorsque SMB est le transport DCE ou RPC.

Parts SMB non valides

Identifie une ou plusieurs ressources partagées SMB que le préprocesseur détectera lors d'une tentative de connexion à une ressource partagée que vous spécifiez. Vous pouvez spécifier plusieurs partages dans une liste séparées par des virgules et, éventuellement, vous pouvez mettre entre guillemets les partages, ce qui était obligatoire dans les versions précédentes du logiciel, mais qui ne sont plus nécessaires. Par exemple :

```
"C$", D$, "admin", private
```

Le préprocesseur détecte les partages non valides dans le trafic SMB lorsque vous avez activé les **ports SMB**.

Notez que dans la plupart des cas, vous devez ajouter un signe de dollar à un lecteur nommé par Windows que vous identifiez comme partage non valide. Par exemple, identifiez le lecteur C de la façon suivante : C$ ou "C$".

Notez également que pour détecter les partages SMB non valides, vous devez également activer les **ports SMB ou la détection automatique des ports SMB.**

Vous pouvez activer la règle 133:26 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Chaîne AndX et SMB maximale

Le nombre maximal de commandes SMB AndX en chaîne à autoriser. En règle générale, plusieurs commandes AndX en chaîne représentent un comportement anormal et peuvent indiquer une tentative d'évitement. Spécifiez 1 pour n'autoriser aucune commande en chaîne ou 0 pour désactiver la détection du nombre de commandes en chaîne.

Notez que le préprocesseur commence par compter le nombre de commandes en chaîne et génère un événement si les règles de préprocesseur SMB associées sont activées et que le nombre de commandes en chaîne est égal ou supérieur à la valeur configurée. Le traitement se poursuit ensuite.

Mise en garde Seule un expert du protocole SMB doit modifier le paramètre de l'option **de chaînes SMB maximales AndX**.

Vous pouvez activer la règle 133:20 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Uniquement le trafic du serveur mandataire RPC

L'activation **des ports RPC sur HTTP** indique si le trafic RPC sur HTTP côté client détecté est uniquement du trafic de proxy ou s'il peut inclure un autre trafic de serveur Web. Par exemple, le port 80 peut acheminer à la fois le trafic du serveur mandataire et d'autres trafics de serveur Web.

Lorsque cette option est désactivée, le trafic du serveur mandataire et celui des autres serveurs Web sont attendus. Activez cette option, par exemple, si le serveur est un serveur mandataire dédié. Lorsque cette option est activée, le préprocesseur teste le trafic pour déterminer s'il transporte DCE ou RPC, ignore le trafic si ce n'est pas le cas et poursuit le traitement dans le cas inverse. Notez que l'activation de cette option ajoute des fonctionnalités uniquement si la case **RPC sur les ports du mandataire HTTP** est également cochée.

RPC sur les ports serveur mandataire HTTP

Active la détection du trafic DCE/RPC acheminé par tunnellisation par RPC sur HTTP sur chaque port spécifié lorsque votre périphérique géré est placé entre le client DCE/RPC et le serveur mandataire Microsoft IIS RPC.

Lorsque cette option est activée, vous pouvez ajouter n'importe quel port sur lequel vous voyez du trafic DCE/RPC, bien que cela soit peu susceptible d'être nécessaire, car les serveurs Web utilisent généralement le port par défaut pour le trafic DCE/RPC et le reste du trafic. Lorsque cette option est activée, vous n'activez pas la **détection automatique des ports de mandataire RPC sur HTTP**, mais vous activez le **trafic de serveur mandataire RPC uniquement** lorsque le trafic RPC sur HTTP du côté client est détecté est du trafic de serveur mandataire uniquement et n'inclut pas d'autres trafics de serveur Web.

Remarque Vous sélectionneriez rarement cette option.

RPC sur les ports du serveur HTTP

Active la détection du trafic DCE/RPC acheminé par tunnellisation par RPC sur HTTP sur chaque port spécifié lorsque le serveur mandataire Microsoft IIS RPC et le serveur DCE/RPC sont situés sur des hôtes différents et que le périphérique surveille le trafic entre les deux serveurs.

En règle générale, lorsque vous activez cette option, vous devez également activer **RPC sur HTTP les ports de détection automatique du serveur** avec une plage de ports comprise entre 1 025 et 65 535 pour cette option, même si vous n'avez connaissance d'aucun serveur Web mandataire sur votre réseau. Notez que le port du serveur RPC sur HTTP est parfois reconfiguré, auquel cas vous devez ajouter le port du serveur reconfiguré à la liste de ports pour cette option.

Ports TCP

Active la détection du trafic DCE/RPC dans TCP sur chaque port précisé.

Le trafic et les exploits DCE/RPC légitimes peuvent utiliser une grande variété de ports, et les autres ports supérieurs au port 1024 sont courants. En règle générale, lorsque cette option est activée, vous devez également activer **les ports à détection automatique TCP** avec une plage de ports comprise entre 1 025 et 65 535 pour cette option.

Ports UDP

Active la détection du trafic DCE/RPC en UDP sur chaque port précisé.

Le trafic et les exploits DCE/RPC légitimes peuvent utiliser une grande variété de ports, et les autres ports supérieurs au port 1024 sont courants. En règle générale, lorsque cette option est activée, vous devez également activer **les ports à détection automatique UDP** avec une plage de ports comprise entre 1 025 et 65 535 pour cette option.

Ports SMB

Active la détection du trafic DCE/RPC dans SMB sur chaque port spécifié.

Vous pourriez rencontrer du trafic SMB en utilisant les ports de détection par défaut. Les autres ports sont rares. En général, utilisez les paramètres par défaut.

Notez que vous pouvez activer l'option globale **de détection automatique de la politique lors de la session SMB** pour remplacer automatiquement le type de politique configuré pour une politique ciblée par session lorsque SMB est le transport DCE/RPC.

RPC sur les ports du serveur mandataire HTTP à détection automatique

Active la détection automatique du trafic DCE/RPC acheminé par le tunnel RPC sur HTTP sur les ports spécifiés lorsque votre périphérique géré est placé entre le client DCE/RPC et le serveur mandataire Microsoft IIS RPC.

Lorsque cette option est activée, vous devez généralement préciser une plage de ports comprise entre 1 025 et 65 535 pour couvrir toute la plage des ports éphémères.

RPC sur les ports de serveur HTTP à détection automatique

Active la détection automatique du trafic DCE/RPC tunnelisé par RPC sur HTTP sur les ports spécifiés lorsque le serveur mandataire Microsoft IIS RPC et le serveur DCE/RPC sont situés sur des hôtes différents et que le périphérique surveille le trafic entre les deux serveurs.

Ports TCP à détection automatique

Active la détection automatique du trafic DCE/RPC dans TCP sur les ports spécifiés.

Ports UDP à détection automatique

Active la détection automatique du trafic DCE/RPC en UDP sur chaque port spécifié.

Ports SMB à détection automatique

Active la détection automatique du trafic DCE/RPC dans SMB.

Remarque Vous sélectionneriez rarement cette option.

Inspection de fichier SMB

Active l'inspection du trafic SMB pour la détection de fichiers. Vous avez les options suivantes :

- Sélectionnez **Off** (désactiver) pour désactiver l'inspection des fichiers.
- Sélectionnez **Only** (uniquement) pour inspecter les données du fichier sans inspecter le trafic DCE/RPC dans SMB. La sélection de cette option peut améliorer les performances par rapport à l'inspection des fichiers et du trafic DCE/RPC.
- Sélectionnez **On** (activer) pour inspecter à la fois les fichiers et le trafic DCE/RPC dans SMB. La sélection de cette option peut avoir des conséquences sur les performances.

L'inspection du trafic SMB n'est pas prise en charge pour les éléments suivants :

- les fichiers transférés simultanément au cours d'une seule session TCP ou SMB
- les fichiers transférés entre plusieurs sessions TCP ou SMB

- les fichiers transférés avec des données non contiguës, par exemple lors de la négociation de la signature de message
- les fichiers transférés avec des données différentes au même décalage, se chevauchant les données
- les fichiers ouverts sur un client distant en vue de leur modification que le client enregistre sur le serveur de fichiers

Profondeur d'inspection de fichier SMB

Si l'**inspection de fichier SMB** est définie sur **Only** ou sur **On**, il s'agit du nombre d'octets inspectés lorsqu'un fichier est détecté dans le trafic SMB. Spécifiez l'une des valeurs suivantes :

- une valeur positive
- `0` pour inspecter l'ensemble du fichier
- `-1` pour désactiver l'inspection des fichiers

Saisissez une valeur dans ce champ égale ou inférieure à celle définie dans la section Paramètres des fichiers et des programmes malveillants de l'onglet Avancé de votre politique de contrôle d'accès. Si vous définissez pour cette option une valeur supérieure à celle définie pour **Limite le nombre d'octets inspectés lors de la détection du type de fichier**, le système utilise le paramètre de politique de contrôle d'accès comme maximum fonctionnel.

Si l'**inspection de fichiers SMB** est **désactivée**, ce champ est désactivé.

Règles DCE/RPC associées au trafic

La plupart des règles de préprocesseur DCE/RPC se déclenchent en cas d'anomalies et de techniques de contournement détectées dans le trafic SMB, DCE/RPC en mode orienté connexion ou DCE/RPC sans connexion. Le tableau suivant identifie les règles que vous pouvez activer pour chaque type de trafic.

Tableau 1 : Règles DCE/RPC associées au trafic

Trafic	GID de la règle de préprocesseur : SID
SMB	Contrôles de 133:2 à 133:26 et de 133:48 à 133:59
DCE/RPC orienté connexion	133:27 à 133:39
Détecter DCE/RPC sans connexion	133:40 à 133:43

Configuration du préprocesseur DCE/RPC

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Vous configurez le préprocesseur DCE/RPC en modifiant n'importe quelle des options globales qui contrôlent le fonctionnement du préprocesseur et en spécifiant une ou plusieurs politiques de serveur basées sur la cible

qui identifient les serveurs DCE/RPC de votre réseau par adresse IP et par ou de Samba. La configuration de politiques basées sur la cible comprend également l'activation des protocoles de transport, la spécification des ports acheminant le trafic DCE/RPC vers ces hôtes et la définition d'autres options spécifiques au serveur.

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Avant de commencer

- Confirmez que les réseaux que vous souhaitez identifier dans une politique basée sur une cible personnalisée correspondent ou constituent un sous-ensemble des réseaux, des zones et des VLAN gérés par sa politique d'analyse de réseau parente. Consultez Paramètres avancés pour les politiques d'analyse de réseau pour obtenir de plus amples renseignements.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation à gauche.

Étape 5 Si **la configuration DCE/RPC** est désactivée sous **Préprocesseurs de la couche d'application**, cliquez sur **Enabled** (Activé).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Configuration DCE/RPC**.

Étape 7 Modifiez les options dans la section **Global Settings** (Paramètres globaux); voir Options globales DCE/RPC, à la page 6.

Étape 8 Vous avez les choix suivants :

- Add a server profile (ajouter un profil de serveur) : cliquez sur **Ajouter** (+) à côté de **Servers** (Serveurs). Précisez une ou plusieurs adresses IP dans le champ **Server Address** (adresse du serveur), puis cliquez sur **OK**.
- Supprimer un profil de serveur : cliquez sur **Supprimer** (🗑) à côté de la politique.
- Edit a server profile (modifier un profil de serveur) : cliquez sur l'adresse configurée pour le profil sous **Servers**, ou cliquez sur Default (**par défaut**). Vous pouvez modifier n'importe quel paramètre dans la section **Configuration** ; voir Options de politique basées sur la cible DCE/RPC, à la page 7.

Étape 9 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez générer des incidents d'intrusion, activez les règles de préprocesseur DCE/RPC (GID 132 ou 133). Pour plus de renseignements, consultez Définition des états des règles d’intrusion, Options globales DCE/RPC, à la page 6, Options de politique basées sur la cible DCE/RPC, à la page 7, et Règles DCE/RPC associées au trafic, à la page 12.
- Déployer les changements de configuration.

Sujets connexes

Options de rendement et de stockage pour l'inspection des fichiers et des logiciels malveillants
Mots-clés DCE/RPC
Gestion des couches
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions

Le préprocesseur DNS

Remarque Cette section s’applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le préprocesseur DNS inspecte les réponses des serveurs de noms DNS à la recherche des exploits spécifiques suivants :

- Tentatives de dépassement de capacité sur les champs de texte RData
- Types d’enregistrements de ressource DNS obsolètes
- Types d’enregistrements de ressources DNS expérimentaux

Le type de réponse de serveur de noms DNS le plus courant fournit une ou plusieurs adresses IP qui correspondent aux noms de domaine dans la requête qui a entraîné la réponse. D’autres types de réponses de serveur fournissent, par exemple, la destination d’un courriel ou l’emplacement d’un serveur de noms qui peut fournir des informations non disponibles sur le serveur interrogé initialement.

Une réponse DNS comprend les éléments suivants :

- En-tête du message
- Une section Question qui contient une ou plusieurs requêtes
- Trois sections qui répondent aux demandes de la section Question

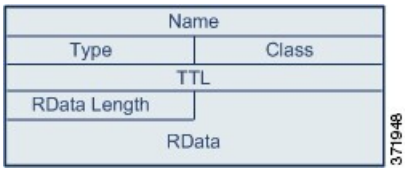
- Réponse
- Autorité
- Autres renseignements.

Les réponses dans ces trois sections reflètent les informations contenues dans *les enregistrements de ressources* (RR) conservés sur le serveur de noms. Le tableau suivant décrit ces trois options.

Tableau 2 : Réponses RR du serveur de noms DNS

Cette section...	Comprend...	Par exemple...
Réponse	Éventuellement, un ou plusieurs enregistrements de ressource qui fournissent une réponse précise à une requête	L'adresse IP correspondant à un nom de domaine
Autorité	Éventuellement, un ou plusieurs enregistrements de ressource qui pointent vers un serveur de noms faisant autorité	Le nom d'un serveur de noms faisant autorité pour la réponse
Autres renseignements	Facultativement, un ou plusieurs enregistrements de ressource ayant fourni des renseignements supplémentaires liés aux sections de réponses	L'adresse IP d'un autre serveur à interroger

Il existe de nombreux types d'enregistrements de ressources, qui respectent tous la structure suivante :



En principe, tout type d'enregistrement de ressource peut être utilisé dans la section Réponse, Autorité ou Renseignements supplémentaires d'un message de réponse de serveur de noms. Le préprocesseur DNS inspecte tout enregistrement de ressource dans chacune des trois sections de réponse pour repérer les exploits qu'il détecte.

Les champs d'enregistrement de ressource Type et RData sont particulièrement importants pour le préprocesseur DNS. Le champ Type identifie le type de l'enregistrement de ressource. Le champ RData (resource data) fournit le contenu de la réponse. La taille et le contenu du champ RData varient selon le type d'enregistrement de ressource.

Les messages DNS utilisent généralement le protocole de transport UDP, mais aussi TCP lorsque le type du message nécessite une livraison fiable ou que la taille du message dépasse les capacités d'UDP. Le préprocesseur DNS inspecte les réponses du serveur DNS dans le trafic UDP et TCP.

Le préprocesseur DNS n'inspecte pas les sessions TCP détectées en cours de route et interrompt l'inspection si une session perd son état en raison de paquets abandonnés.

Options du préprocesseur DNS

Ports

Ce champ spécifie le ou les ports source que le préprocesseur DNS doit surveiller pour les réponses du serveur DNS. Séparez les valeurs de ports multiples par des virgules.

Le port typique à configurer pour le préprocesseur DNS est le port bien connu 53, que les serveurs de noms DNS utilisent pour les messages DNS en UDP et TCP.

Détecter les tentatives de dépassement de capacité sur les champs de texte RData

Lorsque le type d'enregistrement de ressource est TEXT (texte), le champ RData est un champ de texte ASCII de longueur variable.

Lorsqu'elle est sélectionnée, cette option détecte une vulnérabilité précise identifiée par l'entrée CVE-2006-3441 dans la base de données des vulnérabilités et expositions actuelles de MITRE. Il s'agit d'une vulnérabilité connue de Microsoft Windows 2000, Service Pack 4, Windows XP Service Pack 1 et Service Pack 2, et Windows Server 2003 Service Pack 1. Un attaquant peut exploiter cette vulnérabilité et prendre le contrôle total d'un hôte en envoyant ou en faisant recevoir à l'hôte une réponse de serveur de noms conçue de manière malveillante qui entraîne une erreur de calcul dans la longueur d'un champ de texte RData, ce qui entraîne un débordement de la mémoire tampon.

Vous devez activer cette option lorsque votre réseau peut comprendre des hôtes exécutant des systèmes d'exploitation qui n'ont pas été mis à niveau pour corriger cette vulnérabilité.

Vous pouvez activer la règle 131:3 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Détecter les types de DNS RR obsolètes

La RFC 1035 identifie plusieurs types d'enregistrements de ressource comme obsolètes. Puisqu'il s'agit de types d'enregistrements obsolètes, certains systèmes ne les prennent pas en compte et peuvent être exposés aux exploits. Vous ne vous attendez pas à rencontrer ces types d'enregistrements dans des réponses DNS normales, sauf si vous avez délibérément configuré votre réseau pour les inclure.

Vous pouvez configurer le système pour détecter les types d'enregistrements de ressource obsolètes connus. Le tableau suivant répertorie et décrit ces types d'enregistrements.

Tableau 3 : Types d'enregistrements de ressource DNS obsolètes

Type RR	Code	Description
3	MD	une destination de messagerie
4	mf	un redirecteur de courrier

Vous pouvez activer la règle 131:1 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Détecter les types de DNS RR expérimentaux

La RFC 1035 identifie plusieurs types d'enregistrements de ressource comme expérimentaux. Puisqu'il s'agit de types d'enregistrements expérimentaux, certains systèmes ne les prennent pas en compte et peuvent être sujets à des exploits. Vous ne vous attendez pas à rencontrer ces types d'enregistrements dans des réponses DNS normales, sauf si vous avez délibérément configuré votre réseau pour les inclure.

Vous pouvez configurer le système pour détecter les types d'enregistrements de ressource expérimentaux connus. Le tableau suivant répertorie et décrit ces types d'enregistrements.

Tableau 4 : Types d'enregistrements de ressource DNS exploratoires

Type RR	Code	Description
7	Mo	un nom de domaine de boîte de courriel
8	MG	un membre du groupe de messagerie
9	MR	nom de domaine de changement de nom de messagerie
10	nulle	un enregistrement de ressource nul

Vous pouvez activer la règle 131:2 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Configuration du préprocesseur DNS

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si **la configuration DNS** est désactivée sous **Préprocesseurs de la couche d'application**, cliquez sur **Enabled** (Activé).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Configuration DNS**.

Étape 7 Modifiez les paramètres comme décrit dans Options du préprocesseur DNS, à la page 16.

Étape 8 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez générer des incidents d'intrusion, activez les règles de préprocesseur DNS (GID 131). Pour plus de renseignements, consultez les sections Définition des états des règles d'intrusion et Options du préprocesseur DNS, à la page 16.
- Déployer les changements de configuration.

Sujets connexes

Couches des politiques d'analyse des réseaux et de prévention des intrusions
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions

Le décodeur Telnet/FTP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le décodeur FTP/Telnet analyse les flux de données FTP et Telnet, normalise les commandes FTP et Telnet avant leur traitement par le moteur de règles.

Options globales FTP et Telnet

Vous pouvez définir des options globales pour déterminer si le décodeur FTP/Telnet effectue une inspection des paquets avec ou sans état, si le décodeur détecte les sessions FTP ou Telnet chiffrées et s'il continue de vérifier un flux de données après avoir rencontré des données chiffrées.

Si aucune règle de préprocesseur n'est mentionnée dans les descriptions suivantes, l'option n'est associée à aucune règle de préprocesseur.

Inspection dynamique

Lorsque cette option est sélectionnée, le décodeur FTP/Telnet enregistre l'état et fournit un contexte de session pour les paquets individuels et inspecte uniquement les sessions réassemblées. Lorsqu'elle est désélectionnée, cette option analyse chaque paquet individuellement sans contexte de session.

Pour vérifier les transferts de données FTP, cette option doit être sélectionnée.

Détection de trafic chiffré

Détecte les sessions Telnet et FTP chiffrées.

Vous pouvez activer les règles 125:7 et 126:2 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Continuer à inspecter les données chiffrées

Demande au préprocesseur de continuer à vérifier un flux de données après son chiffrement, à la recherche d'éventuelles données déchiffrées qui peuvent être traitées.

Options Telnet

Vous pouvez activer ou désactiver la normalisation des commandes telnet par le décodeur FTP/Telnet, activer ou désactiver un cas d'anomalie spécifique et définir le nombre seuil d'attaques Are You There (AYT) à autoriser.

Si aucune règle de préprocesseur n'est mentionnée dans les descriptions suivantes, l'option n'est associée à aucune règle de préprocesseur.

Ports

Indique les ports dont vous souhaitez normaliser le trafic Telnet. Telnet se connecte généralement au port TCP 23. Dans l'interface, répertoriez plusieurs ports séparés par des virgules.

Mise en garde Comme le trafic chiffré (SSL) ne peut pas être décodé, l'ajout du port 22 (SSH) peut donner des résultats inattendus.

Normaliser

Normalise le trafic Telnet vers les ports spécifiés.

Détecter les anomalies

Permet la détection de Telnet SB (début de sous-négociation) sans le SE correspondant (fin de sous-négociation).

Telnet prend en charge la sous-négociation, qui commence par SB (Subnegotiation starts) et doit se terminer par un SE (Subnegotiation End). Cependant, certaines implémentations de serveurs Telnet ignoreront le SB sans SE correspondant. Il s'agit d'un comportement anormal qui pourrait être un cas d'évitement. Étant donné que FTP utilise le protocole Telnet sur la connexion de contrôle, il est également susceptible de faire preuve de ce comportement.

Vous pouvez activer la règle 126:3 pour générer un événement et, dans le cadre d'un déploiement en ligne, abandonner les paquets incriminés lorsque cette anomalie est détectée dans le trafic Telnet, et la règle 125:9 lorsqu'elle est détectée sur le canal de commande FTP. Consultez Définition des états des règles d'intrusion.

Seuil du nombre d'attaques Are You There (Êtes-vous là)?

Détecte lorsque le nombre de commandes AYT (Are You There) consécutives dépasse le seuil spécifié. Cisco vous recommande de définir le seuil AYT à une valeur non supérieure à la valeur par défaut.

Vous pouvez activer la règle 126:1 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Options FTP au niveau du serveur

Vous pouvez définir des options de décodage sur plusieurs serveurs FTP. Chaque profil de serveur que vous créez contient l'adresse IP du serveur et les ports du serveur sur lesquels le trafic doit être surveillé. Vous pouvez spécifier les commandes FTP à valider et celles à ignorer pour un serveur particulier et définir les longueurs maximales des paramètres pour les commandes. Vous pouvez également définir la syntaxe de commande spécifique à l'aide du décodeur pour des commandes particulières et définir d'autres longueurs maximales des paramètres de commande.

Si aucune règle de préprocesseur n'est mentionnée dans les descriptions suivantes, l'option n'est associée à aucune règle de préprocesseur.

Réseaux

Utilisez cette option pour spécifier une ou plusieurs adresses IP de serveurs FTP.

Vous pouvez spécifier une adresse IP unique, ou un bloc d'adresses, ou une liste séparée par des virgules composée de l'un ou des deux. Vous pouvez configurer jusqu'à 1 024 caractères et spécifier jusqu'à 255 profils, y compris le profil par défaut.

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Notez que le paramètre par `défaut` de la politique par défaut spécifie toutes les adresses IP de votre segment de réseau surveillé qui ne sont pas couvertes par une autre politique basée sur la cible. Par conséquent, vous ne pouvez pas et n'avez pas besoin de spécifier une adresse IP ou un bloc d'adresses pour la politique par défaut, et vous ne pouvez pas laisser ce paramètre vide dans une autre politique ou utiliser la notation d'adresse pour représenter `une` (par exemple, 0.0.0.0/0 ou : : /0).

Ports

Utilisez cette option pour préciser les ports du serveur FTP sur lesquels le périphérique géré doit surveiller le trafic. Dans l'interface, répertoriez plusieurs ports séparés par des virgules. Le port 21 est le port bien connu pour le trafic FTP.

Fichier de commandes Get

Utilisez cette option pour définir les commandes FTP utilisées pour transférer les fichiers du serveur au client. Ne modifiez pas ces valeurs, sauf si le service d'assistance vous le demande.

Mise en garde Ne modifiez pas le champ **File Get Commands**, sauf sur instruction du service d'assistance.

Fichier de commande Put

Utilisez cette option pour définir les commandes FTP utilisées pour transférer les fichiers du client au serveur. Ne modifiez pas ces valeurs, sauf si le service d'assistance vous le demande.

Mise en garde Ne modifiez pas le champ **File Push Commands**, sauf sur instruction du service d'assistance.

Commandes FTP supplémentaires

Utilisez cette ligne pour spécifier les commandes supplémentaires que le décodeur doit détecter. Séparez les commandes supplémentaires par des espaces.

Vous souhaitez peut-être ajouter des commandes supplémentaires : `XPWD`, `XCWD`, `XCUP`, `XMKD`, et `XRMD`. Pour en savoir plus sur ces commandes, consultez la RFC 775, la spécification de commandes FTP axées sur le répertoire du Network Working Group.

Longueur maximale par défaut de paramètre

Utilisez cette option pour détecter la longueur maximale de paramètre pour les commandes pour lesquelles une autre longueur maximale de paramètre n'a pas été définie. Vous pouvez ajouter autant de longueurs maximales de paramètres alternatives que nécessaire.

Vous pouvez activer la règle 125:3 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Autre longueur maximale de paramètre

Utilisez cette option pour spécifier les commandes pour lesquelles vous souhaitez détecter une longueur maximale de paramètre différente et pour spécifier la longueur de paramètre maximale pour ces commandes. Cliquez sur **Add** (ajouter) pour ajouter des lignes dans lesquelles vous pouvez spécifier une longueur maximale de paramètre différente à détecter pour des commandes particulières.

Vérifier les commandes pour les attaques de format de chaîne

Utilisez cette option pour vérifier les commandes spécifiées pour les attaques de format de chaîne.

Vous pouvez activer la règle 125:5 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Validité de la commande

Utilisez cette option pour saisir un format valide pour une commande précise. Cliquez sur **Add** pour ajouter une ligne de validation de commande.

Vous pouvez activer les règles 125:2 et 125:4 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Ignorer les transferts FTP

Utilisez cette option pour améliorer les performances des transferts de données FTP en désactivant toutes les inspections autres que l'inspection d'état sur le canal de transfert de données.

Remarque Pour inspecter les transferts de données, l'option globale FTP/Telnet **Stateful Inspection** (Inspection avec état) doit être sélectionnée.

Détecter les codes d'échappement Telnet dans les commandes FTP

Utilisez cette option pour détecter quand les commandes Telnet sont utilisées sur le canal de commande FTP.

Vous pouvez activer la règle 125:1 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Ignorer les commandes d'effacement pendant la normalisation

Lorsque **Detect Telnet Escape Codes within FTP Commands** (Détecter les codes d'échappement Telnet dans les commandes FTP)) est sélectionné, utilisez cette option pour ignorer les commandes de suppression de caractère et de ligne Telnet lors de la normalisation du trafic FTP. Le paramètre doit correspondre à la façon dont le serveur FTP gère les commandes d'effacement Telnet. Notez que les nouveaux serveurs FTP ignorent généralement les commandes d'effacement Telnet, tandis que les serveurs plus anciens les traitent généralement.

Option de dépannage : enregistrer la configuration de validation de commande FTP

Lors d'un appel de dépannage, le service d'assistance peut vous demander de configurer votre système pour imprimer les informations de configuration pour chaque commande FTP répertoriée pour le serveur.

Mise en garde N'activez pas **Enregistrer la configuration de validation de commande FTP** sauf si le service d'assistance vous le demande.

Énoncés de validation des commandes FTP

Lors de la configuration d'une instruction de validation pour une commande FTP, vous pouvez spécifier un groupe de paramètres alternatifs en séparant les paramètres par des espaces. Vous pouvez également créer une relation OU binaire entre deux paramètres en les séparant par une barre verticale (`|`) dans l'instruction de validation. Les paramètres entre crochets (`[ ]`) environnants indiquent que ces paramètres sont facultatifs. Les paramètres environnants entre accolades (`{}`) indiquent que ces paramètres sont obligatoires.

Vous pouvez créer des instructions de validation de paramètre de commande FTP pour valider la syntaxe d'un paramètre reçu dans le cadre d'une communication FTP.

N'importe lequel des paramètres répertoriés dans le tableau suivant peut être utilisé dans les instructions de validation des paramètres de commande FTP.

Tableau 5 : Paramètres de commande FTP

Si vous utilisez...	La validation suivante se produit...
`int`	Le paramètre représenté doit être un entier.
`number`	Le paramètre représenté doit être un entier entre 1 et 255.
`char` _chars	Le paramètre représenté doit être un caractère unique et un membre des caractères spécifiés dans l'argument _chars. Par exemple, la définition de la validité de la commande `MODE` avec l'instruction de validation `char` SBC vérifie que le paramètre de la commande `MODE` comprend le caractère `S` (représentant le mode Flux), le caractère `B` (représentant le mode Bloquer) ou le caractère `C` (représentant le mode Compressé).
`date` _datefmt	Si _datefmt contient `#`, le paramètre représenté doit être un nombre. Si _datefmt contient `C`, le paramètre représenté doit être un caractère. Si _datefmt contient des chaînes littérales, le paramètre représenté doit correspondre à la chaîne littérale.
`chaîne`	Le paramètre représenté doit être une chaîne.
`host_port`	Le paramètre représenté doit être un spécificateur de port hôte valide au sens de la RFC 959, la spécification du protocole de transfert de fichiers (File Transfer Protocol) du Network Working Group.

Vous pouvez combiner la syntaxe du tableau ci-dessus selon vos besoins pour créer des instructions de validation de paramètres qui valident correctement chaque commande FTP où vous devez valider le trafic.

Remarque Lorsque vous incluez une expression complexe dans une commande TYPE, entourez-la d'espaces. En outre, entourez chaque opérande de l'expression par des espaces. Par exemple, tapez `char A | B` , et non `char A|B`.

Sujets connexes

Options FTP au niveau du serveur, à la page 20
Énoncés de validation des commandes FTP, à la page 22

Options FTP au niveau du client

Utilisez ces options pour configurer des profils client FTP personnalisés. Si la description d'option n'inclut pas de règle de préprocesseur, l'option n'est associée à aucune règle de préprocesseur.

Réseaux

Utilisez cette option pour spécifier une ou plusieurs adresses IP de clients FTP.

Vous pouvez spécifier une adresse IP unique, ou un bloc d'adresses, ou une liste séparée par des virgules composée de l'un ou des deux. Vous pouvez définir jusqu'à 1 024 caractères et 255 profils, y compris le profil par défaut.

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Notez que le paramètre par `défaut` de la politique par défaut spécifie toutes les adresses IP de votre segment de réseau surveillé qui ne sont pas couvertes par une autre politique basée sur la cible. Par conséquent, vous ne pouvez pas et n'avez pas besoin de spécifier une adresse IP ou un bloc d'adresses pour la politique par défaut, et vous ne pouvez pas laisser ce paramètre vide dans une autre politique ou utiliser la notation d'adresse pour représenter `une` (par exemple, 0.0.0.0/0 ou : : /0).

Temps maximal de réponse

Utiliser cette option pour préciser la longueur de réponse maximale autorisée à une commande FTP acceptée par le client. Cela peut détecter les débordements de base de la mémoire tampon.

Vous pouvez activer la règle 125:6 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Détecter les tentatives de rebond FTP

Utilisez cette option pour détecter les attaques par rebond FTP.

Vous pouvez activer la règle 125:8 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Autoriser le rebond FTP vers

Utilisez cette option pour configurer une liste d'hôtes et de ports supplémentaires sur les hôtes sur lesquels les commandes PORT FTP ne doivent pas être traitées comme des attaques par rebond FTP.

Détecter les codes d'échappement Telnet dans les commandes FTP

Utilisez cette option pour détecter quand les commandes Telnet sont utilisées sur le canal de commande FTP.

Vous pouvez activer la règle 125:1 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Ignorer les commandes d'effacement pendant la normalisation

Lorsque **Detect Telnet Escape Code within FTP Commands** (Détecter le code d'interruption Telnet dans les commandes FTP) est sélectionné, utilisez cette option pour ignorer les commandes d'effacement de caractère et de ligne Telnet lors de la normalisation du trafic FTP. Le paramètre doit correspondre à la façon dont le client FTP gère les commandes d'effacement Telnet. Notez que les nouveaux clients FTP ignorent généralement les commandes d'effacement Telnet, tandis que les clients plus anciens les traitent.

Configuration du décodeur FTP/Telnet

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Vous pouvez configurer des profils client pour les clients FTP afin de surveiller le trafic FTP provenant des clients.

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Avant de commencer

- Confirmez que les réseaux que vous souhaitez identifier dans une politique basée sur la cible personnalisée correspondent ou constituent un sous-ensemble des réseaux, des zones et des VLAN gérés par sa politique d'analyse de réseau parente. Consultez Paramètres avancés pour les politiques d'analyse de réseau pour obtenir de plus amples renseignements.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si **la configuration FTP et Telnet** est désactivée sous **Préprocesseurs de couche d'application**, cliquez sur **Enabled** (Activé).

Étape 6 Cliquez sur **Edit** (✎) (Modifier) à côté de **Configuration FTP et Telnet**.

Étape 7 Définissez les options dans la section des **paramètres globaux** comme décrit dans Options globales FTP et Telnet, à la page 18.

Étape 8 Définissez les options dans la section des **paramètres Telnet** comme décrit dans Options Telnet, à la page 19.

Étape 9 Gérer les profils de serveur FTP :

- Add a server profile (ajouter un profil de serveur) : cliquez sur **Ajouter** (+) à côté de **FTP Server** (serveur FTP). Précisez une ou plusieurs adresses IP pour le client dans le champ **Server Address** (adresse du serveur) et cliquez sur **OK**. Vous pouvez spécifier une adresse IP unique, ou bloc d'adresses, ou une

liste de ces deux éléments (séparés par des virgules) ou des deux. Vous pouvez définir jusqu'à 1 024 caractères et configurer jusqu'à 255 politiques, y compris la politique par défaut.

- Edit a server profile (modifier un profil de serveur) : cliquez sur l'adresse configurée pour un profil personnalisé sous **FTP Server** (serveur FTP), ou cliquez sur Default (**par défaut**). Vous pouvez modifier les paramètres dans la section **Configuration** ; voir Options FTP au niveau du serveur, à la page 20.
- Supprimer un profil de serveur : cliquez sur **Supprimer** ( ) à côté du profil.

Étape 10 Gérer les profils client FTP :

- Add a client profile (ajouter un profil client) : cliquez sur **Ajouter** ( ) à côté de **FTP Client**. Précisez une ou plusieurs adresses IP pour le client dans le champ **Client Address** (adresse du client) et cliquez sur **OK**. Vous pouvez spécifier une adresse IP unique, ou bloc d'adresses, ou une liste de ces deux éléments (séparés par des virgules) ou des deux. Vous pouvez définir jusqu'à 1 024 caractères et configurer jusqu'à 255 politiques, y compris la politique par défaut.
- Edit a client profile (modifier le profil client) . Cliquez sur l'adresse configurée pour un profil que vous avez ajouté sous **FTP Client**, ou cliquez sur Default (**par défaut**). Vous pouvez modifier les paramètres dans la zone de page de configuration; voir Options FTP au niveau du client, à la page 23.
- Delete a client profile (Supprimer un profil client) : cliquez sur **Supprimer** ( ) à côté d'un profil personnalisé.

Étape 11 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez générer des incidents d'intrusion, activez les règles de préprocesseur FTP et Telnet (GID 125 et 126). Pour en savoir plus, consultez Définition des états des règles d'intrusion.
- Déployer les changements de configuration.

Sujets connexes

Gestion des couches
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions

Le préprocesseur d'inspection HTTP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le préprocesseur HTTP Inspect est responsable de ce qui suit :

- décoder et normaliser les requêtes HTTP envoyées à et les réponses HTTP reçues des serveurs Web de votre réseau
- séparer les messages envoyés aux serveurs Web en composants URI, en-tête non témoin, en-tête de témoin, méthode et corps de message pour améliorer les performances des règles de prévention des intrusions liées à HTTP
- séparer les messages reçus des serveurs Web selon les composants code d'état, message d'état, en-tête non défini de témoin, en-tête de témoin et corps de la réponse pour améliorer les performances des règles de prévention des intrusions liées au protocole HTTP
- la détection d'attaques possibles par encodage d'URI
- mettre les données normalisées à disposition pour un traitement de règle supplémentaire
- la détection et la prévention des attaques par le biais de scripts malveillants tels que JavaScript.

Le trafic HTTP peut être codé dans une variété de formats, ce qui complique l'inspection appropriée des règles. HTTP Inspect décode 14 types de codage, ce qui fait en sorte que votre trafic HTTP reçoive la meilleure inspection possible.

Vous pouvez configurer les options HTTP Inspect globalement, sur un serveur unique ou pour une liste de serveurs.

Notez que le moteur de préprocesseur effectue la normalisation HTTP *sans état*. C'est-à-dire qu'il normalise les chaînes HTTP paquet par paquet et ne peut traiter que les chaînes HTTP qui ont été réassemblées par le préprocesseur de flux TCP.

fast_blocking

Parmi les options de configuration globales pour le préprocesseur HTTP Inspect, l'option fast_blocking a été introduite à partir de la version Snort 2.9.16.0. Cette option permet l'inspection des données HTTP avant l'effacement des données. Cela permet une évaluation précoce des règles IPS de sorte que les règles de blocage soient appliquées et que la connexion soit bloquée au plus tôt au lieu de la bloquer après avoir effacé les données. Cette configuration est effective uniquement lorsque la normalisation en ligne est activée.

Pour activer l'option fast_blocking, vous devez utiliser une politique d'analyse de réseau avec la détection maximale comme politique de base.

Options globales de normalisation HTTP

Les options HTTP globales fournies pour le préprocesseur HTTP Inspect contrôlent le fonctionnement du préprocesseur. Utilisez ces options pour activer ou désactiver la normalisation HTTP lorsque des ports non spécifiés comme ports de serveur Web reçoivent le trafic HTTP.

Tenez compte des points suivants :

- Si vous activez **Unlimited Decompression** (décompression illimitée), les options de **profondeur maximale compressée** et de **profondeur maximale décompressée** sont automatiquement définies à 65535 lorsque vous validez vos modifications.
- La valeur la plus élevée est utilisée lorsque les valeurs de la **Profondeur maximale des données compressées** ou de la **Profondeur maximale des données décompressées** varient en :
  - La politique d'analyse du réseau par défaut

- Toute autre politique d'analyse de réseau personnalisée appelée par les règles d'analyse de réseau dans la même politique de contrôle d'accès

Si aucune règle de préprocesseur n'est mentionnée dans les descriptions suivantes, l'option n'est associée à aucune règle de préprocesseur.

Détecter les serveurs HTTP irréguliers

Détecte le trafic HTTP envoyé vers ou reçu par les ports non spécifiés comme ports de serveur Web.

Remarque Si vous activez cette option, assurez-vous de répertorier tous les ports qui reçoivent le trafic HTTP dans un profil de serveur dans la page de configuration HTTP. Si vous ne le faites pas et que vous activez cette option et la règle de préprocesseur qui l'accompagne, le trafic normal à destination et en provenance du serveur générera des événements. Le profil de serveur par défaut contient tous les ports normalement utilisés pour le trafic HTTP, mais si vous avez modifié ce profil, vous devrez peut-être ajouter ces ports à un autre profil pour empêcher la génération d'événements.

Vous pouvez activer la règle 120:1 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Détecter les serveurs mandataires HTTP

Détecte le trafic HTTP à l'aide de serveurs mandataires non définis par l'option **Allow HTTP Proxy Use** (autoriser l'utilisation du serveur mandataire HTTP).

Vous pouvez activer la règle 119:17 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Profondeur maximale des données compressées

Définit la taille maximale des données compressées à décompresser lorsque l' **inspection des données compressées** (et, le cas échéant, la **décompression du fichier SWF (LZMA)**, la **décompression du fichier SMF (Dégonfler)** ou **la décompression du fichier PDF (Dégonfler)**) est activée.

Profondeur maximale des données décompressées

Définit la taille maximale des données décompressées normalisées lorsque l'**inspection des données compressées** (et, le cas échéant, la **décompression du fichier SWF (LZMA)**, la **décompression du fichier STF (dégonfler)** ou la **décompression du fichier PDF (Dégonfler)**) est activée.

Options de normalisation HTTP au niveau du serveur

Vous pouvez définir des options au niveau du serveur pour chaque serveur que vous surveillez, globalement pour tous les serveurs ou pour une liste de serveurs. En outre, vous pouvez utiliser un profil de serveur prédéfini pour définir ces options, ou vous pouvez les définir individuellement pour répondre aux besoins de votre environnement. Utilisez ces options, ou l'un des profils par défaut qui définissent ces options, pour spécifier les ports du serveur HTTP dont vous souhaitez normaliser le trafic, la quantité de charge utile de réponse du serveur que vous souhaitez normaliser et les types de codage que vous souhaitez normaliser.

Si aucune règle de préprocesseur n'est mentionnée dans les descriptions suivantes, l'option n'est associée à aucune règle de préprocesseur.

Réseaux

Utilisez cette option pour préciser l'adresse IP d'un ou de plusieurs serveurs. Vous pouvez spécifier une adresse IP unique, ou un bloc d'adresses, ou une liste séparée par des virgules composée de l'un ou des deux.

En plus d'une limite de 255 profils au total, y compris le profil par défaut, vous pouvez inclure jusqu'à 496 caractères, soit environ 26 entrées, dans une liste de serveurs HTTP et spécifier un total de 256 entrées d'adresses pour tous les profils de serveur.

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Notez que le paramètre par `défaut` de la politique par défaut spécifie toutes les adresses IP de votre segment de réseau surveillé qui ne sont pas couvertes par une autre politique basée sur la cible. Par conséquent, vous ne pouvez pas et n'avez pas besoin de spécifier une adresse IP ou une longueur de bloc ou de préfixe CIDR pour la politique par défaut, et vous ne pouvez pas laisser ce paramètre vide dans une autre politique ou utiliser la notation de l'adresse pour représenter `toute` (par exemple, 0.0.0.0/0 ou:/0).

Ports

Les ports dont le trafic HTTP est normalisé par le moteur du préprocesseur. Séparez les valeurs de ports multiples par des virgules

Longueur de répertoire surdimensionné

Détecte les répertoires URL dont la longueur est supérieure à la valeur spécifiée.

Vous pouvez activer la règle 119:15 to générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque le préprocesseur détecte une demande pour une URL plus longue que la longueur spécifiée.

Profondeur du flux du client

Spécifie le nombre d'octets que les règles doivent inspecter dans les paquets HTTP bruts, y compris les données d'en-tête et de charge utile, dans le trafic HTTP côté client défini dans la section **Ports**. La profondeur de flux du client ne s'applique pas lorsque les options de règle de contenu HTTP d'une règle inspectent des parties spécifiques d'un message de demande.

Précisez l'un des éléments suivants :

- Une valeur positive inspecte le nombre d'octets spécifié dans le premier paquet. Si le premier paquet contient moins d'octets que spécifié, inspecte le paquet entier. Notez que la valeur spécifiée s'applique aux paquets segmentés et réassemblés.

  Notez également qu'une valeur de 300 élimine généralement l'inspection des témoins HTTP volumineux qui s'affichent à la fin de nombreux en-têtes de requêtes des clients.

- 0 inspecte tout le trafic côté client, y compris plusieurs paquets dans une session et le dépassement de la limite supérieure d'octets si nécessaire. Notez que cette valeur est susceptible d'affecter les performances.
- La commande -1 ignore tout le trafic côté client.

Profondeur du flux du serveur

Spécifie le nombre d'octets que les règles doivent inspecter dans les paquets HTTP bruts dans le trafic HTTP côté serveur spécifié par les **ports**. L'inspection comprend l'en-tête brut et la charge utile lorsque **Inspect HTTP Responses** (Inspecter les réponses HTTP) est désactivé et uniquement le corps de la réponse brut lorsque **Inspect HTTP Responses** est activé.

La profondeur de flux du serveur spécifie le nombre d'octets de données de réponse brutes du serveur dans une session en vue d'une inspection par les règles dans le trafic HTTP côté serveur défini dans la section **Ports**. Vous pouvez utiliser cette option pour équilibrer les performances et le niveau d'inspection des données de réponse du serveur HTTP. La profondeur de flux du serveur ne s'applique pas lorsque les options de contenu HTTP d'une règle inspectent des parties spécifiques d'un message de réponse.

Contrairement à la profondeur de flux du client, la profondeur de flux du serveur spécifie le nombre d'octets par réponse HTTP, et non par paquet de requête HTTP, que les règles doivent inspecter.

Vous pouvez définir l'un des éléments suivants :

- Une valeur positive :

  Lorsque **Inspecter les réponses HTTP** est **activé**, inspecte uniquement le corps brut de la réponse HTTP, et non les en-têtes HTTP bruts; inspecte également les données décompressées lorsque la fonction **Inspecter les données compressées** est activée.

  Lorsque **Inspecter les réponses HTTP** est **désactivé**, inspecte l'en-tête brut du paquet et la charge utile.

  Si la session comprend moins d'octets de réponse que spécifié, les règles inspectent entièrement tous les paquets de réponse dans une session donnée, sur plusieurs paquets selon les besoins. Si la session comprend plus d'octets de réponse que spécifié, les règles inspectent uniquement le nombre d'octets spécifié pour cette session, sur plusieurs paquets selon les besoins.

  Notez qu'une faible valeur de profondeur de flux peut provoquer de faux négatifs de la part des règles qui ciblent le trafic côté serveur défini dans la **section Ports**. La plupart de ces règles ciblent soit l'en-tête HTTP, soit le contenu susceptible de se trouver dans les environ 100 premiers octets des données non d'en-tête. Les en-têtes font généralement moins de 300 octets, mais leur taille peut varier.

  Notez également que la valeur spécifiée s'applique aux paquets segmentés et réassemblés.

- 0 inspecte le paquet entier pour tout le trafic côté serveur HTTP défini dans **Ports**, y compris les données de réponse dans une session qui dépasse 65535 octets.

  Notez que cette valeur est susceptible d'affecter les performances.

- -1 :

  Lorsque **Inspecter les réponses HTTP** est **activé**, inspecte uniquement les en-têtes HTTP bruts et non le corps de la réponse HTTP brut.

  Lorsque **Inspecter les réponses HTTP** est **désactivé**, ignore tout le trafic côté serveur défini dans **Ports.**

Longueur maximale de l'en-tête

Détecte un champ d'en-tête plus long que le nombre maximal d'octets dans une requête HTTP ; également dans les réponses HTTP lorsque **Inspecter les réponses HTTP** est activé. La valeur 0 désactive cette option. Spécifiez une valeur positive pour l'activer.

Vous pouvez activer la règle 119:19 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion..

Nombre maximal d'en-têtes

Détecte quand le nombre d'en-têtes dépasse ce paramètre dans une requête HTTP. La valeur 0 désactive cette option. Spécifiez une valeur positive pour l'activer.

Vous pouvez activer la règle 119:20 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion..

Nombre maximum d'espaces

Détecte lorsque le nombre d'espaces dans une ligne repliée est égal ou supérieur à ce paramètre dans une requête HTTP. La valeur 0 désactive cette option. Spécifiez une valeur positive pour l'activer.

Vous pouvez activer la règle 119:26 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion..

Profondeur d'extraction du corps du client HTTP

Spécifie le nombre d'octets à extraire du corps du message d'une requête client HTTP. Vous pouvez utiliser une règle d'intrusion pour inspecter les données extraites en sélectionnant le mot-clé `content` ou `protected_content` de l'option **HTTP Client Body** (Corps client HTTP).

Spécifiez -1 pour ignorer le corps client. Spécifiez 0 pour extraire le corps client entier. Notez que l'identification d'octets spécifiques à extraire peut améliorer les performances du système. Notez également que vous devez spécifier une valeur supérieure ou égale à 0 pour l'option **HTTP Client Body** (corps du client HTTP) fonctionne dans une règle de prévention des intrusions.

Petit bloc

Spécifie le nombre maximum d'octets à partir duquel un bloc est considéré comme petit. Spécifiez une valeur positive. La valeur 0 désactive la détection des petits fragments consécutifs anormaux. Consultez l'option **Petits fragments consécutifs** pour plus d'informations.

Petits blocs consécutifs

Spécifie combien de petits fragments consécutifs représentent un nombre anormalement élevé dans le trafic client ou serveur qui utilise le codage de transfert en fragments. L'option **Small Chunk Size** spécifie la taille maximale d'un petit fragment.

Par exemple, réglez la **taille des petits fragments** à 10 et la **taille des petits fragments consécutifs** à 5 pour détecter 5 fragments consécutifs de 10 octets ou moins.

Vous pouvez activer la règle de préprocesseur 119:27 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés sur les petits fragments dans le trafic client, et la règle 120:7 dans le trafic du serveur. Lorsque l'option **Small Chunk Size** (taille des petits fragments) est activée et que cette option est définie sur 0 ou 1, l'activation de ces règles déclenche un événement sur chaque bloc de la taille spécifiée ou moins.

Méthode HTTP

Spécifie les méthodes de requête HTTP en plus de GET et POST que vous vous attendez à ce que le système rencontre dans le trafic. Utiliser une virgule pour séparer plusieurs valeurs.

Les règles de prévention des intrusions utilisent le mot-clé `content` ou `protected_content` avec l'argument **HTTP Method** (Méthode HTTP) pour rechercher du contenu dans les méthodes HTTP. Vous pouvez activer la règle 119:31 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsqu'une méthode autre que GET, POST ou une méthode configurée pour cette option est rencontrée dans le trafic. Consultez Définition des états des règles d'intrusion.

Aucune alerte

Désactive les incidents d'intrusion lorsque les règles de préprocesseur associées sont activées.

Remarque Cette option ne désactive **pas** les règles de texte standard HTTP et les règles d'objet partagé.

Normaliser les en-têtes HTTP

Lorsque **Inspect HTTP Responses** (Inspecter les réponses HTTPt) est activé, permet la normalisation des données autres que les témoins dans les en-têtes de demande et de réponse. Lorsque **Inspect HTTP Responses** n'est **pas** activé, active la normalisation de l'ensemble de l'en-tête HTTP, y compris les témoins, dans les en-têtes de demande et de réponse.

Inspecter les témoins HTTP

Active l'extraction des témoins des en-têtes de requête HTTP. Active également l'extraction des données définies par les témoins à partir des en-têtes de réponse lorsque l'option **Inspect HTTP Responses** est activée. La désactivation de cette option lorsque l'extraction de témoin n'est pas requise peut améliorer les performances.

Notez que les noms d'en-tête `Cookie:` et `Set-Cookie` :, les espaces au début de la ligne d'en-tête et le `CRLF` qui termine la ligne d'en-tête sont inspectés dans le cadre de l'en-tête et non dans le cadre du témoin.

Normaliser les témoins dans les en-têtes HTTP

Active la normalisation des témoins dans les en-têtes de requête HTTP. Lorsque **Inspect HTTP Responses** est activé, permet également la normalisation des données des témoins définis dans les en-têtes de réponse. Vous devez sélectionner **Inspect HTTP cookies** Inspecter les témoins HTTP) avant de sélectionner cette option.

Autoriser l'utilisation du serveur mandataire HTTP

Permet au serveur Web surveillé d'être utilisé comme serveur mandataire HTTP. Cette option est utilisée uniquement pour l'inspection des requêtes HTTP.

Inspecter uniquement l'URI

Inspecte uniquement la partie URI du paquet de requête HTTP normalisé.

Inspecter les réponses HTTP

Active l'inspection étendue des réponses HTTP afin que, en plus de décoder et de normaliser les messages de requête HTTP, le préprocesseur extrait les champs de réponse pour inspection par le moteur de règles. L'activation de cette option permet au système d'extraire l'en-tête, le corps, le code d'état, etc. de la réponse, et il extrait également les données set-cookie lorsque la fonction **Inspecter les témoins HTTP** est activée.

Vous pouvez activer les règles 120:2 et 120:3 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, comme suit:

Tableau 6 : Règles Inspecter les réponses HTTP

Cette règle...	Se déclenche quand...
120:2	un code d'état de réponse HTTP non valide se produit.
120:3	une réponse HTTP n'inclut pas Content-Length ou Transfer-Encoding.

Normaliser les encodages UTF en UTF-8

Lorsque **Inspect HTTP Responses** est activé, détecte les encodages UTF-16LE, UTF-16BE, UTF-32LE et UTF32-BE dans les réponses HTTP et les normalise à UTF-8.

Vous pouvez activer la règle 120:4 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque la normalisation UTF échoue.

Inspecter les données compressées

Lorsque **Inspect HTTP Responses** (Inspecter les réponses HTTP) est activé, cette option permet la décompression des données compressées compatibles avec gzip et deflate dans le corps de la réponse HTTP et l'inspection des données décompressées normalisées. Le système inspecte les données de réponse HTTP avec et sans grappe. Le système inspecte plusieurs paquets, au besoin, les données décompressées, paquet par paquet; c'est-à-dire que le système ne combine pas les données décompressées de différents paquets pour l'inspection. La décompression se termine lorsque la **profondeur maximale des données compressées**, la **profondeur maximale des données décompressées** ou la fin des données compressées est atteinte. L'inspection des données décompressées se termine lorsque **la profondeur de flux du serveur** est atteinte, sauf si vous sélectionnez également **Unlimited Decompression** (Décompression illimitée). Vous pouvez utiliser le mot-clé de la règle `file_data` pour inspecter les données décompressées.

Vous pouvez activer les règles 120:6 et 120:24 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, comme suit :

Tableau 7 : Inspecter les règles de réponse HTTP compressées

Cette règle...	Se déclenche quand...
120:6	la décompression d'une réponse HTTP compressée échoue.
120:24	la décompression partielle d'une réponse HTTP compressée échoue.

Décompression illimitée

Lorsque **la fonction Inspecter les données comprimées** (et, facultativement, **Décompresser le fichier SMF (LZMA)**, **décompresser le fichier SWA (dépression)** ou **Décompresser le fichier PDF (dépression)**) est activée, remplace **la profondeur maximale des données décompressées** sur plusieurs paquets; C'est-à-dire que cette option active une décompression illimitée sur plusieurs paquets. Notez que l'activation de cette option n'affecte pas la **profondeur maximale des données compressées** ni la **profondeur maximale des données décompressées** dans un seul paquet. (L'activation de cette option définit la **profondeur maximale des données compressées** et la **profondeur maximale des données décompressées** à 65535 pendant la validation)

Normaliser JavaScript

Lorsque **Inspect HTTP Responses** (Inspecter les réponses HTTP) est activé, cette option permet la détection et la normalisation de Javascript dans le corps de la réponse HTTP. Le préprocesseur normalise les données Javascript brouillées, telles que les fonctions unescape et decodeURI et la méthode String.fromCharCode Le préprocesseur normalise les encodages suivants dans les fonctions unescape, decodeURI, et decodeURIComponent :

- %XX
- %uXXXX
- 0xXX
- \xXX
- \uXXXX

Le préprocesseur détecte les espaces consécutifs et les normalise en un seul espace. Lorsque cette option est activée, un champ de configuration vous permet de spécifier le nombre maximal d'espaces consécutifs à autoriser dans les données Javascript brouillées. Vous pouvez entrer une valeur comprise entre 1 et 65 535. La valeur 0 désactive la génération d'événements, peu importe que la règle de préprocesseur (120:10) associée à ce champ soit activée ou non.

Le préprocesseur normalise également l'opérateur Javascript plus (+) et concatène les chaînes à l'aide de l'opérateur.

Vous pouvez utiliser le mot-clé de règle de prévention des intrusions `file_data` pour pointer les règles de prévention des intrusions vers les données Javascript normalisées.

Vous pouvez activer les règles 120:9, 120:10 et 120:11 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, comme suit :

Tableau 8 : Normaliser les règles d'option Javascript

Cette règle...	Se déclenche quand...
120:9	le niveau d'obscurcissement dans le préprocesseur est supérieur ou égal à 2.
120:10	le nombre d'espaces consécutifs dans les données Javascript masquées est supérieur ou égal à la valeur configurée pour le nombre maximal d'espaces consécutifs autorisé.
120:11	les données échappées ou codées comprennent plus d'un type de codage.

Décompression du fichier SWA (LZMA) et décompression du fichier SWA (dépression)

Lorsque **HTTP Inspect Responses** (Inspecter les réponses HTTP) est activée, ces options décompressent les parties compressées des fichiers situés dans le corps de la réponse HTTP des requêtes HTTP.

Remarque Vous pouvez **uniquement** décompresser les parties compressées des fichiers trouvés dans les réponses HTTP GET.

- La **décompression du fichier SMF (LZMA)** décompresse les parties compressées compatibles avec LZMA des fichiers d'Adobe ShockWave Flash (`.Swf`).
- La **décompression du fichier SWA (dépression)** décompresse les parties compressées compatibles avec la décompression des fichiers ShockWave Flash d'Adobe (`.Swf`).

La décompression se termine lorsque la **profondeur maximale des données compressées**, la **profondeur maximale des données décompressées** ou la fin des données compressées est atteinte. L'inspection des données décompressées se termine lorsque **la profondeur de flux du serveur** est atteinte, sauf si vous sélectionnez également **Unlimited Decompression** (Décompression illimitée). Vous pouvez utiliser le mot-clé de règle de prévention des intrusions `file_data` pour inspecter les données décompressées.

Vous pouvez activer les règles 120:12 et 120:13 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, comme suit :

Tableau 9 : Règles d'option de décompression de fichier SWA

Cette règle...	Se déclenche quand...
120:12	Échec de la décompression du fichier
120:13	Échec de la décompression du fichier LZMA.

Décompresser le fichier PDF (Deflate)

Lorsque l'option **Inspecter les réponses HTTP** est activée, **Décompresser les fichiers PDF (Dépression)** décompresse les parties compressées compatibles avec la dépression des fichiers Portable Document Format (`.pdf`) situés dans le corps de la réponse HTTP des requêtes HTTP. Le système peut uniquement décompresser les fichiers PDF avec le filtre de flux `/FlateDecode`. Les autres filtres de flux (y compris `/FlateDecode /FlateDecode`) ne sont pas pris en charge.

Remarque Vous pouvez **uniquement** décompresser les parties compressées des fichiers trouvés dans les réponses HTTP GET.

La décompression se termine lorsque la **profondeur maximale des données compressées**, la **profondeur maximale des données décompressées** ou la fin des données compressées est atteinte. L'inspection des données décompressées se termine lorsque **la profondeur de flux du serveur** est atteinte, sauf si vous sélectionnez également **Unlimited Decompression** (Décompression illimitée). Vous pouvez utiliser le mot-clé de règle de prévention des intrusions `file_data` pour inspecter les données décompressées.

Vous pouvez activer les règles 120:14, 120:15, 120:16 et 120:17 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, comme suit :

Tableau 10 : Règles de l'option de décompression des fichiers PDF (Dépression)

Cette règle...	Se déclenche quand...
120:14	échec de la décompression du fichier
120:15	la décompression du fichier échoue en raison d'un type decompression non pris en charge.
120:16	la décompression du fichier échoue en raison d'un filtre de flux PDF non pris en charge.
120:17	l'analyse du fichier échoue.

Extraire l'adresse IP du client original

Permet l'examen des adresses IP du client d'origine lors de l'inspection des intrusions. Le système extrait l'adresse IP du client d'origine à partir des en-têtes X-Forwarded-For (XFF), True-Client-IP ou HTTP personnalisés que vous définissez dans l'option de **priorité d'en-tête XFF**. Vous pouvez afficher l'adresse IP du client d'origine extraite dans le tableau des incidents d'intrusion.

Vous pouvez activer les règles 119:23, 119:29 et 119:30 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion..

Priorité d'en-tête XFF

Précise l'ordre dans lequel le système traite les en-têtes IP du client d'origine lorsque plusieurs en-têtes sont présents dans une requête HTTP. Par défaut, le système examine les en-têtes X-Forwarded-For (XFF), puis les en-têtes True-Client-IP. Utilisez les icônes de flèches vers le haut et vers le bas à côté de chaque type d'en-tête pour ajuster sa priorité.

Cette option vous permet également de spécifier des en-têtes IP du client d'origine autres que XFF ou True-Client-IP pour l'extraction et l'évaluation. Cliquez sur **Add** (ajouter) pour ajouter des noms d'en-tête personnalisés à la liste de priorités. Le système prend uniquement en charge les en-têtes personnalisés qui utilisent la même syntaxe qu'un en-tête XFF ou True-Client-IP.

Gardez à l'esprit les éléments suivants lors de la configuration de cette option :

- Le système utilise cet ordre de priorité lors de l'évaluation des en-têtes d'adresses IP du client d'origine pour le contrôle d'accès et l'inspection des intrusions.
- Si plusieurs en-têtes IP du client d'origine sont présents, le système traite uniquement l'en-tête ayant la priorité la plus élevée.
- L'en-tête XFF contient une liste d'adresses IP, qui représentent les serveurs proxy par lesquels la demande est passée. Pour éviter l'usurpation d'usurpation, le système utilise la dernière adresse IP de la liste (c'est-à-dire l'adresse ajoutée par le proxy de confiance) comme adresse IP du client d'origine.

Enregistrer l'URI

Active l'extraction de l'URI brut, le cas échéant, des paquets de requête HTTP et associe l'URI à tous les incidents d'intrusion générés pour la session.

Lorsque cette option est activée, vous pouvez afficher les cinquante premiers caractères de l'URI extrait dans la colonne HTTP URI de la vue du tableau des incidents d'intrusion. Vous pouvez afficher l'URI complet, jusqu'à 2 048 octets, dans la vue des paquets.

Enregistrer le nom d'hôte

Active l'extraction du nom d'hôte, le cas échéant, de l'en-tête Host de la requête HTTP et associe le nom d'hôte à tous les incidents d'intrusion générés pour la session. Lorsque plusieurs en-têtes Host sont présents, extrait le nom d'hôte du premier en-tête.

Lorsque cette option est activée, vous pouvez afficher les cinquante premiers caractères du nom d'hôte extrait dans la colonne HTTP Hostname du tableau des incidents d'intrusion. Vous pouvez afficher le nom d'hôte complet, jusqu'à 256 octets, dans la vue des paquets.

Vous pouvez activer la règle 119:25 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Notez que, lorsqu'elle est activée, la règle 119:24 se déclenche si elle détecte plusieurs en-têtes Host dans une requête HTTP, quel que soit le paramètre de cette option.

Profil

Spécifie les types de codage normalisés pour le trafic HTTP. Le système fournit un profil par défaut approprié pour la plupart des serveurs, des profils par défaut pour les serveurs Apache et IIS, et des paramètres par défaut personnalisés que vous pouvez adapter pour répondre aux besoins de votre trafic surveillé :

- Sélectionnez **All** pour utiliser le profil standard par défaut, approprié pour tous les serveurs.
- Sélectionnez **IIS** pour utiliser le profil IIS fourni par le système.
- Sélectionnez **Apache** pour utiliser le profil Apache fourni par le système.
- Sélectionnez **Personnalisé** pour créer votre propre profil de serveur.

Options de codage de la normalisation HTTP au niveau du serveur

Lorsque vous définissez l'option de **profil** de niveau serveur HTTP sur `Personnalisé`, vous pouvez préciser les types de codage normalisés pour le trafic HTTP et activer les règles de préprocesseur HTTP afin de générer des événements pour le trafic contenant les différents types de codage.

Si aucune règle de préprocesseur n'est mentionnée dans les descriptions suivantes, l'option n'est associée à aucune règle de préprocesseur.

Encodage ASCII

Décode les caractères ASCII codés et spécifie si le moteur de règles génère un événement sur les URI codées en ASCII.

Vous pouvez activer la règle 119:1 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Encodage UTF-8

Décode les séquences Unicode UTF-8 standard dans l'URI.

Vous pouvez activer la règle 119:6 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Encodage Microsoft %U

Décode le schéma de codage IIS %u qui utilise %u suivi de quatre caractères, où les 4 caractères sont une valeur codée hexadécimale en corrélation avec un point de code Unicode IIS.

Astuces Les clients légitimes utilisent rarement les encodages %u, c'est pourquoi Cisco recommande de décoder le trafic HTTP codé avec des codages %u.

Vous pouvez activer la règle 119:3 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Encodage Bare Byte UTF-8

Décode l'encodage des octets nus, qui utilise des caractères non-ASCII comme valeurs valides pour le décodage des valeurs UTF-8.

Astuces Le codage de l'octet nu permet à l'utilisateur d'émuler un serveur IIS et d'interpréter correctement les codages non standard. Cisco recommande d'activer cette option, car aucun client légitime ne code l'UTF-8 de cette façon.

Vous pouvez activer la règle 119:4 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Encodage Microsoft IIS

Décode à l'aide du mappage de point de code Unicode.

Astuces Cisco recommande d'activer cette option, car elle est principalement observée dans les attaques et les tentatives d'évitement.

Vous pouvez activer la règle 119:7 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Double encodage

Décode le trafic IIS doublement codé en effectuant deux passages dans l'URI de demande qui exécute le décodage de celui-ci. Cisco recommande d'activer cette option, car elle ne se trouve généralement que dans les scénarios d'attaque.

Vous pouvez activer la règle 119:2 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Obscurcissement à multiples barres obliques

Normalise plusieurs barres obliques d'affilée en une seule barre oblique.

Vous pouvez activer la règle 119:8 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Obscurcissement IIS à barre oblique inversée

Normalise les barres obliques inverses en barres obliques.

Vous pouvez activer la règle 119:9 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Répertoire des traverses

Normalise les traversées de répertoires et les répertoires autoréférentiels. Si vous activez les règles de préprocesseur associées pour générer des événements par rapport à ce type de trafic, des faux positifs peuvent être générés, car certains sites Web font référence à des fichiers en utilisant des traversées de répertoire.

Vous pouvez activer les règles 119:10 et 119:11 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Obscurcissement d'onglet

Normalise la norme non-RFC de l'utilisation d'une tabulation comme délimiteur d'espace. Apache et les autres serveurs Web autres que IIS utilisent la tabulation (0x09) comme délimiteur dans les URL.

Remarque Quelle que soit la configuration de cette option, le préprocesseur de HTTP Inspect traite une tabulation comme un espace si un espace (0x20) le précède.

Vous pouvez activer la règle 119:12 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Délimiteur de RFC non valide

Normalise les sauts de ligne (\n) dans les données d'URI.

Vous pouvez activer la règle 119:13 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Traversée de répertoire Webroot

Détecte les traversées de répertoires qui dépassent le répertoire initial dans l'URL.

Vous pouvez activer la règle 119:18 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Délimiteur d'onglet URI

Active l'utilisation de la tabulation (0x09) comme délimiteur pour un URI. Apache, les versions plus récentes d'IIS et certains autres serveurs Web utilisent la tabulation comme délimiteur dans les URL.

Remarque Quelle que soit la configuration de cette option, le préprocesseur de HTTP Inspect traite une tabulation comme un espace si un espace (0x20) le précède.

Caractères non RFC

Détecte la liste de caractères non-RFC que vous ajoutez dans le champ correspondant lorsqu'elle apparaît dans les données URI entrantes ou sortantes. Lorsque vous modifiez ce champ, utilisez le format hexadécimal qui représente le caractère octet. Si vous configurez cette option, définissez sa valeur avec précaution. L'utilisation d'un caractère très courant pourrait vous submerger d'événements.

Vous pouvez activer la règle 119:14 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Taille maximale de l'encodage de bloc

Détecte des tailles de blocs anormalement grandes dans les données d'URI.

Vous pouvez activer les règles 119:16 et 119:22 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Désactiver le décodage du pipeline

Désactive le décodage HTTP pour les demandes en pipeline. Lorsque cette option est désactivée, les performances sont améliorées, car les requêtes HTTP en attente dans le pipeline ne sont pas décodées ou analysées et sont uniquement inspectées à l'aide de la mise en correspondance de schémas génériques.

Analyse non stricte de l'URI

Active l'analyse non stricte des URI. Utilisez cette option uniquement sur les serveurs qui acceptent les URI non standard au format « GET /index.html abc ko qr \n ». En utilisant cette option, le décodeur suppose que l'URI est entre le premier et le deuxième espace, même s'il n'y a pas d'identifiant HTTP valide après le deuxième espace.

Encodage ASCII étendu

Active l'analyse des caractères ASCII étendus dans une URI de requête HTTP. Notez que cette option est disponible uniquement dans les profils de serveur personnalisés, et non dans les profils par défaut fournis pour Apache, IIS ou tous les serveurs.

Sujets connexes

Présentation : Contenu HTTP et arguments du mot-clé protected_content
Le mot-clé file_data

Configuration du préprocesseur d'inspection HTTP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Avant de commencer

- Confirmez que les réseaux que vous souhaitez identifier dans une politique basée sur la cible personnalisée correspondent ou constituent un sous-ensemble des réseaux, des zones et des VLAN gérés par sa politique d'analyse de réseau parente. Consultez Paramètres avancés pour les politiques d'analyse de réseau pour obtenir de plus amples renseignements.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si la **configuration HTTP** est désactivée sous **Préprocesseurs de la couche applicative**, cliquez sur **Enabled** (Activée).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Configuration HTTP**.

Étape 7 Modifiez les options de la zone de page Global Settings (paramètres globaux). voir Options globales de normalisation HTTP, à la page 27.

Étape 8 Vous avez trois possibilités :

- Add a server profile (ajouter un profil de serveur) : cliquez sur **Ajouter** (+) dans la section **Servers** (Serveurs). Précisez une ou plusieurs adresses IP pour le client dans le champ **Server Address** (adresse du serveur), puis cliquez sur **OK**. Vous pouvez spécifier une adresse IP unique, ou bloc d'adresses, ou une liste de ces deux éléments (séparés par des virgules) ou des deux. Vous pouvez inclure jusqu'à 496 caractères dans une liste, spécifier un total de 256 entrées d'adresses pour tous les profils de serveur et créer un total de 255 profils, y compris le profil par défaut.
- Edit a server Profile (modifier un profil de serveur) : cliquez sur l'adresse configurée pour un profil que vous avez ajouté sous **Servers** (serveurs), ou cliquez sur **Default** (par défaut). Vous pouvez modifier n'importe quel paramètre dans la section **Configuration** ; voir Options de normalisation HTTP au niveau du serveur, à la page 28. Si vous choisissez **Personnalisé** pour la valeur de **profil**, vous pouvez également modifier les options de codage décrites dans Options de codage de la normalisation HTTP au niveau du serveur, à la page 37.
- Supprimer un profil de serveur : cliquez sur **Supprimer** (🗑) à côté d'un profil personnalisé.

Étape 9 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous voulez générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, activez les règles de préprocesseur HTTP (GID 119). Pour en savoir plus, consultez Définition des états des règles d'intrusion.
- Déployer les changements de configuration.

Sujets connexes

Gestion des couches
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions

Règles supplémentaires pour le préprocesseur d'inspection HTTP

Vous pouvez activer les règles de la colonne **Règle du préprocesseur GID:SID** du tableau suivant pour générer des événements pour les règles de préprocesseur HTTP Inspect qui ne sont pas associés à des options de configuration spécifiques.

Tableau 11 : Règles supplémentaires pour le préprocesseur d'inspection HTTP

GID de la règle de préprocesseur : SID	Se déclenche quand...
119:21	un en-tête de requête HTTP a plus d'un champ `de longueur de contenu`.
119:24	une requête HTTP comporte plusieurs en-têtes Host.
119:28	une méthode HTTP POST n'a ni en-tête `content-length` ni `transfer-encoding` en blocs.
119:32	HTTP version 0.9 rencontré dans le trafic. Notez que la configuration du flux TCP doit également être activée.
119:33	un URI HTTP comprend un espace non échappé.
119:34	une connexion TCP contient 24 requêtes HTTP ou plus en pipeline.
120:5	L'encodage UTF-7 est rencontré dans le trafic de réponse HTTP; UTF-7 ne doit s'afficher que lorsque la parité de 7 bits est requise, comme dans le trafic SMTP.
120:8	la `content-length` (longueur du contenu) ou la taille de bloc n'est pas valide.
120:18	une réponse du serveur HTTP précède la demande du client.
120:19	une réponse HTTP comprend plusieurs longueurs de contenu.

GID de la règle de préprocesseur : SID	Se déclenche quand...
120:20	une réponse HTTP comprend plusieurs encodages de contenu.
120:25	une réponse HTTP comprend un pli d'en-tête non valide.
120:26	une ligne indésirable se produit avant un en-tête de réponse HTTP.
120:27	une réponse HTTP n'inclut pas d'en-tête de fin.
120:28	une taille de bloc non valide se produit, ou la taille de bloc est suivie de caractères indésirables.

Le préprocesseur RPC de Sun

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

La normalisation des appels de procédure à distance (RPC) prend des enregistrements d'appels RPC fragmentés et les normalise en un seul enregistrement afin que le moteur de règles puisse inspecter l'enregistrement complet. Par exemple, un attaquant peut tenter de découvrir le port sur lequel s'exécute la commande RPC `admind`. Certains hôtes UNIX utilisent la commande RPC `admind` pour effectuer des tâches de système distribué à distance. Si l'hôte effectue une authentification faible, un utilisateur malveillant pourrait prendre le contrôle de l'administration à distance. La règle de texte standard (GID : 1) avec le ID de Snort (SID) 575 détecte cette attaque en recherchant le contenu dans des emplacements spécifiques pour identifier les demandes `portmap GETPORT` inappropriées.

Options du préprocesseur RPC de Sun

Ports

Précisez les ports dont vous souhaitez normaliser le trafic. Dans l'interface, répertoriez plusieurs ports séparés par des virgules. Les ports RPC typiques sont 111 et 32771. Si votre réseau envoie le trafic d'appels RPC vers d'autres ports, pensez à les ajouter.

Détecter les enregistrements RPC fragmentés

Détecter les enregistrements RPC fragmentés

Vous pouvez activer les règles 106:1 et 106:5 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Détecter plusieurs enregistrements dans un paquet

Détecte plus d'une requête RPC par paquet (ou paquet réassemblé).

Vous pouvez activer la règle 106:2 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Détecter les sommes d'enregistrement fragmentées qui dépassent un paquet

Détecte les longueurs d'enregistrement de fragments réassemblés qui dépassent la longueur de paquet actuelle.

Vous pouvez activer la règle 106:3 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Détecter les enregistrements à fragment unique dont la taille dépasse celle d'un paquet

Détecte les enregistrements partiels

Vous pouvez activer la règle 106:4 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Configuration du préprocesseur RPC de Sun

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si **la configuration RPC Sun** est désactivée sous **Application Layer Preprocessors** (Préprocesseurs de la couche applicative), cliquez sur **Enabled** (Activer).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Configuration Sun RPC**.

Étape 7 Modifiez les paramètres décrits enOptions du préprocesseur RPC de Sun, à la page 43.

Étape 8 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, activez les règles de préprocesseur RPC de Sun (GID 106). Pour en savoir plus, consultez Définition des états des règles d'intrusion.
- Déployer les changements de configuration.

Sujets connexes

Gestion des couches

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions

Le préprocesseur SIP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le protocole SIP (Session Initiation Protocol) permet d'établir, de modifier et de supprimer les sessions pour un ou plusieurs utilisateurs d'applications clientes telles que la téléphonie sur Internet, les conférences multimédias, la messagerie instantanée, les jeux en ligne et le transfert de fichiers. Un champ de *méthode* dans chaque requête SIP identifie l'objectif de la demande et un URI de demande précise où envoyer la demande. Un code d'état dans chaque réponse SIP indique le résultat de l'action demandée.

Une fois les appels établis à l'aide de SIP, le protocole RTP (Real-time Transport Protocol) est responsable des communications audio et vidéo ultérieures. cette partie de la session est parfois appelée canal d'appel, canal de données ou canal de données audio/vidéo. RTP utilise le protocole SDP (Session Description Protocol) dans le corps du message SIP pour la négociation des paramètres du canal de données, l'annonce de session et l'invitation à la session.

Le préprocesseur SIP est responsable de ce qui suit :

- décodage et analyse du trafic SIP 2.0
- extraction de l'en-tête SIP et le corps du message, y compris les données SDP, le cas échéant, et transmission des données extraites au moteur de règles pour une inspection plus approfondie
- génération des événements lorsque les conditions suivantes sont détectées et que les règles de préprocesseur correspondantes sont activées :
  - anomalies et vulnérabilités connues dans les paquets SIP
  - séquences d'appels dans le désordre et non valides
- ignorer le canal d'appel (facultatif)

Le préprocesseur identifie le canal RTP en fonction du port identifié dans le message SDP, qui est intégré dans le corps du message SIP, mais le préprocesseur ne fournit pas d'inspection de protocole RTP.

Tenez compte des éléments suivants lorsque vous utilisez le préprocesseur SIP :

- UDP achemine généralement les sessions multimédias prises en charge par SIP. Le prétraitement de flux UDP assure le suivi de session SIP pour le préprocesseur SIP.

- Les mots-clés de règles SIP vous permettent de pointer vers l'en-tête ou le corps du paquet SIP et de limiter la détection aux paquets pour des méthodes SIP ou des codes d'état spécifiques.

Options du préprocesseur SIP

Pour les options suivantes, vous pouvez spécifier une valeur positive comprise entre 1 et 65 535 octets, ou 0 afin de désactiver la génération d'événements pour l'option, que la règle associée soit activée ou non.

- **Longueur maximale de la demande d'URI**
- **Longueur maximale de l'ID d'appel**
- **Longueur maximale du nom de la demande**
- **Longueur maximale de l'origine**
- **Longueur maximale de la destination**
- **Longueur maximale de l'intermédiaire**
- **Longueur maximale du contact**
- **Longueur maximale du contenu**

Si aucune règle de préprocesseur n'est mentionnée dans les descriptions suivantes, l'option n'est associée à aucune règle de préprocesseur.

Ports

Spécifie les ports à inspecter pour le trafic SIP. Vous pouvez spécifier un nombre entier entre 0 et 65 535. Séparez les valeurs de ports multiples par des virgules

Méthodes à vérifier

Spécifie les méthodes SIP à détecter. Vous pouvez spécifier l'une des méthodes SIP actuellement définies suivantes :

```
ack, benotify, bye, cancel, do, info, invite, join, message,
notify, options, prack, publish, quath, refer, register,
service, sprack, subscribe, unsubscribe, update
```

Les méthodes sont insensibles à la casse. Le nom de la méthode peut inclure des caractères alphabétiques, des chiffres et le caractère de soulignement. Aucun autre caractère spécial n'est autorisé. Séparez les valeurs de ports multiples par des virgules.

Étant donné que de nouvelles méthodes SIP pourraient être définies à l'avenir, votre configuration peut inclure une chaîne alphabétique qui n'est pas définie actuellement. Le système prend en charge jusqu'à 32 méthodes, y compris les 21 méthodes actuellement définies et 11 autres méthodes. Le système ignore toutes les méthodes non définies que vous pourriez configurer.

Notez qu'en plus des méthodes que vous spécifiez pour cette option, les 32 méthodes au total comprennent les méthodes spécifiées à l'aide du mot-clé `sip_method` dans les règles de prévention des intrusions.

Nombre maximum de boîtes de dialogue dans une session

Spécifie le nombre maximal de boîtes de dialogue autorisé dans une session de flux. Si plus de boîtes de dialogue sont créées que ce nombre, les boîtes de dialogue les plus anciennes sont abandonnées jusqu'à ce que le nombre de boîtes de dialogue ne dépasse pas le nombre maximal spécifié. Vous pouvez spécifier un entier entre 1 et 4194303.

Vous pouvez activer la règle 140:27 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion.

Longueur maximale de la demande d'URI

Spécifie le nombre maximal d'octets à autoriser dans le champ d'en-tête Request-URI. Un URI générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés plus long lorsque la règle 140:3 est activée. Le champ URI de la demande indique le chemin ou la page de destination de la demande.

Longueur maximale de l'ID d'appel

Spécifie le nombre maximal d'octets à autoriser dans le champ d'en-tête Call-ID de la demande ou de la réponse. Un Call-ID générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés (Identifiant d'appel) plus long lorsque la règle 140:5 est activée. Le champ Call-ID identifie de manière unique la session SIP dans les demandes et les réponses.

Longueur maximale du nom de la demande

Spécifie le nombre maximal d'octets à autoriser dans le nom de la demande, qui est le nom de la méthode spécifiée dans l'identifiant de transaction CSeq. Un nom de requête générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés plus long lorsque la règle 140:7 est activée.

Longueur maximale de l'origine

Spécifie le nombre maximal d'octets à autoriser dans le champ d'en-tête From de la demande ou de la réponse. Un générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés d'origine plus long lorsque la règle 140:9 est activée. Le champ De identifie l'initiateur du message.

Longueur maximale de la destination

Spécifie le nombre maximal d'octets à autoriser dans le champ d'en-tête À de la demande ou de la réponse. Une durée À générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés plus longue lorsque la règle 140:11 est activée. Le champ À identifie le destinataire du message.

Longueur maximale de l'intermédiaire

Spécifie le nombre maximal d'octets à autoriser dans le champ d'en-tête Via de la demande ou de la réponse. Un Via générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés plus long lorsque la règle 140:13 est activée. Le champ Via fournit le chemin suivi par la demande et, dans une réponse, les informations de réception.

Longueur maximale du contact

Spécifie le nombre maximal d'octets à autoriser dans le champ d'en-tête Contact de la demande ou de la réponse. Un Contactgénérer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés plus long lorsque la règle 140:15 est activée. Le champ Contact fournit une URI qui spécifie l'emplacement à contacter pour les messages suivants.

Longueur maximale du contenu

Spécifie le nombre maximal d'octets à autoriser dans le contenu du corps du message de demande ou de réponse. Contenu plus long générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque la règle 140:16 est activée.

Ignorer le canal de données audio et vidéo

Active et désactive l'inspection du trafic du canal de données. Notez que le préprocesseur poursuit l'inspection du reste du trafic SIP non lié au canal de données lorsque vous activez cette option.

Sujets connexes

Mots-clés SIP

Configuration du préprocesseur SIP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si **la configuration SIP** est désactivée sous **Préprocesseurs de la couche d'application**, cliquez sur **Enabled** (activée).

Étape 6 Cliquez sur **Edit** (✎) à côté de **SIP Configuration** (Configuration SIP).

Étape 7 Modifiez les options décrites dans Options du préprocesseur SIP, à la page 46.

Étape 8 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, activez les règles de préprocesseur SIP (GID 140). Pour en savoir plus, consultez Définition des états des règles d'intrusion.
- Déployer les changements de configuration.

Sujets connexes

Gestion des couches

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions

Règles de préprocesseur SIP supplémentaires

Les règles de préprocesseur SIP dans le tableau suivant ne sont pas associées à des options de configuration spécifiques. Comme pour les autres règles de préprocesseur SIP, vous devez activer ces règles si vous souhaitez qu'elles générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés.

Tableau 12 : Règles de préprocesseur SIP supplémentaires

GID de la règle de préprocesseur : SID	Se déclenche quand...
1401	le préprocesseur surveille le nombre maximal de sessions SIP autorisées par le système.
140:2	le champ Request_URI obligatoire est vide dans une requête SIP.
140:4	le champ d'en-tête Call-ID est vide dans une demande ou une réponse SIP.
140:6	la valeur du numéro de séquence dans le champ CSeq de demande ou de réponse SIP n'est pas un entier non signé de 32 bits inférieur à 231.
140:8	le champ d'en-tête De est vide dans une demande ou réponse SIP.
140:10	le champ d'en-tête To (À) est vide dans une requête ou une réponse SIP.
140:12	le champ d'en-tête Via est vide dans une requête ou une réponse SIP
140:14	le champ d'en-tête Contact obligatoire est vide dans une demande ou une réponse SIP.
140:17	une seule demande SIP ou un seul paquet de réponse dans le trafic UDP contient plusieurs messages. Notez que les anciennes versions SIP prenaient en charge plusieurs messages, mais que SIP 2.0 ne prend en charge qu'un seul message par paquet.
140:18	la longueur réelle du corps du message dans une demande ou une réponse SIP dans un trafic UDP ne correspond pas à la valeur spécifiée dans le champ d'en-tête Content-Length (Longueur du contenu) d'une demande ou d'une réponse SIP.
140:19	le préprocesseur ne reconnaît pas de nom de méthode dans le champ CSeq d'une réponse SIP.
140:20	le serveur SIP ne conteste pas un message d'invitation authentifié. Notez que cela se produit dans le cas de l'attaque de facturation InviteReplay.

GID de la règle de préprocesseur : SID	Se déclenche quand...
140:21	les informations relatives à la session changent avant l'établissement de l'appel. Notez que cela se produit dans le cas de l'attaque de facturation FakeBusy.
140:22	le code d'état de réponse n'est pas un nombre à trois chiffres.
140:23	le champ d'en-tête Content-Type ne spécifie pas de type de contenu et le corps du message contient des données.
140:24	la version SIP n'est pas 1, 1.1 ou 2.0.
140:25	la méthode spécifiée dans l'en-tête CSeq et le champ méthode ne correspondent pas dans une requête SIP.
140:26	le préprocesseur ne reconnaît pas la méthode indiquée dans le champ de la méthode de requête SIP.

Le préprocesseur GTP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le protocole de tunnellisation GPRS (General Service Packet Radio) permet de communiquer sur un réseau central GTP. Le préprocesseur GTP détecte les anomalies dans le trafic GTP et transfère les messages de signalisation du canal de commande au moteur de règles pour inspection. Vous pouvez utiliser les mots-clés de règle `gtp_version`, `gtp_type` et `gtp_info` pour inspecter le trafic du canal de commande GTP à la recherche d'exploits.

Une seule option de configuration vous permet de modifier le paramètre par défaut des ports que le préprocesseur inspecte pour les messages du canal de commande GTP.

Règles de préprocesseur GTP

Vous devez activer les règles de préprocesseur GTP dans le tableau suivant si vous souhaitez les appliquer à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés.

Tableau 13 : Règles de préprocesseur GTP

GID de la règle de préprocesseur : SID	Description
143:1	Génère un événement lorsque le préprocesseur détecte une longueur de message non valide.
143:2	Génère un événement lorsque le préprocesseur détecte une longueur d'élément d'information non valide.

GID de la règle de préprocesseur : SID	Description
143:3	Génère un événement lorsque le préprocesseur détecte des éléments d'information qui ne sont pas dans l'ordre.

Configuration du préprocesseur GTP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Vous pouvez utiliser cette procédure pour modifier les ports que le préprocesseur GTP surveille pour les messages de commande GTP.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation à gauche.

Étape 5 Si la **configuration du canal de commande GTP** est désactivée sous **Préprocesseurs de la couche d'application**, cliquez sur **Enabled** (Activée).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Configuration du canal de commande GTP**.

Étape 7 Saisissez une valeur de **ports**.

Séparez les valeurs de ports multiples par des virgules.

Étape 8 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez activer les incidents d'intrusion, activez les règles de préprocesseur GTP (GID 143). Pour en savoir plus, consultez Définition des états des règles d’intrusion.
- Déployer les changements de configuration.

Le préprocesseur IMAP

Remarque Cette section s’applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le protocole IMAP (Internet Message Application Protocol) est utilisé pour récupérer les courriels d’un serveur IMAP distant. Le préprocesseur IMAP inspecte le trafic IMAP4 serveur à client et, lorsque les règles de préprocesseur associées sont activées, génère des événements sur le trafic anormal. Le préprocesseur peut également extraire et décoder les pièces jointes à un courriel dans le trafic IMAP4 client-serveur et envoyer les données des pièces jointes au moteur de règles. Vous pouvez utiliser le mot-clé `file_data` dans une règle de prévention des intrusions pour pointer vers les données de la pièce jointe.

L’extraction et le décodage comprennent plusieurs pièces jointes, le cas échéant, et les pièces jointes volumineuses qui s’étendent sur plusieurs paquets.

Options du préprocesseur IMAP

Notez que le déchiffrement, ou l’extraction lorsque la pièce jointe MIME ne nécessite pas de décodage, inclut plusieurs pièces jointes le cas échéant et des pièces jointes volumineuses qui s’étendent sur plusieurs paquets.

Notez également que la valeur la plus élevée est utilisée lorsque les valeurs des **Base64 Decoding Depth**, **7-Bit/8-Bit/Binary Decoding Depth**, **Quoted-Printable Decoding Depth**, ou **Unix-to-Unix Decoding Depth** sont différentes dans :

- La politique d’analyse du réseau par défaut
- Toute autre politique d’analyse de réseau personnalisée appelée par les règles d’analyse de réseau dans la même politique de contrôle d’accès

Si aucune règle de préprocesseur n’est mentionnée dans les descriptions suivantes, l’option n’est associée à aucune règle de préprocesseur.

Ports

Spécifie les ports à inspecter pour le trafic IMAP. Vous pouvez spécifier un nombre entier entre 0 et 65 535. Séparez les valeurs de ports multiples par des virgules

Profondeur de décodage en base 64

Spécifie le nombre maximal d’octets à extraire et à décoder de chaque pièce jointe de courriel MIME codée en Base64. Vous pouvez spécifier une valeur positive ou 0 pour décoder toutes les données Base64. Spécifiez -1 pour ignorer les données Base64.

Notez que les valeurs positives non divisibles par 4 sont arrondies au multiple supérieur de 4, sauf pour les valeurs 65533, 65534 et 65535, qui sont arrondies à 65532.

Lorsque cette option est activée, vous pouvez activer la règle 141:4 générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque le décodage échoue; Le décodage peut échouer, par exemple, en raison d'un encodage incorrect ou de données endommagées.

7 bits/8 bits/profondeur de décodage binaire

Spécifie le nombre maximal d'octets de données à extraire de chaque pièce jointe MIME de courriel qui ne nécessite pas de décodage. Ces types de pièces jointes comprennent des types de pièces jointes 7 bits, 8 bits, binaires et en plusieurs parties comme du texte brut, des images jpeg, des fichiers mp3, etc. Vous pouvez spécifier une valeur positive ou 0 pour extraire toutes les données du paquet. Spécifiez -1 pour ignorer les données non décodées.

Lorsque cette option est activée, vous pouvez activer la règle 141:6 générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque l'extraction échoue; L'extraction peut échouer, par exemple en raison de données endommagées

Profondeur de décodage Quoted-Printable

Spécifie le nombre maximum d'octets à extraire et à décoder de chaque pièce jointe MIME de courriel codée en quoted-printable (QP). Vous pouvez spécifier une valeur positive ou 0 pour décoder toutes les données codées QP du paquet. Spécifiez -1 pour ignorer les données codées QP.

Lorsque cette option est activée, vous pouvez activer la règle 141:5 générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque le décodage échoue; Le décodage peut échouer, par exemple, en raison d'un encodage incorrect ou de données endommagées.

Profondeur de décodage Unix-à-Unix

Spécifie le nombre maximal d'octets à extraire et à décoder de chaque pièce jointe de courriel encodée Unix à Unix (uuencoded). Vous pouvez spécifier une valeur positive ou 0 pour décoder toutes les données uuencodées dans le paquet. Spécifiez -1 pour ignorer les données uuencodées.

Lorsque cette option est activée, vous pouvez activer la règle 141:7 générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque le décodage échoue; Le décodage peut échouer, par exemple, en raison d'un encodage incorrect ou de données endommagées.

Sujets connexes

Le mot-clé file_data

Configuration du préprocesseur IMAP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si **la configuration IMAP** est désactivée sous **Préprocesseurs de la couche d'application**, cliquez sur **Enabled** (Activée).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Configuration IMAP**.

Étape 7 Modifiez les paramètres décrits enOptions du préprocesseur IMAP, à la page 52.

Étape 8 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez activer les incidents d'intrusion, activez les règles de préprocesseur IMAP (GID 141). voir Définition des états des règles d'intrusion.
- Déployer les changements de configuration.

Sujets connexes

Couches des politiques d'analyse des réseaux et de prévention des intrusions
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions

Règles de préprocesseur IMAP supplémentaires

Les règles de préprocesseur IMAP dans le tableau suivant ne sont pas associées à des options de configuration spécifiques. Comme pour les autres règles de préprocesseur IMAP, vous devez activer ces règles si vous souhaitez qu'elles générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés.

Tableau 14 : Règles de préprocesseur IMAP supplémentaires

GID de la règle de préprocesseur : SID	Description
1411	Génère un événement lorsque le préprocesseur détecte une commande client qui n'est pas définie dans la RFC 3501.
141:2	Génère un événement lorsque le préprocesseur détecte une réponse du serveur qui n'est pas définie dans la RFC 3501.
1413	Génère un événement lorsque le préprocesseur utilise la quantité maximale de mémoire autorisée par le système. À ce stade, le préprocesseur arrête le décodage jusqu'à ce que la mémoire se libère.

Le préprocesseur POP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le protocole POP (post Office Protocol) est utilisé pour récupérer les courriels d'un serveur de messagerie POP distant. Le préprocesseur POP inspecte le trafic POP3 serveur à client et, lorsque les règles de préprocesseur associées sont activées, génère des événements sur le trafic anormal. Le préprocesseur peut également extraire et décoder les pièces jointes dans le trafic POP3 client-serveur et envoyer les données des pièces jointes au moteur de règles. Vous pouvez utiliser le mot-clé `file_data` dans une règle de prévention des intrusions pour pointer vers les données de la pièce jointe.

L'extraction et le décodage comprennent plusieurs pièces jointes, le cas échéant, et les pièces jointes volumineuses qui s'étendent sur plusieurs paquets.

Options du préprocesseur POP

Notez que le déchiffrement, ou l'extraction lorsque la pièce jointe MIME ne nécessite pas de décodage, inclut plusieurs pièces jointes le cas échéant et des pièces jointes volumineuses qui s'étendent sur plusieurs paquets.

Notez également que la valeur la plus élevée est utilisée lorsque les valeurs des **Base64 Decoding Depth**, **7-Bit/8-Bit/Binary Decoding Depth**, **Quoted-Printable Decoding Depth**, ou **Unix-to-Unix Decoding Depth** sont différentes dans :

- La politique d'analyse du réseau par défaut
- Toute autre politique d'analyse de réseau personnalisée appelée par les règles d'analyse de réseau dans la même politique de contrôle d'accès

Si aucune règle de préprocesseur n'est mentionnée dans les descriptions suivantes, l'option n'est associée à aucune règle de préprocesseur.

Ports

Spécifie les ports à inspecter pour le trafic POP. Vous pouvez spécifier un nombre entier entre 0 et 65 535. Séparez les valeurs de ports multiples par des virgules

Profondeur de décodage en base 64

Spécifie le nombre maximal d'octets à extraire et à décoder de chaque pièce jointe de courriel MIME codée en Base64. Vous pouvez spécifier une valeur positive ou 0 pour décoder toutes les données Base64. Spécifiez -1 pour ignorer les données Base64.

Notez que les valeurs positives non divisibles par 4 sont arrondies au multiple supérieur de 4, sauf pour les valeurs 65533, 65534 et 65535, qui sont arrondies à 65532.

Lorsque cette option est activée, vous pouvez activer la règle 142:4 sur le générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque le décodage échoue; Le décodage peut échouer, par exemple, en raison d'un encodage incorrect ou de données endommagées.

7 bits/8 bits/profondeur de décodage binaire

Spécifie le nombre maximal d'octets de données à extraire de chaque pièce jointe MIME de courriel qui ne nécessite pas de décodage. Ces types de pièces jointes comprennent des types de pièces jointes 7 bits, 8 bits, binaires et en plusieurs parties comme du texte brut, des images jpeg, des fichiers mp3, etc. Vous pouvez spécifier une valeur positive ou 0 pour extraire toutes les données du paquet. Spécifiez -1 pour ignorer les données non décodées.

Lorsque cette option est activée, vous pouvez activer la règle 142:6 sur le générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque l'extraction échoue; L'extraction peut échouer, par exemple en raison de données endommagées.

Profondeur de décodage Quoted-Printable

Spécifie le nombre maximum d'octets à extraire et à décoder de chaque pièce jointe MIME de courriel codée en quoted-printable (QP). Vous pouvez spécifier une valeur positive ou 0 pour décoder toutes les données codées QP du paquet. Spécifiez -1 pour ignorer les données codées QP.

Lorsque cette option est activée, vous pouvez activer la règle 142:5 sur le générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque le décodage échoue; Le décodage peut échouer, par exemple, en raison d'un encodage incorrect ou de données endommagées.

Profondeur de décodage Unix-à-Unix

Spécifie le nombre maximal d'octets à extraire et à décoder de chaque pièce jointe de courriel encodée Unix à Unix (uuencoded). Vous pouvez spécifier une valeur positive ou 0 pour décoder toutes les données uuencodées dans le paquet. Spécifiez -1 pour ignorer les données uuencodées.

Lorsque cette option est activée, vous pouvez activer la règle 142:7 sur le générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque le décodage échoue; Le décodage peut échouer, par exemple, en raison d'un encodage incorrect ou de données endommagées.

Sujets connexes

Gestion des couches

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions

Le mot-clé file_data

Configuration du préprocesseur POP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si **Configuration POP** est désactivée sous **Préprocesseurs de la couche d'application**, cliquez sur **Activé**.

Étape 6 Cliquez sur **Edit** (✎) à côté de la **Configuration POP**.

Étape 7 Modifiez les paramètres décrits enOptions du préprocesseur POP, à la page 55.

Étape 8 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez activer les incidents d'intrusion, activez les règles de préprocesseur POP (GID 142). Pour en savoir plus, consultez Définition des états des règles d'intrusion.
- Déployer les changements de configuration.

Sujets connexes

Gestion des couches
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions

Règles de préprocesseur POP supplémentaires

Les règles de préprocesseur POP dans le tableau suivant ne sont pas associées à des options de configuration spécifiques. Comme pour les autres règles de préprocesseur POP, vous devez activer ces règles si vous souhaitez qu'elles générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés.

Tableau 15 : Règles de préprocesseur POP supplémentaires

GID de la règle de préprocesseur : SID	Description
1421	Génère un événement lorsque le préprocesseur détecte une commande client qui n'est pas définie dans la RFC 1939.
142:2	Génère un événement lorsque le préprocesseur détecte une réponse de serveur qui n'est pas définie dans la RFC 1939.
142:3	Génère un événement lorsque le préprocesseur utilise la quantité maximale de mémoire autorisée par le système. À ce stade, le préprocesseur arrête le décodage jusqu'à ce que la mémoire se libère.

Le préprocesseur SMTP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le préprocesseur SMTP indique au moteur de règles de normaliser les commandes SMTP. Le préprocesseur peut également extraire et décoder les pièces jointes dans le trafic client-serveur et, selon la version du logiciel, extraire les noms des fichiers de courriel, les adresses et les données d'en-tête pour fournir un contexte lors de l'affichage des incidents d'intrusion déclenchés par le trafic SMTP.

Options du préprocesseur SMTP

Vous pouvez activer ou désactiver la normalisation, et vous pouvez configurer des options pour contrôler les types de trafic anormal détectés par le décodeur SMTP.

Notez que le déchiffrement, ou l'extraction lorsque la pièce jointe MIME ne nécessite pas de décodage, inclut plusieurs pièces jointes le cas échéant et des pièces jointes volumineuses qui s'étendent sur plusieurs paquets.

Notez également que la valeur la plus élevée est utilisée lorsque les valeurs des **Base64 Decoding Depth**, **7-Bit/8-Bit/Binary Decoding Depth**, **Quoted-Printable Decoding Depth**, ou **Unix-to-Unix Decoding Depth** sont différentes dans :

- La politique d'analyse du réseau par défaut
- Toute autre politique d'analyse de réseau personnalisée appelée par les règles d'analyse de réseau dans la même politique de contrôle d'accès

Si aucune règle de préprocesseur n'est mentionnée dans les descriptions suivantes, l'option n'est associée à aucune règle de préprocesseur.

Ports

Spécifie les ports dont vous souhaitez normaliser le trafic SMTP. Vous pouvez spécifier une valeur supérieure ou égale à 0. Séparez les valeurs de ports multiples par des virgules.

Inspection dynamique

Lorsque cette option est sélectionnée, le décodeur SMTP enregistre l'état et fournit un contexte de session pour les paquets individuels et inspecte uniquement les sessions réassemblées. Lorsqu'elle est désélectionnée, cette option analyse chaque paquet individuellement sans contexte de session.

Normaliser

Lorsqu'elle est définie sur `All` (Toutes), cela normalise toutes les commandes. Vérifie s'il y a plusieurs espaces après une commande.

Lorsqu'elle est définie sur `None` (Aucune), ne normalise aucune commande.

Lorsqu'elle est définie sur `Cmds`, normalise les commandes répertoriées dans **Commandes personnalisées**.

Commandes personnalisées

Lorsque **Normaliser** est défini sur `Cmds`, normalise les commandes répertoriées.

Précisez les commandes qui doivent être normalisées dans la zone de texte. Vérifie s'il y a plusieurs espaces après une commande.

Les espaces (ASCII 0x20) et les tabulations (ASCII 0x09) sont considérées comme des espaces à des fins de normalisation.

Ignorer les données

Ne traite pas les données de messagerie; traite uniquement les données d'en-tête de messagerie MIME.

Ignorer les données de TLS

Ne traite pas les données chiffrées avec le protocole de Transport Layer Security.

Aucune alerte

Désactive les incidents d'intrusion lorsque les règles de préprocesseur associées sont activées.

Détecter les commandes inconnues

Détecte les commandes inconnues dans le trafic SMTP.

Vous pouvez activer la règle 124:5 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Longueur maximale de la ligne de commande

Détecte quand une ligne de commande SMTP est plus longue que cette valeur. Spécifiez `0` pour ne jamais détecter la longueur de la ligne de commande.

La RFC 2821, la spécification du groupe de travail en réseau sur le protocole Simple Mail Transfer Protocol, recommande une longueur de ligne de commande maximale de 512 comme longueur de ligne de commande.

Vous pouvez activer la règle 124:1 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Longueur maximale de la ligne d'en-tête

Détecte lorsqu'une ligne d'en-tête de données SMTP dépasse cette valeur. Spécifiez `0` pour ne jamais détecter la longueur de ligne d'en-tête de données.

Vous pouvez activer les règles 124:2 et 128:7 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Longueur maximale de la ligne de réponse

Détecte quand une ligne de réponse SMTP est plus longue que cette valeur. Spécifiez `0` pour ne jamais détecter la longueur de la ligne de réponse.

La RFC 2821 recommande une longueur de ligne maximale de 512 comme longueur de ligne de réponse.

Vous pouvez activer la règle 125:3 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option ainsi que pour la fonction **Alt Mac Command Line Len** (Longueur de la ligne de commande Mac Alt), lorsque cette option est activée.

Longueur maximale alternative de la ligne de commande

Détecte lorsque la ligne de commande SMTP pour l'une des commandes spécifiées est plus longue que cette valeur. Spécifiez `0` pour ne jamais détecter la longueur de ligne de commande pour les commandes spécifiées. Différentes longueurs de ligne par défaut sont définies pour de nombreuses commandes.

Ce paramètre remplace le paramètre Max Command Line Len (Longueur maximale de la ligne de commande) pour les commandes spécifiées.

Vous pouvez activer la règle 125:3 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option ainsi que pour **Max Response Line Len** (Longueur maximale de la ligne de réponse) lorsque cette option est activée.

Commandes non valides

Détecte si ces commandes sont envoyées du côté client.

Vous pouvez activer la règle 124:6 to générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option ainsi que pour les **commandes non valides**.

Commandes valides

Autorise les commandes dans cette liste.

Même si cette liste est vide, le préprocesseur autorise les commandes valides suivantes : ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SIZE SOML STARTTLS TICK TIME TURN TURNME VERB VRFY XADR XAUTH XCIR XEXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE XSTA XTRN XUSR

Remarque RCPT TO et MAIL FROM sont des commandes SMTP. La configuration du préprocesseur utilise des noms de commande RCPT et MAIL, respectivement. Dans le code, le préprocesseur mappe CRPT et MAIL au nom de commande correct.

Vous pouvez activer la règle 124:4 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option ainsi que pour les **commandes non valides** lorsque cette option est configurée.

Commandes de données

Répertorie les commandes qui lancent l'envoi de données de la même manière que la commande SMTP DATA envoie des données selon la RFC 5321. Séparez les commandes par des espaces.

Commandes de données binaires

Répertorie les commandes qui lancent l'envoi de données d'une manière similaire à la façon dont la commande BDAT envoie des données selon la RFC 3030. Séparez les commandes par des espaces.

Commandes d'authentification

Répertorie les commandes qui lancent un échange d'authentification entre le client et le serveur. Séparez les commandes par des espaces.

Détecter xlink2state

Détecte les paquets qui font partie des attaques X-Link2State par débordement des données de la mémoire tampon Microsoft Exchange. Dans les déploiements en ligne, le système peut également abandonner ces paquets.

Vous pouvez activer la règle 124:8 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Profondeur de décodage en base 64

Lorsque **Ignorer les données** est désactivé, cette option spécifie le nombre maximal d'octets à extraire et à décoder de chaque pièce jointe MIME encodée en Base64. Vous pouvez choisir parmi une valeur positive ou spécifier 0 pour décoder toutes les données Base64. Spécifiez -1 pour ignorer les données Base64. Le préprocesseur ne décode pas les données lorsque **Ignore Data** (Ignorer les données) est sélectionné.

Notez que les valeurs positives non divisibles par 4 sont arrondies au multiple supérieur de 4, sauf pour les valeurs 65533, 65534 et 65535, qui sont arrondies à 65532.

Lorsque cette option est activée, vous pouvez activer la règle 124:10 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque le décodage échoue; Le décodage peut échouer, par exemple, en raison d'un encodage incorrect ou de données endommagées.

Notez que cette option remplace les options obsolètes **Enable MIME Decoding** (Activer le décodage MIME) et **Maximum MIME Depth** (profondeur maximale de décodage MIME), qui sont toujours prises en charge dans les politiques de prévention des intrusions existantes pour des raisons de compatibilité.

7 bits/8 bits/profondeur de décodage binaire

Lorsque **Ignorer les données** est désactivé, cette option spécifie le nombre maximal d'octets de données à extraire de chaque pièce jointe MIME de courriel qui ne nécessite pas de décodage. Ces types de pièces jointes comprennent des types de pièces jointes 7 bits, 8 bits, binaires et en plusieurs parties comme du texte brut, des images jpeg, des fichiers mp3, etc. Vous pouvez spécifier une valeur positive ou 0 pour extraire toutes les données du paquet. Spécifiez -1 pour ignorer les données non décodées. Le préprocesseur n'extrait pas les données lorsque **Ignore Data** (Ignorer les données) est sélectionné.

Profondeur de décodage Quoted-Printable

Lorsque **Ignorer les données** est désactivé, spécifie le nombre maximal d'octets à extraire et à décoder de chaque pièce jointe MIME encodée que l'on peut imprimer (QP).

Vous pouvez spécifier de 1 à 65 535 octets, ou spécifier 0 pour décoder toutes les données codées QP du paquet. Spécifiez -1 pour ignorer les données codées QP. Le préprocesseur ne décode pas les données lorsque **Ignore Data** (Ignorer les données) est sélectionné.

Lorsque cette option est activée, vous pouvez activer la règle 124:11 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque le décodage échoue; Le décodage peut échouer, par exemple, en raison d'un encodage incorrect ou de données endommagées.

Profondeur de décodage Unix-à-Unix

Lorsque **Ignorer les données** est désactivé, spécifie le nombre maximal d'octets à extraire et à décoder de chaque pièce jointe de courriel encodée Unix à Unix (uuencoded). Vous pouvez spécifier de 1 à 65 535 octets, ou spécifier 0 pour décoder toutes les données uuencodées dans le paquet. Spécifiez -1 pour ignorer les données uuencodées. Le préprocesseur ne décode pas les données lorsque **Ignore Data** (Ignorer les données) est sélectionné.

Lorsque cette option est activée, vous pouvez activer la règle 124:13 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque le décodage échoue; Le décodage peut échouer, par exemple, en raison d'un encodage incorrect ou de données endommagées.

Consigner les noms des pièces jointes MIME

Active l'extraction des noms de fichiers joints MIME de l'en-tête MIME Content-Disposition et associe les noms de fichiers à tous les incidents d'intrusion générés pour la session. Les noms de fichiers multiples sont pris en charge.

Lorsque cette option est activée, vous pouvez afficher les noms de fichiers associés aux événements dans la colonne Pièce jointe de courriel du tableau des incidents d'intrusion.

Consigner à ces adresses

Active l'extraction des adresses de courriel des destinataires à partir de la commande SMTP RCPT TO et associe les adresses des destinataires à tous les incidents d'intrusion générés pour la session. Les destinataires multiples sont pris en charge.

Lorsque cette option est activée, vous pouvez afficher les destinataires associés aux événements dans la colonne Email Recipient (Destinataire du courriel) du tableau des incidents d'intrusion.

Consigner à partir de ces adresses

Active l'extraction des adresses courriel des expéditeurs à partir de la commande SMTP MAIL OF et associe les adresses des expéditeurs à tous les incidents d'intrusion générés pour la session. Les adresses d'expéditeur multiples sont prises en charge.

Lorsque cette option est activée, vous pouvez afficher les expéditeurs associés aux événements dans la colonne Email Sender (Expéditeur du courriel) du tableau des incidents d'intrusion.

En-têtes du journal

Active l'extraction des en-têtes de courriel. Le nombre d'octets à extraire est déterminé par la valeur spécifiée pour la **profondeur d'en-tête du journal**.

Vous pouvez utiliser le mot-clé `content` ou `protected_content` pour écrire des règles de prévention des intrusions qui utilisent les données d'en-tête de courriel comme modèle. Vous pouvez également afficher l'en-tête du courriel extrait dans la vue des paquets d'incidents d'intrusion.

Profondeur de l'en-tête du journal

Spécifie le nombre d'octets de l'en-tête de courriel à extraire lorsque **en-têtes de journal** est activé. Vous pouvez spécifier de 0 à 20 480 octets. La valeur 0 désactive les **en-têtes**des journaux.

Sujets connexes

Arguments pour le contenu de base et le mot-clé protected_content

Configuration du décodage SMTP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le volet de navigation.

Étape 5 Si **la configuration SMTP** est désactivée sous **Préprocesseurs de couche d'application**, cliquez sur **Enabled** (Activée).

Étape 6 Cliquez sur **Edit** ( ) à côté de **SMTP Configuration** (Configuration SMTP)..

Étape 7 Modifiez les options décrites dans Options du préprocesseur SMTP, à la page 58.

Étape 8 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, activez les règles de préprocesseur SMTP (GID 124). Pour en savoir plus, consultez Définition des états des règles d'intrusion.
- Déployer les changements de configuration.

Sujets connexes

Gestion des couches
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions

Le préprocesseur SSH

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le préprocesseur SSH détecte :

- Exploit par débordement de la mémoire tampon défi-réponse
- L'exploit CRC-32
- Exploit du débordement de la mémoire tampon SecureCRT SSH du client
- Incompatibilités de protocole
- Direction du message SSH incorrecte
- Toute chaîne de version autre que la version 1 ou 2

Les attaques par débordement de la mémoire tampon défi-réponse et CRC-32 se produisent après l'échange de clés et sont, par conséquent, chiffrées. Les deux attaques envoient une charge utile anormalement élevée de plus de 20 Koctets au serveur immédiatement après la demande d'authentification. Les attaques CRC-32 s'appliquent uniquement à SSH version 1; Les exploitations de défi-réponse de débordement de la mémoire tampon s'appliquent uniquement à SSH version 2. La chaîne de version est lue au début de la session. À l'exception de la différence dans la chaîne de version, les deux attaques sont gérées de la même manière.

Les attaques d'exploit SSH de SecureCRT et d'incompatibilité de protocole se produisent lors de la tentative de sécurisation d'une connexion, avant l'échange de clé. L'exploit de SecureCRT envoie une chaîne d'identifiant de protocole trop longue au client, ce qui provoque un débordement de la mémoire tampon. Une incompatibilité de protocole se produit lorsqu'une application cliente non-SSH tente de se connecter à un serveur SSH sécurisé ou lorsque les numéros de version du serveur et du client ne correspondent pas.

Vous pouvez configurer le préprocesseur SSH pour inspecter le trafic sur un port ou une liste de ports spécifiés, ou pour détecter automatiquement le trafic SSH. Il continuera à inspecter le trafic SSH jusqu'à ce qu'un nombre spécifié de paquets chiffrés soit passé dans un nombre spécifié d'octets, ou jusqu'à ce qu'un nombre maximal d'octets soit dépassé dans le nombre de paquets spécifié. Si le nombre maximal d'octets est dépassé, on suppose qu'une attaque CRC-32 (SSH version 1) ou Défi-réponse par débordement de la mémoire tampon (SSH version 2) a eu lieu. Notez que sans configuration, le préprocesseur détecte toute valeur de chaîne de version autre que la version 1 ou 2.

Notez également que le préprocesseur SSH ne gère pas les attaques par force brute.

Options du préprocesseur SSH

Le préprocesseur interrompt l'inspection du trafic pour une session lorsque l'une des situations suivantes se produit :

- un échange valide entre le serveur et le client a eu lieu pour ce nombre de paquets chiffrés; la connexion se poursuit.
- le **nombre d'octets envoyés sans réponse du serveur** est atteint avant le nombre de paquets chiffrés à inspecter; on suppose qu'il y a une attaque.

Chaque réponse valide de serveur pendant le **nombre de paquets chiffrés à inspecter** réinitialise le **nombre d'octets envoyés sans réponse du serveur**, et le nombre de paquets se poursuit.

Considérez l'exemple de configuration de préprocesseur SSH suivant :

- **Ports de serveur** : 22
- **Détection automatique de ports** : désactivée
- **Longueur maximale de la chaîne de version du protocole** : 80
- **Nombre de paquets chiffrés à inspecter** : 25
- **Nombre d'octets envoyés sans réponse du serveur** : 19 600
- Toutes les options de détection sont activées.

Dans l'exemple, le préprocesseur inspecte le trafic uniquement sur le port 22. C'est-à-dire que la détection automatique est désactivée, de sorte qu'elle inspecte uniquement le port spécifié.

En outre, le préprocesseur de l'exemple arrête d'inspecter le trafic lorsque l'une des situations suivantes se produit :

- Le client envoie 25 paquets chiffrés qui ne contiennent pas plus de 19 600 octets, en cumulé. L'hypothèse est qu'il n'y a pas d'attaque.
- Le client envoie plus de 19 600 octets dans 25 paquets chiffrés. Dans ce cas, le préprocesseur considère qu'il s'agit d'une attaque de débordement de tampon défi-réponse, car la session dans l'exemple est une session SSH version 2.

Le préprocesseur de l'exemple détectera également l'un des événements suivants qui se produisent pendant le traitement du trafic:

- un débordement de serveur, déclenché par une chaîne de version supérieure à 80 octets et indiquant un exploit SecureCRT
- une différence de protocole
- un paquet s'écoule dans la mauvaise direction

Enfin, le préprocesseur détectera automatiquement toute chaîne de version autre que la version 1 ou la version 2.

Si aucune règle de préprocesseur n'est mentionnée dans les descriptions suivantes, l'option n'est associée à aucune règle de préprocesseur.

Ports de serveur

Spécifie sur quels ports le préprocesseur SSH doit inspecter le trafic.

Vous pouvez configurer un port unique ou une liste de ports séparés par des virgules.

Détection automatique de ports

Définit le préprocesseur pour détecter automatiquement le trafic SSH.

Lorsque cette option est sélectionnée, le préprocesseur inspecte tout le trafic à la recherche d'un numéro de version SSH. Il arrête le traitement lorsque ni le paquet client ni le paquet serveur ne contiennent de numéro de version. Lorsque cette option est désactivée, le préprocesseur inspecte uniquement le trafic identifié par l'option **Server Ports** (ports du serveur).

Nombre de paquets chiffrés à inspecter

Spécifie le nombre de paquets chiffrés réassemblés de flux à examiner par session.

La définition de cette option à zéro permettra à tout le trafic de passer.

La réduction du nombre de paquets chiffrés à inspecter peut faire en sorte que certaines attaques aient échappé à la détection. L'augmentation du nombre de paquets chiffrés à inspecter peut nuire aux performances.

Nombre d'octets envoyés sans réponse du serveur

Spécifie le nombre maximal d'octets qu'un client SSH peut envoyer à un serveur sans obtenir de réponse avant de supposer qu'il y a un débordement de tampon de défi-réponse ou une attaque par CRC-32.

Augmentez la valeur de cette option si le préprocesseur génère des faux positifs lors du débordement de la mémoire tampon de défi-réponse ou d'exploitation CRC-32.

Longueur maximale de la chaîne de version du protocole

Spécifie le nombre maximal d'octets autorisés dans la chaîne de version du serveur avant de la considérer comme un exploit SecureCRT.

Détecter l'attaque de débordement de la mémoire tampon de la réponse au défi

Active ou désactive la détection de l'exploitation de débordement de la mémoire tampon défi-réponse.

Vous pouvez activer la règle 128:1 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Notez qu'une session SFTP peut occasionnellement déclencher la règle 128:1.

Détecter l'attaque SSH1 CRC-32

Active ou désactive la détection de l'exploitation CRC-32.

Vous pouvez activer la règle 128:2 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter le débordement du serveur

Active ou désactive la détection du débordement de la mémoire tampon SecureCRT SSH du client.

Vous pouvez activer la règle 128:3 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter les différences de protocole

Active ou désactive la détection des incompatibilités de protocole.

Vous pouvez activer la règle 128:4 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter la mauvaise direction des messages

Active ou désactive la détection du trafic dans la mauvaise direction (c'est-à-dire si le serveur présumé génère du trafic client ou un client génère du trafic sur le serveur).

Vous pouvez activer la règle 128:5 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter la taille de la charge utile incorrecte pour la charge utile donnée

Active ou désactive la détection des paquets avec une taille de charge utile incorrecte, par exemple lorsque la longueur spécifiée dans le paquet SSH n'est pas cohérente avec la longueur totale spécifiée dans l'en-tête IP ou que le message est tronqué, c'est-à-dire qu'il n'y a pas assez de données pour un SSH complet.

Vous pouvez activer la règle 128:6 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter la mauvaise chaîne de version

Notez que, lorsqu'elle est activée, le préprocesseur détecte sans configuration toute chaîne de version autre que la version 1 ou 2.

Vous pouvez activer la règle 128:7 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Configuration du préprocesseur SSH

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si **la configuration SSH** est désactivé sous **Préprocesseurs de la couche d'application**, cliquez sur **Enabled** (Activé).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Configuration SSH**.

Étape 7 Modifiez les options décrites dans Options du préprocesseur SSH, à la page 65.

Étape 8 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez activer les incidents d'intrusion, activez les règles de préprocesseur SSH (GID 128). Pour en savoir plus, consultez Définition des états des règles d'intrusion.
- Déployer les changements de configuration.

Sujets connexes

Gestion des couches

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions

Le préprocesseur SSL

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le préprocesseur SSL vous permet de configurer l'inspection SSL, qui peut bloquer le trafic chiffré, le déchiffrer ou inspecter le trafic avec le contrôle d'accès. Que vous configuriez ou non l'inspection SSL, le préprocesseur SSL analyse également les messages d'établissement de liaison SSL lorsqu'il est détecté dans le trafic et détermine quand une session est chiffrée. L'identification du trafic chiffré permet au système de bloquer les intrusions et l'inspection des fichiers des charges utiles chiffrées, ce qui contribue à réduire les faux positifs et à améliorer les performances.

Le préprocesseur SSL peut également examiner le trafic chiffré pour détecter les tentatives d'exploit du bogue Heartbleed et générer des événements lorsqu'il détecte de telles exploits.

Vous pouvez suspendre l'inspection du trafic pour détecter les intrusions et les programmes malveillants une fois la session chiffrée. Si vous configurez l'inspection SSL, le préprocesseur SSL identifie également le trafic chiffré que vous pouvez bloquer, déchiffrer ou inspecter à l'aide du contrôle d'accès.

L'utilisation du préprocesseur SSL pour déchiffrer le trafic chiffré ne nécessite pas de licence. Toutes les autres fonctionnalités du préprocesseur SSL, y compris l'arrêt de l'inspection des données utiles chiffrées à la recherche de programmes malveillants et de prévention des intrusions, et la détection des exploits de bogues Heartbleed, nécessitent une licence de protection.

Fonctionnement du prétraitement SSL

Le préprocesseur SSL arrête les intrusions et l'inspection de fichiers des données chiffrées, et inspecte le trafic chiffré à l'aide d'une politique SSL si vous configurez l'inspection SSL. Cela permet d'éliminer les faux positifs. Le préprocesseur SSL gère les informations d'état pendant qu'il inspecte l'établissement de liaison SSL, en suivant à la fois l'état et la version SSL pour cette session. Lorsque le préprocesseur détecte qu'un état de session est chiffré, le système marque le trafic de cette session comme chiffré. Vous pouvez configurer le système pour arrêter le traitement de tous les paquets d'une session chiffrée lorsque le chiffrement est établi, et pour générer un événement lorsqu'il détecte une tentative d'exploitation de bogue heartbleed.

Pour chaque paquet, le préprocesseur SSL vérifie que le trafic contient un en-tête IP, un en-tête TCP et une charge utile TCP, et qu'il se produit sur les ports spécifiés pour le prétraitement SSL. Pour le trafic admissible, les scénarios suivants déterminent si le trafic est chiffré :

- Le système observe tous les paquets d'une session, **les données du côté serveur sont sécurisées** ne sont pas activées, et la session comprend un message Finished (Terminé) du serveur et du client et au moins un paquet de chaque côté avec un enregistrement d'application et sans enregistrement d'alerte.
- Le système manque une partie du trafic, **les données côté serveur sont approuvées** ne sont pas activées et la session comprend au moins un paquet de chaque côté avec un enregistrement d'application auquel il n'est pas réponse par un enregistrement d'alerte.

- Le système observe tous les paquets dans une session, **les données côté serveur sont sécurisées** sont activées, et la session comprend un message Terminé du client et au moins un paquet du client avec un enregistrement d'application et sans enregistrement d'alerte.
- Le système manque une partie du trafic, **les données du côté serveur sont sécurisées** sont activées et la session comprend au moins un paquet du client avec un enregistrement d'application auquel aucun enregistrement d'alerte ne répond par un enregistrement d'alerte.

Si vous choisissez d'arrêter le traitement du trafic chiffré, le système ignorera les futurs paquets de la session après avoir marqué la session comme chiffrée.

En outre, pendant l'établissement de liaison SSL, le préprocesseur surveille les demandes et les réponses de pulsation. Le préprocesseur génère un événement s'il détecte :

- une demande de pulsation contenant une valeur de longueur de charge utile supérieure à la charge utile elle-même
- une réponse de pulsation qui est supérieure à la valeur stockée dans le champ Max Heartbeat Longueur (longueur de pulsation max.)

Remarque Vous pouvez ajouter les mots-clés `ssl_state` et `ssl_version` à une règle pour utiliser les informations d'état ou de version SSL dans la règle.

Sujets connexes

Mots-clés SSL

Options du préprocesseur SSL

Remarque Les politiques d'analyse de réseau fournies par le système activent le préprocesseur SSL par défaut. Cisco vous recommande de ne pas désactiver le préprocesseur SSL dans les déploiements personnalisés si vous vous attendez à ce qu'un trafic chiffré traverse votre réseau.

Si l'inspection SSL n'est pas configurée, le système tente d'inspecter le trafic chiffré à la recherche de programmes malveillants et de prévention des intrusions sans le déchiffrer. Lorsque vous activez le préprocesseur SSL, il détecte le chiffrement d'une session. Une fois le préprocesseur SSL activé, le moteur de règles peut appeler le préprocesseur pour obtenir des informations sur l'état et la version de SSL. Si vous activez des règles à l'aide des mots-clés `ssl_state` et `ssl_version` dans une politique de prévention des intrusions, vous devez également activer le préprocesseur SSL dans cette politique.

Ports

Spécifie les ports, séparés par des virgules, où le préprocesseur SSL doit surveiller le trafic pour les sessions chiffrées. Seuls les ports spécifiés dans ce champ feront l'objet d'une vérification du trafic chiffré.

Remarque Si le préprocesseur SSL détecte du trafic non SSL sur les ports spécifiés pour la surveillance SSL, il essaie de décoder le trafic en tant que trafic SSL, puis le signale comme corrompu.

Arrêter d'inspecter le trafic chiffré

Active ou désactive l'inspection du trafic dans une session une fois que la session est marquée comme chiffrée.

Activez cette option pour désactiver l'inspection et le réassemblage pour les sessions chiffrées. Le préprocesseur SSL gère l'état de la session afin de pouvoir désactiver l'inspection de tout le trafic de la session. Lorsque cette option est activée, quelques paquets d'une session sont vérifiés pour s'assurer que le flux est chiffré, après quoi l'inspection approfondie est contournée. Chaque session contournée augmente le nombre de flux à avance rapide affiché dans la réponse à la commande **show snort statistics**. De plus, comme l'inspection approfondie est contournée, les octets de l'initiateur et du répondeur dans l'événement de connexion ne sont pas précis. Ils sont inférieurs à la valeur de la session réelle, car ils n'incluent que les paquets inspectés par Snort et aucun paquet une fois que l'inspection approfondie est contournée. Ce comportement s'applique aux événements des résumés de connexion et à toutes les valeurs de trafic affichées dans les gadgets.

Le système arrête d'inspecter le trafic dans les sessions chiffrées uniquement si à la fois :

- Le prétraitement SSL est activé
- Cette option est sélectionnée

Si vous décochez cette option, vous ne pouvez pas modifier l'option **Les données du côté du serveur sont de confiance**.

Les données du côté serveur sont sécurisées

Lorsque l'activation de l'option Arrêter l'inspection du trafic chiffré, permet l'identification du trafic chiffré en fonction uniquement du trafic côté client,

Longueur maximale de la pulsation

En spécifiant un nombre d'octets, permet d'inspecter les demandes et les réponses de pulsation dans la prise de contact SSL à la recherche de tentatives d'exploit par heartbeat. Vous pouvez spécifier un entier compris entre `1` et `65 535`ou `0` pour désactiver l'option.

Si le préprocesseur détecte une demande heartbeat dont la longueur de charge utile est supérieure à la longueur de charge utile réelle et que la règle 136:3 est activée, ou une réponse heartbeat supérieure en taille à la valeur configurée pour cette option lorsque la règle 136:4 est activée, le préprocesseur générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés.

Configuration du préprocesseur SSL

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si **la configuration SSL** est désactivée sous **Préprocesseurs de la couche d'application** est désactivée, cliquez sur **Enabled** (Activé).

Étape 6 Cliquez sur **Edit** (✎) à côté de **SSL Configuration**.

Étape 7 Modifiez l'un des paramètres décrits en Options du préprocesseur SSL, à la page 70.

- Saisissez une valeur dans le champ **Ports**. Séparez les valeurs multiples par des virgules
- Cochez ou décochez la case **Stop inspecting encrypted traffic** (Arrêter l'inspection du trafic chiffré).
- Si vous avez coché **Arrêter d'inspecter le trafic chiffré**, cochez ou décochez la case**Server side data is trusted** (les données côté serveur sont de confiance).
- Saisissez une valeur dans le champ **Max heartbeat Length** (longueur de pulsation max.).

Astuces La valeur `0` désactive cette option.

Étape 8 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez activer les événements d'intrusion, activez les règles de préprocesseur SSL (GID 137).incidents Pour en savoir plus, consultez Définition des états des règles d'intrusion.
- Déployer les changements de configuration.

Sujets connexes

Gestion des couches

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions

Règles de préprocesseur SSL

Si vous souhaitez générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, activez les règles de préprocesseur SSL (GID 137).

Le tableau suivant décrit les règles de préprocesseur SSL que vous pouvez activer.

Tableau 16 : Règles de préprocesseur SSL

GID de la règle de préprocesseur : SID	Description
137:1	Détecte un message ClientHello après un message ServerHello, qui n'est pas valide et est considéré comme un comportement anormal.
137:2	Détecte un message ServerHello sans message ClientHello lorsque l'option de préprocesseur SSL **Les données côté serveur sont de confiance** est désactivée, ce qui est non valide et considéré comme un comportement anormal.
137:3	Détecte une requête de pulsation heartbeat avec une longueur de charge utile supérieure à la charge utile elle-même lorsque l'option de préprocesseur SSL contient une valeur non nulle, ce qui indique une tentative d'exploitation du bogue **heartbleed**.
137:4	Détecte une réponse de pulsation supérieure à une valeur non nulle spécifiée dans la **longueur max**. de pulsation du préprocesseur SSL , ce qui indique une tentative d'exploitation du bogue heartbleed.

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.