Préprocesseurs des couches transport et réseau

Les rubriques suivantes expliquent les préprocesseurs de transport et de réseau, et la façon de les configurer :

Introduction aux préprocesseurs des couches transport et réseau

Les préprocesseurs de la couche de transport et de la couche réseau détectent les attaques qui exploitent la fragmentation IP, la validation de la somme de contrôle et le prétraitement des sessions TCP et UDP. Avant l'envoi des paquets aux préprocesseurs, le décodeur de paquets convertit les en-têtes de paquets et les charges utiles dans un format facilement utilisable par les préprocesseurs et le moteur de règles de prévention des intrusions, et il détecte divers comportements anormaux dans les en-têtes de paquets. Après le décodage des paquets et avant d'envoyer des paquets à d'autres préprocesseurs, le préprocesseur de normalisation en ligne normalise le trafic pour les déploiements en ligne.

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.

Exigences de licences pour les préprocesseurs de couches de transport et de réseau

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables pour les préprocesseurs de couches de transport et de réseau

Prise en charge des modèles

Tout.

Domaines pris en charge

N’importe quel

Rôles utilisateur

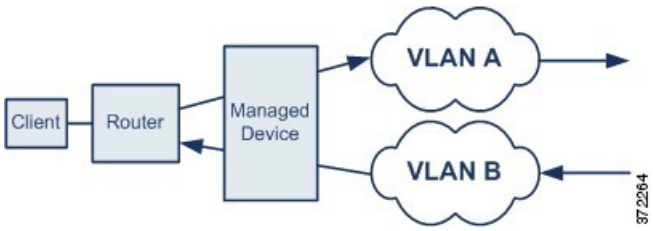
- Admin
- Administrateur d’intrusion

Paramètres avancés du préprocesseur de couche transport/réseau

Les paramètres avancés de transport et de préprocesseur de réseau s’appliquent globalement à tous les réseaux, toutes les zones et tous les VLAN dans lesquels vous déployez votre politique de contrôle d’accès. Vous configurez ces paramètres avancés dans le cadre d'une politique de contrôle d’accès plutôt que dans une politique d’analyse de réseau.

En-tête VLAN ignorés

Différentes balises VLAN dans le trafic circulant dans différentes directions pour une même connexion peuvent avoir une incidence sur le réassemblage du trafic et le traitement des règles. Par exemple, dans le graphique suivant, le trafic pour la même connexion pourrait être transmis sur le VLAN A et reçu sur le VLAN B.



Vous pouvez configurer le système pour ignorer l'en-tête VLAN afin que les paquets puissent être traités correctement pour votre déploiement.

Réponses actives dans les règles de suppression de prévention des intrusions

Une règle de suppression est une règle de prévention des intrusions ou de préprocesseur dont l'état est réglé à Supprimer et Générer des événements. Dans un déploiement en ligne, le système répond aux règles de suppression TCP ou UDP en abandonnant le paquet déclencheur et en bloquant la session à l'origine du paquet.

Astuces Comme les flux de données UDP ne sont généralement pas considérés en termes de *sessions*, le préprocesseur de flux utilise les champs d'adresse IP source et de destination de l'en-tête du datagramme IP d'encapsulation et les champs de port de l'en-tête UDP pour déterminer la direction du flux et identifier une session UDP.

Vous pouvez configurer le système pour lancer une ou plusieurs *réponses actives* afin de fermer plus précisément et spécifiquement une connexion TCP ou une session UDP lorsqu'un paquet fautif déclenche une règle d'abandon TCP ou UDP. Vous pouvez utiliser des réponses actives dans les déploiements en ligne, y compris les déploiements routés et transparents. Les réponses actives ne sont pas adaptées ou prises en charge pour les déploiements passifs.

Pour configurer les réponses actives :

- Créez ou modifiez une règle de prévention des intrusions TCP ou UDP (mot-clé **resp** uniquement). Consultez Protocole d'en-tête de règle de prévention des intrusions.
- Ajoutez le mot-clé **react** ou **resp** à la règle de prévention des intrusions; voir xMots-clés de la réponse active.
- Éventuellement, pour une connexion TCP, spécifiez le nombre maximal de réponses actives supplémentaires à envoyer et le nombre de secondes à attendre entre les réponses actives. consultez **Nombre maximal de réponses actives** et **Nombre minimal de secondes de réponse** dans Options avancées de préprocesseur transport/réseau, à la page 4.

Les réponses actives ferment la session lorsque la correspondance du trafic déclenche une règle de suppression, comme suit :

- **TCP** : abandonne le paquet déclencheur et insère un paquet de réinitialisation TCP (RST) dans le trafic client et serveur.
- **UDP** : envoie un paquet ICMP inaccessible à chaque extrémité de la session.

Options avancées de préprocesseur transport/réseau

Ignorer l'en-tête VLAN lors du suivi des connexions

Spécifie s'il faut ignorer ou inclure les en-têtes VLAN lors de l'identification du trafic, comme suit :

- Lorsque cette option est sélectionnée, le système ignore les en-têtes VLAN. Utilisez ce paramètre pour les périphériques déployés qui pourraient détecter différentes balises VLAN pour la même connexion dans le trafic circulant dans différentes directions
- Lorsque cette option est désactivée, le système inclut les en-têtes VLAN. Utilisez ce paramètre pour les périphériques déployés qui ne détecteront pas différentes balises VLAN pour le même trafic de connexion circulant dans des directions différentes.

Nombre maximal de réponses actives

Spécifie un nombre maximal de réponses actives par connexion TCP. Lorsque du trafic supplémentaire se produit sur une connexion où une réponse active a été lancée et que le trafic se produit plus que le nombre **minimal de secondes de réponse** après une réponse active précédente, le système envoie une autre réponse active, sauf si le nombre maximal spécifié a été atteint. La valeur 0 désactive les réponses actives supplémentaires déclenchées par les règles **resp** ou **react**. Consultez Réponses actives dans les règles de suppression de prévention des intrusions, à la page 3 et Mots-clés de la réponse active.

Notez qu'une règle **resp** ou **react** déclenchée déclenche une réponse active, quelle que soit la configuration de cette option.

Nombre minimal de secondes de réponses

Jusqu'à ce que le **Nombre maximum de réponses actives** se produise, spécifie le nombre de secondes à attendre avant que tout trafic supplémentaire sur une connexion où le système a initié une réponse active n'entraîne une réponse active ultérieure.

Options de dépannage : seuil de journalisation de la fin de session

Mise en garde Ne modifiez pas le seuil de journalisation de fin de session, sauf si le service d'assistance vous le demande.

Lors d'un appel de dépannage, le service d'assistance peut vous demander de configurer votre système pour consigner un message lorsqu'une connexion individuelle dépasse le seuil spécifié. La modification du paramètre de cette option affectera les performances et doit être effectuée uniquement avec les conseils du service d'assistance.

Cette option spécifie le nombre d'octets qui entraînent un message enregistré lorsque la session se termine et que le nombre spécifié a été dépassé.

Remarque La limite supérieure de 1 Go est également limitée par la quantité de mémoire sur le périphérique géré allouée au traitement du flux.

Sujets connexes

Mots-clés de la réponse active

Configuration des paramètres avancés du préprocesseur de transport/réseau

Vous devez être Admin, Administrateur d'accèsou Administrateur de réseau pour effectuer cette tâche.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Edit** (✎) au niveau de la politique que vous souhaitez modifier.

Étape 2 Cliquez sur **More** > **Advanced Settings**(autres paramètres avancés), puis cliquez sur **Edit** (✎) à côté de la section **Transport/Network Preprocessor Settings** (paramètres de transport/préprocesseur de réseau).

Étape 3 À l'exception de l'option de dépannage **Seuil de journalisation de fin de session**, modifiez les options décrites dans Options avancées de préprocesseur transport/réseau, à la page 4.

Mise en garde Ne modifiez pas **le seuil de journalisation de fin de session**, sauf si le service d'assistance vous le demande.

Étape 4 Cliquez sur **OK**.

Prochaine étape

- Vous pouvez également poursuivre la configuration de la politique comme décrit dans Modification d'une politique de contrôle d'accès.
- Déployer les changements de configuration.

Vérification de la somme de contrôle

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 peut vérifier toutes les sommes de contrôle au niveau du protocole pour s'assurer que des transmissions IP, TCP, UDP et ICMP complètes sont reçues et que, à un niveau de base, les paquets n'ont pas été altérés ou altérés accidentellement en transit. Une somme de contrôle utilise un algorithme pour vérifier l'intégrité d'un protocole dans le paquet. Le paquet est considéré comme inchangé si le système calcule la même valeur que celle écrite dans le paquet par l'hôte final.

La désactivation de la vérification de la somme de contrôle peut rendre votre réseau vulnérable aux attaques par insertion. Remarque : Le système ne génère pas d'événements de vérification de somme de contrôle. Dans un déploiement en ligne, vous pouvez configurer le système pour abandonner les paquets avec des sommes de contrôle non valides.

Options de vérification de la somme de contrôle

Vous pouvez définir l'une des options suivantes sur **Enabled** ou **Disabled** (activer ou désactiver) dans un déploiement passif ou en ligne, ou à **Drop** (abandonner) dans un déploiement en ligne :

- **Sommes de contrôle ICMP**
- **Sommes de contrôle IP**
- **Sommes de contrôle TCP**
- **Sommes de contrôle UDP**

Pour supprimer les paquets fautifs, en plus de définir une option sur **Drop** (Abandonner), vous devez également activer le **mode en ligne** dans la politique d'analyse de réseau associée et vous assurer que le périphérique est déployé en ligne.

Régler ces options à **Drop** (abandon) dans un déploiement passif, ou dans un déploiement en ligne en mode TAP (surveilleur de données), est similaire à les définir sur **Enabled** (Activer).

Attention Sous les **sommes de contrôle TCP**, l'option **Ignore** (valeur par défaut) contourne ou ignore toutes les règles configurées Snort.

La valeur par défaut pour toutes les options de vérification de la somme de contrôle est **Enabled** (Activé). Cependant, les interfaces routées et transparentes défense contre les menaces abandonnent toujours les paquets qui échouent à la vérification de la somme de contrôle IP. Notez que les interfaces routées et transparentes défense contre les menaces corrigent les paquets UDP ayant une somme de contrôle erronée avant de les transmettre au processus Snort.

Sujets connexes

Modification du trafic de préprocesseur dans les déploiements en ligne

Vérification des sommes de contrôle

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 **Vérification de la somme de contrôle** sous **Préprocesseurs de la couche transport/réseau** est désactivée, cliquez sur **Activé**.

Étape 6 Cliquez sur **Edit** (✎) à côté de la **Vérification de la somme de contrôle**.

Étape 7 Modifiez les options décrites dans Vérification de la somme de contrôle, à la page 5.

Remarque Sous les **sommes de contrôle TCP**, l'option **Ignore** (valeur par défaut) contourne ou ignore toutes les règles configurées Snort.

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

- Déployer les changements de configuration.

Sujets connexes

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

Le préprocesseur de normalisation en ligne

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 de normalisation en ligne normalise le trafic pour minimiser les risques que des agresseurs échappant à la détection dans les déploiements en ligne.

Remarque Pour que le système puisse affecter le trafic, vous devez déployer les configurations pertinentes sur les périphériques gérés à l'aide d'interfaces routées, commutées ou transparentes, ou de paires d'interfaces en ligne.

Vous pouvez spécifier la normalisation de n'importe quelle combinaison de trafic IPv4, IPv6, ICMPv4, ICMPv6 et TCP. La plupart des normalisations sont effectuées par paquet et sont effectuées par le préprocesseur

de normalisation en ligne. Cependant, le préprocesseur de flux TCP gère la plupart des normalisations de paquets et de flux liées à l'état, y compris la normalisation de la charge utile TCP.

La normalisation en ligne a lieu immédiatement après le décodage par le décodeur de paquets et avant le traitement par les autres préprocesseurs. La normalisation se poursuit des couches de paquets internes vers les couches externes.

Le préprocesseur de normalisation en ligne ne génère pas d'événements ; il prépare les paquets à une utilisation par d'autres préprocesseurs et le moteur de règles dans les déploiements en ligne. Le préprocesseur permet également de s'assurer que les paquets traités par le système sont les mêmes que les paquets reçus par les hôtes de votre réseau.

Remarque Dans un déploiement en ligne, il est conseillé d'activer le mode en ligne et de configurer le préprocesseur de normalisation en ligne avec l'option **Normalize TCP Payload (normaliser la charge utile TCP)** activée. Dans un déploiement passif, il est conseillé d'utiliser Mises à niveau des profils adaptatifs.

Sujets connexes

Modification du trafic de préprocesseur dans les déploiements en ligne
À propos des profils adaptatifs

Options de normalisation en ligne

TTL minimum

Lorsque la valeur de **réinitialisation de la TTL** est supérieure ou égale à la valeur définie pour cette option, spécifie les éléments suivants :

- la valeur minimale que le système autorisera dans le champ Durée de vie (TTL) IPv4 lorsque la fonction **Normaliser IPv4** est activée; une valeur inférieure entraîne la normalisation de la valeur du paquet pour la TTL à la valeur définie pour la **réinitialisation de la TTL**
- la valeur minimale que le système autorisera pour le champ Limite de sauts IPv6 lorsque la fonction **Normaliser IPv6** est activée; une valeur inférieure entraîne la normalisation de la valeur de paquet pour la limite de sauts à la valeur définie pour la **réinitialisation de la TTL**

Le système suppose une valeur de 1 lorsque le champ est vide.

Remarque Pour les interfaces routées et transparentes défense contre les menaces , les options **Minimum TTL** et **Reset TTL** sont ignorées. La TTL maximale pour une connexion est déterminée par la TTL dans le paquet initial. La TTL des paquets suivants peut diminuer, mais elle ne peut pas augmenter. Le système réinitialisera la TTL au plus bas TTL vu précédemment pour cette connexion. Cela empêche les attaques d'évitement TTL.

Lorsque l'option **de détection des anomalies d'en-tête de protocole** de décodage de paquets est activée, vous pouvez activer les règles suivantes dans la catégorie de règles de décodeur de générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option :

- Vous pouvez activer la règle 116:428 pour se déclencher lorsque le système détecte un paquet IPv4 avec une TTL inférieure au minimum spécifié.

- Vous pouvez activer la règle 116:270 pour se déclencher lorsque le système détecte un paquet IPv6 avec une limite de sauts inférieure au minimum spécifié.

Réinitialiser le TTL

Lorsqu'il est défini sur une valeur supérieure ou égale à **Minimum TTL**, normalise les éléments suivants :

- le champ TTL IPv4 lorsque **Normaliser IPv4** est activé
- le champ IPv6 Hop Limit lorsque **Normaliser IPv6** est activé

Le système normalise le paquet en modifiant sa valeur TTL ou sa valeur de limite de sauts par la valeur définie pour cette option lorsque la valeur du paquet est inférieure à la **TTL minimale**. Laisser ce champ vide ou le définir à `0`ou à une valeur inférieure à la **TTL minimale** désactive l'option.

Normaliser IPv4

Active la normalisation du trafic IPv4. Le système normalise également le champ TTL selon les besoins dans les cas suivants :

- cette option est activée et
- la valeur définie pour **Réinitialiser la TTL** active la normalisation TTL.

Vous pouvez également activer des options IPv4 supplémentaires lorsque cette option est activée.

Lorsque vous activez cette option, le système effectue les normalisations IPv4 de base suivantes :

- tronque les paquets avec une charge utile excédentaire à la longueur de datagramme spécifiée dans l'en-tête IP
- efface le champ Differentiated Services (DS), auparavant connu sous le nom de champ Type of Service (TOS)
- définit tous les octets d'option à 1 (pas d'opération)

Cette option est ignorée pour les interfaces routées et transparentes défense contre les menaces . Les périphériques Défense contre les menaces abandonnent tout paquet RSVP contenant des options IP autres que les options router alert, end of options list (EOOL) et no operation (NOP) sur toute interface routée ou transparente.

Normaliser Don't Fragment Bit (bit à ne pas fragmenter)

Efface le sous-champ Ne pas fragmenter du bit unique du champ d'en-tête IPv4 Flags. L'activation de cette option permet à un routeur en aval de fragmenter les paquets si nécessaire au lieu de les abandonner; l'activation de cette option peut également empêcher les contournements basés sur la fabrication de paquets d'être abandonnés. Vous devez activer **Normaliser IPv4** pour sélectionner cette option.

Normaliser Reserved Bit (bit réservé)

Efface le sous-champ Reserved à un seul bit du champ d'en-tête indicateurs IPv4. Vous devez généralement activer cette option. Vous devez activer **Normaliser IPv4** pour sélectionner cette option.

Normaliser TOS Bit (bit TOS)

Efface le champ d'un octet Services différentiés, anciennement Type de service. Vous devez activer **Normaliser IPv4** pour sélectionner cette option.

Normaliser la charge utile excédentaire

Tronque les paquets avec une charge utile excédentaire à la longueur de datagramme spécifiée dans l'en-tête IP plus l'en-tête de couche 2 (par exemple, Ethernet), mais ne les tronque pas en dessous de la longueur de trame minimale. Vous devez activer **Normaliser IPv4** pour sélectionner cette option.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes. Les paquets avec une charge utile excédentaire sont toujours abandonnés sur ces interfaces.

Normaliser IPv6

Définit tous les champs Option Type dans les en-têtes d'extension des options saut par saut et des options de destination sur 00 (ignorer et continuer le traitement). Le système normalise également le champ Hop Limit selon les besoins lorsque cette option est activée et que la valeur définie pour **Réinitialiser la TTL** active la normalisation de la limite de saut.

Normaliser le ICMPv4

Efface le champ Code de 8 bits dans les messages Echo (Requête) et les messages de réponse Echo dans le trafic ICMPv4.

Normaliser le ICMPv6

Efface le champ Code de 8 bits dans les messages Echo (Requête) et les messages de réponse Echo dans le trafic ICMPv6.

Normaliser ou effacer les bits réservés

Efface les bits réservés dans l'en-tête TCP.

Normaliser ou effacer les octets de remplissage optionnel

Efface tous les octets de remplissage d'option TCP.

Effacer le pointeur urgent si URG=0

Efface le champ Urgent Pointer de l'en-tête TCP 16 bits si le bit de contrôle urgent (URG) n'est pas défini.

Effacer le pointeur urgent ou URG sur les charges utiles vides

Efface le champ Urgent Pointer de l'en-tête TCP et le bit de contrôle URG en l'absence de charge utile.

Effacer URG si le pointeur urgent n'est pas défini

Efface le bit de contrôle URG d'en-tête TCP si le pointeur urgent n'est pas défini.

Normaliser le pointeur d'urgence

Définit le champ Urgent Pointer de l'en-tête TCP à deux octets sur la longueur de la charge utile si le pointeur est supérieur à la longueur de la charge utile.

Normaliser la charge utile TCP

Active la normalisation du champ de données TCP pour assurer la cohérence des données retransmises. Tout segment qui ne peut pas être réassemblé correctement est abandonné.

Supprimer des données sur les SYN

Supprime les paquets de données synchronisées (SYN) si la politique de votre système d'exploitation TCP n'est **pas** Mac OS.

Cette option désactive également la règle 129:2, qui peut se déclencher lorsque l'option **politique** du préprocesseur de flux TCP n'est pas définie sur **Mac OS**.

Supprimer des données sur la RST

Supprime toutes les données d'un paquet de réinitialisation TCP (RST).

Découper les données à la fenêtre

Réduit le champ de données TCP à la taille spécifiée dans le champ Window.

Couper les données en MSS

Réduit le champ de données TCP à la taille maximale du segment (MSS) si la charge utile est plus longue que MSS.

Bloquer les anomalies d'en-tête TCP insoluble

Lorsque vous activez cette option, le système bloque les paquets TCP anormaux qui, s'ils étaient normalisés, seraient non valides et seraient probablement bloqués par l'hôte destinataire. Par exemple, le système bloque tout paquet SYN transmis après une session établie.

Le système abandonne également tout paquet qui correspond à l'une des règles de préprocesseur de flux TCP suivantes, peu importe si les règles sont activées :

- 129:1
- 129:3
- 129:4
- 129:6
- 129:8
- 129:11
- 129:14 à 129:19

Le graphique de performance du nombre total de paquets bloqués suit le nombre de paquets bloqués dans les déploiements en ligne et, dans les déploiements passifs et les déploiements en ligne en mode TAP, le nombre qui aurait été bloqué dans un déploiement en ligne.

Notification explicite de congestion

Active la normalisation par paquet ou par flux des indicateurs de notification explicite de congestion (ECN), comme suit :

- sélectionnez **Paquet** pour effacer les indicateurs ECN paquet par paquet, quelle que soit la négociation.
- sélectionnez **Flux** pour effacer les indicateurs ECN flux par flux si l'utilisation d'ECN n'a pas été négociée.

Si vous sélectionnez **Flux**, vous devez également vous assurer que l'option Le préprocesseur de flux **TCP nécessite une prise de contact TCP à 3 voies** est activée pour que cette normalisation ait lieu.

Effacer les options TCP existantes

Active **Allow These TCP Options** (Autoriser ces options TCP).

Autoriser ces options TCP

Désactive la normalisation d'options TCP spécifiques que vous autorisez dans le trafic.

Le système ne normalise pas les options que vous autorisez explicitement. Il normalise les options que vous n'autorisez pas explicitement en définissant les options sur No Operation (option 1 TCP).

Le système autorise toujours les options suivantes, quelle que soit la configuration des **options TCP Autoriser ces options** , car elles sont couramment utilisées pour obtenir des performances TCP optimales :

- Taille de segment maximum (MSS)
- Échelle de la fenêtre
- Horodatage TCP

Le système n'autorise pas automatiquement d'autres options moins couramment utilisées.

Vous pouvez autoriser des options spécifiques en configurant une liste de mots-clés d'options, de numéros d'options ou les deux, séparés par des virgules, comme le montre l'exemple suivant :

```
sack, echo, 19
```

La définition d'un mot-clé d'option revient à préciser le numéro d'une ou de plusieurs options TCP associées au mot-clé. Par exemple, définir `sack` revient à définir les options TCP 4 (accusé de réception sélectif autorisé) et 5 (accusé de réception sélectif). Les mots-clés d'options ne sont pas sensibles à la casse.

Vous pouvez également spécifier `any`, qui autorise toutes les options TCP et désactive efficacement la normalisation de toutes les options TCP.

Le tableau suivant résume comment vous pouvez spécifier les options TCP à autoriser. Si vous laissez ce champ vide, le système autorise uniquement les options MSS, Échelle de fenêtre et Horodatage.

Précisez...	Pour autoriser...
sack	Options TCP 4 (accusé de réception sélectif autorisé) et 5 (accusé de réception sélectif)
echo	TCP options 6 (Echo Request) et 7 (Echo Reply)
partial_order	TCP options 9 (Connexion de commande partielle autorisée) et 10 (Profil de service de commande partielle)
conn_count	Options 11 (CC), 12 (CC.New) et 13 (CC.Echo) du nombre de connexions TCP

Précisez...	Pour autoriser...
alt_checksum	Options TCP 14 (autre demande de somme de contrôle) et 15 (autre somme de contrôle)
md5	TCP option 19 (signature MD5)
le numéro de l'option, 2 à 255	une option précise, y compris les options pour lesquelles il n'y a aucun mot-clé
Tous	toutes les options TCP; ce paramètre désactive efficacement la normalisation des options TCP

Lorsque vous ne spécifiez `any` (tout) pour cette option, les normalisations comprennent les éléments suivants :

- à l'exception de MSS, de l'échelle de la fenêtre, de l'horodatage et de toutes les options explicitement autorisées, définit tous les octets d'option sur Aucune opération (option 1 de TCP)
- définit les octets de l'horodatage sur No Operation si l'horodatage est présent mais non valide, ou valide mais non négocié
- bloque le paquet si l'horodatage est négocié, mais absent
- efface le champ d'option de réponse Echo d'horodatage (TSecr) si le bit de contrôle d'accusé de réception (ACK) n'est pas activé
- définit les options MSS etÉchelle de fenêtre sur Aucune opération TCP (option 1) si le bit de contrôle SYN n'est pas activé

Configuration de la normalisation en ligne

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.

Avant de commencer

- Si vous souhaitez normaliser ou abandonner les paquets fautifs, activez le **mode en ligne** comme décrit dans Modification du trafic de préprocesseur dans les déploiements en ligne. Le périphérique géré doit également être déployé en ligne.

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 (PAS le signe d'insertion; cliquez sur le mot).

Étape 5 Si la **normalisation en ligne** sous **les préprocesseurs de transport/couche réseau** est désactivée, cliquez sur **Enabled** (Activée).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Normalisation de l'insertion**.

Étape 7 Définissez les options décrites dans Le préprocesseur de normalisation en ligne, à la page 7.

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 que l'option de normalisation en ligne TTL minimale génère des incidents d'intrusion, activez l'une des règles de décodeur de paquets ou les deux règles de décodeur de paquets 116:429 (IPv4) et 116:270 (IPv6). Pour plus de renseignements, consultez Définition des états des règles d'intrusion etOptions de normalisation en ligne, à la page 8.
- Déployer les changements de configuration.

Sujets connexes

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

Le préprocesseur de défragmentation IP

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.

Lorsqu'un datagramme IP est fragmenté en deux datagrammes IP plus petits ou plus, car sa taille est supérieure à l'unité de transmission maximale (MTU), il est *fragmenté*. Un seul fragment de datagramme IP peut ne pas contenir assez d'informations pour identifier une attaque cachée. Les attaquants peuvent tenter d'éviter la détection en transmettant les données d'attaque dans des paquets fragmentés. Le préprocesseur de défragmentation IP réassemble les datagrammes IP fragmentés avant que le moteur de règles n'exécute des règles à leur encontre, afin que les règles puissent identifier de manière plus appropriée les attaques dans ces paquets. Si les datagrammes fragmentés ne peuvent pas être réassemblés, les règles ne s'appliquent pas à eux.

Exploits de fragmentation IP

L'activation de la défragmentation IP vous aide à détecter les attaques contre les hôtes de votre réseau, comme l'attaque « Tear Drop », et les attaques de consommation de ressources contre le système lui-même, comme l'attaque JoLT2.

L'attaque Tear Drop exploite un bogue de certains systèmes d'exploitation qui les fait planter lors de la tentative de réassemblage de fragments IP qui se chevauchent. Lorsqu'il est activé et configuré pour cela, le préprocesseur de défragmentation IP identifie les fragments qui se chevauchent. Le préprocesseur de défragmentation IP détecte les premiers paquets d'une attaque par fragments en chevauchement telle que « Tear Drop », mais ne détecte pas les paquets suivants pour la même attaque.

L'attaque JoLT2 envoie un grand nombre de copies d'un même paquet IP fragmenté afin d'essayer de surutiliser les défragmenteurs IP et de provoquer une attaque par déni de service. Un plafond de l'utilisation de la mémoire perturbe cette attaque et d'autres similaires dans le préprocesseur de défragmentation IP et place la conservation du système au-dessus d'une inspection exhaustive. Le système n'est pas submergé par l'attaque, reste opérationnel et continue d'inspecter le trafic réseau.

Les différents systèmes d'exploitation réassemblent les paquets fragmentés de différentes manières. Les attaquants qui peuvent déterminer quels systèmes d'exploitation vos hôtes exécutent peuvent également fragmenter les paquets malveillants afin qu'un hôte cible les rassemble d'une manière spécifique. Étant donné que le système ne connaît pas les systèmes d'exploitation des hôtes de votre réseau surveillé, le préprocesseur peut se rassembler et inspecter les paquets de manière incorrecte, permettant ainsi à un exploit de passer sans être détecté. Pour atténuer ce type d'attaque, vous pouvez configurer le préprocesseur de défragmentation pour utiliser la méthode appropriée de défragmentation des paquets pour chaque hôte de votre réseau.

Notez que vous pouvez également utiliser Mises à niveau des profils adaptatifs dans un déploiement passif pour sélectionner de manière dynamique les politiques basées sur la cible pour le préprocesseur de défragmentation IP à l'aide des informations du système d'exploitation hôte pour l'hôte cible dans un paquet.

Politiques de défragmentation basée sur la cible

Le système d'exploitation d'un hôte utilise trois critères pour déterminer les fragments de paquet à favoriser lors du réassemblage du paquet :

- l'ordre dans lequel le fragment a été reçu par le système d'exploitation
- son décalage (la distance entre le fragment et le début du paquet)
- ses position de début et de fin par rapport aux fragments de chevauchement.

Bien que chaque système d'exploitation utilise ces critères, les différents systèmes d'exploitation favorisent différents fragments lors du réassemblage des paquets fragmentés. Par conséquent, deux hôtes avec des systèmes d'exploitation différents sur votre réseau peuvent réassembler les mêmes fragments qui se chevauchent de manière totalement différente.

Un attaquant, connaissant le système d'exploitation de l'un de vos hôtes, pourrait tenter d'éviter la détection et d'exploiter cet hôte en envoyant du contenu malveillant masqué dans des fragments de paquets qui se chevauchent. Ce paquet, une fois réassemblé et inspecté, semble inoffensif, mais lorsqu'il est réassemblé par l'hôte cible, il contient un exploit malveillant. Cependant, si vous configurez le préprocesseur de défragmentation IP pour qu'il détecte les systèmes d'exploitation sur votre segment de réseau surveillé, il rassemblera les fragments de la même manière que l'hôte cible, ce qui lui permettra d'identifier l'attaque.

Options de défragmentation IP

Vous pouvez choisir d'activer ou de désactiver simplement la défragmentation IP; cependant, Cisco vous recommande de préciser le comportement du préprocesseur de défragmentation IP activé à un niveau plus fin.

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

Vous pouvez configurer l'option globale suivante :

Fragments préalloués

Le nombre maximal de fragments individuels que le préprocesseur peut traiter à la fois. La spécification du nombre de nœuds de fragment à préallouer active l'allocation de mémoire statique.

Mise en garde Le traitement d'un fragment individuel utilise environ 1 550 octets de mémoire. Si le préprocesseur a besoin de plus de mémoire pour traiter les fragments individuels que la limite de mémoire autorisée prédéterminée pour le périphérique géré, la limite de mémoire du périphérique prévaut.

Vous pouvez configurer les options suivantes pour chaque politique de défragmentation IP :

Réseaux

L'adresse IP de l'hôte ou des hôtes auxquels vous souhaitez appliquer la politique de défragmentation.

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 spécifier 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

La politique de défragmentation que vous souhaitez utiliser pour un ensemble d'hôtes sur votre segment de réseau surveillé.

Vous pouvez sélectionner l'une des sept politiques de défragmentation, selon le système d'exploitation de l'hôte cible. Le tableau suivant répertorie les sept politiques et les systèmes d'exploitation qui utilisent chacune d'elles. Le prénom et le nom des politiques indiquent si ces politiques encouragent les paquets d'origine ou les paquets ultérieurs qui se chevauchent.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Tableau 1 : Politiques de défragmentation basée sur la cible

Politique	Systèmes d'exploitation
BSD	AIX FreeBSD IRIX VAX/VMS
BSD-right	HP JetDirect
Prénom	Mac OS HP-UX
Linux	Linux OpenBSD
Nom de famille	Cisco IOS
Solaris	SunOS
Windows	Windows

Délai d'expiration

Spécifie le temps maximal, en secondes, que le moteur de préprocesseur peut utiliser pour réassembler un paquet fragmenté. Si le paquet ne peut pas être réassemblé dans la période spécifiée, le moteur de préprocesseur arrête de tenter de réassembler le paquet et élimine les fragments reçus.

TTL minimum

Spécifie la valeur TTL minimale acceptable qu'un paquet peut avoir. Cette option détecte les attaques par insertion basées sur la durée de vie (TTL).

Vous pouvez activer la règle 123:11 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter les anomalies

Détermine les problèmes de fragmentation, tels que les fragments qui se chevauchent.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Vous pouvez activer les règles suivantes pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option :

- 123:1 à 123:4
- 123:5 (politique BSD)
- 123:6 à 123:8

Limite de chevauchement

Spécifie que lorsque le nombre configuré de segments qui se chevauchent dans une session a été détecté, la défragmentation s'arrête pour cette session.

Vous devez activer la **détection des anomalies** pour configurer cette option. Un champ vide désactive cette option. La valeur 0 spécifie un nombre illimité de segments qui se chevauchent.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes. Les fragments qui se chevauchent sont toujours abandonnés sur ces interfaces.

Vous pouvez activer la règle 123:12 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Taille de fragment minimale

Spécifie que lorsqu'un autre fragment, plus petit que le nombre d'octets configuré, est détecté, le paquet est considéré comme malveillant.

Vous devez activer la **détection des anomalies** pour configurer cette option. Un champ vide désactive cette option. La valeur 0 spécifie un nombre illimité d'octets.

Vous pouvez activer la règle 123:13 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Configuration de la défragmentation IP

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 **défragmentation IP** sous **Préprocesseurs de transport ou de couche réseau** est désactivée, cliquez sur **Enabled** (Activée).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Défragmentation IP**.

Étape 7 Si vous le souhaitez, saisissez une valeur dans le **champ Fragments préalloués**.

Étape 8 Vous avez les choix suivants :

- Add a server Profile (ajouter un profil de serveur) : cliquez sur **Ajouter** (+) à côté de **Serveurs** sur le côté gauche de la page, saisissez une valeur dans le champ **Host Address** (adresse de l'hôte) 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 créer un total de 255 politiques basées sur la cible, y compris la politique par défaut.
- Edit a server Profile (modifier un profil de serveur) : cliquez sur l'adresse configurée pour sous **Servers** (serveurs) sur le côté gauche de la page, ou cliquez sur **Default** (par défaut).
- Supprimer un profil : cliquez sur **Supprimer** (🗑) à côté de la politique.

Étape 9 Modifiez les options décrites dans Options de défragmentation IP, à la page 16.

Étape 10 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 défragmentation IP (GID 123). Pour plus de renseignements, consultez les sections Définition des états des règles d'intrusion et Options de défragmentation IP, à la page 16.
- Déployer les changements de configuration.

Sujets connexes

Principes de base des couches

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

Le décodeur de paquets

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.

Avant d'envoyer des paquets capturés à un préprocesseur, le système envoie d'abord les paquets au décodeur de paquets. Le décodeur de paquets convertit les en-têtes de paquets et les charges utiles dans un format que les préprocesseurs et le moteur de règles peuvent facilement utiliser. Chaque couche de pile est décodée à tour de rôle, en commençant par la couche de liaison de données jusqu'aux couches de réseau et de transport.

Options du décodeur de paquets

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

Décoder le canal de données GTP

Décode le canal de données GTP (General Packet Radio Service [GPRS] Tunneling Protocol) encapsulé. Par défaut, le décodeur décode les données de la version 0 sur le port 3386 et les données de la version 1 sur le port 2152. Vous pouvez utiliser la variable par défaut `GTP_PORTS` pour modifier les ports qui identifient le trafic GTP encapsulé.

Vous pouvez activer les règles 116:297 et 106:298 du générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter le Teredo sur les ports non standard

Inspecte la tunnellisation Teredo du trafic IPv6 qui est identifié sur un port UDP autre que le port 3544.

Le système inspecte toujours le trafic IPv6 lorsqu'il est présent. Par défaut, l'inspection IPv6 comprend les schémas de tunnellisation 4en6, 6in4, 6to4 et 6in6, ainsi que la tunnellisation Teredo lorsque l'en-tête UDP spécifie le port 3544.

Dans un réseau IPv4, les hôtes IPv4 peuvent utiliser le protocole Teredo pour canaliser le trafic IPv6 par l'intermédiaire d'un périphérique NAT (Network Address Translation ou NAT). Teredo encapsule les paquets IPv6 dans les datagrammes UDP IPv4 pour permettre la connectivité IPv6 derrière un périphérique NAT IPv4. Le système utilise normalement le port UDP 3544 pour identifier le trafic Teredo. Cependant, un attaquant pourrait utiliser un port non standard pour éviter d'être détecté. Vous pouvez activer la **détection Teredo sur les ports non standard** pour que le système inspecte toutes les charges utiles UDP à la recherche de tunnellisation Teredo.

Le décodage Teredo se produit uniquement sur le premier en-tête UDP et uniquement lorsqu'IPv4 est utilisé pour la couche réseau externe. Lorsqu'une deuxième couche UDP est présente après la couche Teredo IPv6 en raison de données UDP encapsulées dans les données IPv6, le moteur de règles utilise les règles de prévention des intrusions UDP pour analyser les couches UDP interne et externe.

Notez que les règles de prévention des intrusions 12065, 12066, 12067 et 12068 de la catégorie de règles **politique-autre**) détectent le trafic Teredo, mais ne les décodent pas. Vous pouvez également utiliser ces règles pour abandonner le trafic Teredo dans un déploiement en ligne. cependant, vous devez vous assurer

que ces règles sont désactivées ou définies pour générer des événements sans perte de trafic lorsque vous activez la **détection Teredo sur les ports non standard**.

Détecter la valeur de la longueur excessive

Détecte lorsque l'en-tête du paquet spécifie une longueur de paquet supérieure à la longueur réelle de paquet.

Cette option est ignorée pour les interfaces défense contre les menaces routées, transparentes et en ligne. Les paquets qui ont une longueur d'en-tête excessive sont toujours abandonnés. Toutefois, cette option ne s'applique qu'aux interfaces passives et défense contre les menaces en ligne.

Vous pouvez activer les règles 116:6, 106:47, 115:27 et 256:275 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter les options IP non valides

Détecte les options d'en-tête IP non valides pour identifier les exploitations qui utilisent des options IP non valides. Par exemple, il y a une attaque par déni de service contre un pare-feu qui entraîne le blocage du système. Le pare-feu tente d'analyser les options d'horodatage et d'adresse IP de sécurité non valides et ne parvient pas à vérifier une longueur de zéro, ce qui provoque une boucle infinie irrécupérable. Le moteur de règles identifie l'option de longueur nulle et fournit des informations que vous pouvez utiliser pour atténuer l'attaque au niveau du pare-feu.

Les périphériques Défense contre les menaces abandonneront tout paquet RSVP qui contient des options IP autres que les options alerte de routeur, fin de liste d'options (EOOL) et aucune opération (NOP) sur les interfaces routées ou transparentes. Pour les interfaces en ligne, Tap (Inline Tap) ou passives, les options IP seront gérées comme décrit ci-dessus.

Vous pouvez activer les règles 116:4 et 115:5 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter les options TCP expérimentales

Détecte les en-têtes TCP avec des options TCP expérimentales. Le tableau suivant décrit ces options.

Option TCP	Description
9	Connexion d'ordre partiel autorisée
10	Profil de service d'ordre partiel
14	Autre requête de somme de contrôle
15	Autres données de somme de contrôle
18	Somme de contrôle de queue
20	Normes du protocole de communication spatiale (SCPS)
21	Accusés de réception négatifs sélectifs (SCPS)
22	Limites d'enregistrement (SCPS)
23	Corruption (SPCS)
24	SNAP

Option TCP	Description
26	Filtre de Compression TCP

Puisqu'il s'agit d'options expérimentales, certains systèmes ne les prennent pas en compte et peuvent être sujets à des exploits.

Remarque En plus des options expérimentales énumérées dans le tableau ci-dessus, le système considère toute option TCP avec un numéro d'option supérieur à 26 comme expérimentale.

Vous pouvez activer la règle 116:58 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter les options TCP obsolètes

Détecte les en-têtes TCP avec des options TCP obsolètes. Puisqu'il s'agit d'options obsolètes, certains systèmes ne les prennent pas en compte et peuvent être exposés aux exploits. Le tableau suivant décrit ces options.

Option TCP	Description
6	Écho
7	Message Echo Reply
16	SKeeter
17	Bubba
19	Signature MD5
25	Non attribué

Vous pouvez activer la règle 116:57 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter T/TCP

Détecte les en-têtes TCP avec l'option CC.ECHO. L'option CC.ECHO confirme que TCP pour les transactions (T/TCP) est utilisé. Comme les options d'en-tête T/TCP ne sont pas très répandues, certains systèmes ne les prennent pas en compte et peuvent être exposés à des exploits.

Vous pouvez activer la règle 116:56 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter les autres options TCP

Détecte les en-têtes TCP avec des options TCP non valides non détectées par d'autres options d'événement de décodage TCP. Par exemple, cette option détecte les options TCP avec une longueur incorrecte ou avec une longueur qui place les données d'option en dehors de l'en-tête TCP.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes. Les paquets qui ont des options TCP non valides sont toujours abandonnés.

Vous pouvez activer les règles 116:54, 115:55 et 115:59 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter les anomalies d'en-tête de protocole

Détecte les autres erreurs de décodage non détectées par les options de décodeur IP et TCP plus spécifiques. Par exemple, le décodeur peut détecter un en-tête de protocole de liaison de données mal formé.

Cette option est ignorée pour les interfaces défense contre les menaces routées, transparentes et en ligne. Les paquets qui ont des anomalies d'en-tête sont toujours abandonnés. Toutefois, cette option ne s'applique aux interfaces passives et en ligne de Threat Defense.

Pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option, vous pouvez activer l'une des règles suivantes :

GID:SID	Génère un événement si :
116:467	Le paquet est inférieur à la taille minimale d'un paquet encapsulé avec un en-tête Cisco FabricPath.
116:468	Le champ de métadonnées Cisco (CMD) de l'en-tête contient une longueur d'en-tête inférieure à la taille minimale d'un en-tête CMD valide. Le champ CMD est associé au protocole Cisco Trustsec.
116:469	Le champ CMD dans l'en-tête contient une longueur de champ non valide.
116:470	Le champ CMD dans l'en-tête contient un type d'option de balise de groupe de sécurité (SGT) non valide.
116:471	Le champ CMD dans l'en-tête contient une balise SGT avec une valeur réservée.

Vous pouvez également activer une règle de décodeur de paquets non associée à d'autres options de décodeur de paquets.

Sujets connexes

Variables prédéfinies par défaut

Configuration du décodage des paquets

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 le **décodage de paquets** sous **Préprocesseurs de transport ou de couche réseau** est désactivé, cliquer sur **Enabled** (Activé).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Packet Décodage (décodage** de paquets) .

Étape 7 Activer ou désactiver les options décrites dans Options du décodeur de paquets, à la page 20.

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 décodeur de paquets (GID 116). Pour plus de renseignements, consultez les sections Définition des états des règles d'intrusion et Options du décodeur de paquets, à la page 20.
- Déployer les changements de configuration.

Sujets connexes

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

Prétraitement du flux TCP

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 TCP définit divers états dans lesquels des connexions peuvent exister. Chaque connexion TCP est identifiée par les adresses IP source et de destination et les ports source et de destination. TCP n'autorise qu'une seule connexion à la fois avec les mêmes valeurs de paramètres de connexion.

Exploits TCP liés à l'état

Si vous ajoutez le mot-clé `flow` avec l'argument `established` à une règle de prévention des intrusions, le moteur de règles de prévention des intrusions inspecte les paquets correspondant à la règle et à la directive flow en mode dynamique. Le mode avec état évalue uniquement le trafic qui fait partie d'une session TCP établie avec une prise de contact tridirectionnelle légitime entre un client et un serveur.

Vous pouvez configurer le système pour que le préprocesseur détecte tout trafic TCP qui ne peut pas être identifié dans le cadre d'une session TCP établie, bien que cela ne soit pas recommandé pour une utilisation typique, car les événements sur téléverser aient rapidement le système et ne fourniraient pas de données significatives.

Les attaques de type « stick and snot » utilisent les ensembles de règles extensifs du système et l'inspection des paquets contre elles-mêmes. Ces outils génèrent des paquets en fonction des modèles des règles de prévention des intrusions basées sur Snort et les envoient sur le réseau. Si vos règles n'incluent pas le mot-clé `flow` ou `flowbits` pour les configurer pour l'inspection dynamique, chaque paquet déclenchera la règle, surchargeant le système. L'inspection dynamique vous permet d'ignorer ces paquets, car ils ne font pas partie d'une session TCP établie et ne fournissent pas d'informations significatives. Lors de l'exécution de l'inspection dynamique, le moteur de règles ne détecte que les attaques qui font partie d'une session TCP établie, ce qui permet aux analystes de se concentrer sur celles-ci plutôt que sur le volume d'événements causés par les intrusions stick or snot.

Politiques TCP basées sur la cible

Les systèmes d'exploitation peuvent mettre en œuvre le protocole TCP de différentes manières. Par exemple, Windows et certains autres systèmes d'exploitation exigent un segment de réinitialisation TCP pour avoir un numéro de séquence TCP précis afin de réinitialiser une session, tandis que Linux et d'autres systèmes d'exploitation autorisent une plage de numéros de séquence. Dans cet exemple, le préprocesseur de flux doit comprendre exactement comment l'hôte de destination répondra à la réinitialisation en fonction du numéro de séquence. Le préprocesseur du flux arrête de suivre la session uniquement lorsque l'hôte de destination considère la réinitialisation comme valide, de sorte qu'une attaque ne peut pas échappé à la détection en envoyant des paquets après que le préprocesseur ait cessé d'inspecter le flux. Les autres variations des implémentations de TCP comprennent des éléments tels que si un système d'exploitation utilise une option d'horodatage TCP et, si oui, comment il gère l'horodatage, et si un système d'exploitation accepte ou ignore les données dans un paquet SYN.

Les différents systèmes d'exploitation réassemblent également les segments TCP qui se chevauchent de différentes manières. Le chevauchement des segments TCP pourrait refléter des retransmissions normales de trafic TCP non reconnu. Ils peuvent également correspondre à une tentative d'un agresseur, connaissant le système d'exploitation de l'un de vos hôtes, d'éviter la détection et d'exploiter cet hôte en envoyant du contenu malveillant masqué dans des segments qui se chevauchent. Cependant, vous pouvez configurer le préprocesseur de flux pour qu'il détecte les systèmes d'exploitation sur votre segment de réseau surveillé afin qu'il réassemble les segments de la même manière que l'hôte cible, ce qui lui permet d'identifier l'attaque.

Vous pouvez créer une ou plusieurs politiques TCP pour adapter l'inspection et le assemblage des flux TCP aux différents systèmes d'exploitation de votre segment de réseau surveillé. Pour chaque politique, vous définissez l'une des 13 politiques de système d'exploitation. Vous liez chaque politique TCP à une adresse IP ou à un bloc d'adresses spécifique en utilisant autant de politiques TCP que nécessaire pour identifier une

partie ou l'ensemble des hôtes à l'aide d'un système d'exploitation différent. La politique TCP par défaut s'applique à tous les hôtes du réseau surveillé que vous n'identifiez dans aucune autre politique TCP. Il n'est donc pas nécessaire de préciser une adresse IP ou un bloc d'adresses pour la politique TCP par défaut.

Notez que vous pouvez également utiliser Mises à niveau des profils adaptatifs dans un déploiement passif pour sélectionner de manière dynamique les politiques basées sur la cible pour le préprocesseur de flux TCP à l'aide des informations du système d'exploitation hôte pour l'hôte cible dans un paquet.

Réassemblage des flux TCP

Le préprocesseur de flux collecte et réassemble tous les paquets qui font partie d'un flux de communication serveur à client, d'un flux de communication client à serveur ou des deux d'une session TCP. Cela permet au moteur de règles d'inspecter le flux comme une entité unique réassemblée plutôt que d'inspecter uniquement les paquets individuels qui font partie d'un flux donné.

Le réassemblage de flux permet au moteur de règles d'identifier les attaques basées sur les flux, qu'il peut ne pas détecter lors de l'inspection de paquets individuels. Vous pouvez spécifier les flux de communication que le moteur de règles rassemble en fonction des besoins de votre réseau. Par exemple, lors de la surveillance du trafic sur vos serveurs Web, vous pouvez ne vouloir inspecter que le trafic client, car vous êtes beaucoup moins susceptible de recevoir du trafic malveillant de votre propre serveur Web.

Dans chaque politique TCP, vous pouvez spécifier une liste de ports séparés par des virgules pour identifier le trafic à réassembler par le préprocesseur de flux. Si Mises à niveau des profils adaptatifs est activé, vous pouvez également répertorier les services qui identifient le trafic à réassembler, soit comme alternative aux ports, soit en combinaison avec les ports.

Vous pouvez préciser les ports, les services ou les deux. Vous pouvez définir des listes de ports distinctes pour n'importe quelle combinaison de ports clients, de ports de serveur ou des deux. Vous pouvez également définir des listes de services distinctes pour n'importe quelle combinaison de services client, de services de serveur ou des deux. Par exemple, supposons que vous vouliez réassembler les éléments suivants :

- Trafic SMTP (port 25) du client
- Réponses du serveur FTP (port 21)
- trafic telnet (port 23) dans les deux sens

Vous pourriez configurer les éléments suivants :

- Pour les ports client, spécifiez `23, 25`
- Pour les ports de serveur, spécifiez `21, 23`

Sinon, vous pouvez configurer les éléments suivants :

- Pour les ports client, spécifiez `25`
- Pour les ports de serveur, spécifiez `21`
- Pour les deux ports, spécifiez `23`

De plus, prenez l'exemple suivant qui combine les ports et les services et serait valide lorsque Mises à niveau des profils adaptatifs est activé :

- Pour les ports client, spécifiez `23`
- Pour les services clients, spécifiez `smtp`

- Pour les ports de serveur, spécifiez `21`
- Pour les services de serveur, spécifiez `Telnet`

La suppression d'un port (par exemple, `!80`) peut améliorer les performances en empêchant le préprocesseur de flux TCP de traiter le trafic pour ce port.

Bien que vous puissiez également spécifier `les all` comme l'argument pour permettre le assemblage pour tous les ports, Cisco ne recommande **pas** de définir les ports à `all` (tous les ports), car cela pourrait augmenter le volume de trafic inspecté par ce préprocesseur et diminuer les performances inutilement.

Le réassemblage de TCP inclut automatiquement et de manière transparente les ports que vous ajoutez à d'autres préprocesseurs. Cependant, si vous ajoutez explicitement des ports aux listes de réassemblage TCP que vous avez ajoutées à d'autres configurations de préprocesseur, ces ports supplémentaires sont gérés normalement. Cela comprend les listes de ports pour les préprocesseurs suivants :

- FTP/Telnet (FTP au niveau du serveur)
- DCE/RPC
- Inspection HTTP
- SMTP
- Protocole d'initiation de session (SIP)
- POP
- IMAP
- SSL

Notez que le réassemblage de types de trafic supplémentaires (client, serveur, les deux) augmente les demandes en ressources.

Options de prétraitement du flux TCP

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

Vous pouvez configurer l'option TCP globale suivante :

Amélioration de la performance de type de paquet

Permet d'ignorer le trafic TCP pour tous les ports et protocoles d'application qui ne sont pas spécifiés dans les règles de prévention des intrusions activées, sauf lorsqu'une règle TCP avec les ports source et de destination définis sur `any` comporte une option `flow` ou `flowbits`. Cette amélioration des performances pourrait se traduire par des attaques manquées.

Vous pouvez configurer les options suivantes pour chaque politique TCP.

Réseau

Spécifie les adresses IP de l'hôte auxquelles vous souhaitez appliquer la politique de réassemblage de flux TCP.

Vous pouvez spécifier une adresse IP unique ou un bloc d'adresses. Vous pouvez spécifier 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

Identifie le système d'exploitation de la politique TCP de l'hôte ou des hôtes cibles. Si vous sélectionnez une politique autre que **Mac OS**, le système supprime les données des paquets de synchronisation (SYN) et désactive la génération d'événements pour la règle 129:2. Notez que l'activation de l'option **Supprimer les données sur SYN** du préprocesseur de normalisation en ligne désactive également la règle 129:2.

Le tableau suivant identifie les politiques de système d'exploitation et les systèmes d'exploitation hôtes qui utilisent chacune.

Tableau 2 : Politiques du système d'exploitation TCP

Politique	Systèmes d'exploitation
Prénom	système d'exploitation inconnu
Nom de famille	Cisco IOS
BSD	AIX FreeBSD OpenBSD
Linux	Noyau Linux 2.4 Noyau Linux 2.6
Ancien Linux	Noyau Linux 2.2 et antérieur
Windows	Windows 98 Windows NT Windows 2000 Windows XP
Windows 2003	Windows 2003
Windows Vista	Windows Vista

Politique	Systèmes d'exploitation
Solaris	Système d'exploitation Cisco Solaris SunOS
IRIX	SGI Irix
HPUX	HP-UX 11.0 ou version ultérieure
HPUX 10	HP-UX 10.2 ou version antérieure
Mac OS	Mac OS (Mac OS 10)

Astuces La politique Premier système d'exploitation peut offrir une certaine protection lorsque vous ne connaissez pas le système d'exploitation hôte. Cependant, elle peut entraîner des attaques manquées. Vous devez modifier la politique pour spécifier le système d'exploitation approprié si vous le connaissez.

Délai d'expiration

Nombre de secondes entre 1 et 86400 pendant lesquelles le moteur de règles de prévention des intrusions maintient un flux inactif dans la table d'état. Si le flux n'est pas réassemblé dans le délai spécifié, le moteur de règles de prévention des intrusions le supprime de la table d'état.

Remarque Si votre périphérique géré est déployé sur un segment où le trafic réseau est susceptible d'atteindre les limites de la bande passante du périphérique, vous devriez envisager de définir cette valeur plus élevée (par exemple, à 600 secondes) pour réduire le surdébit de traitement.

Les périphériques défense contre les menaces ignorent cette option et utilisent plutôt les paramètres de la politique de service de contrôle d'accès avancé **(Threat Defense Service Policy)**. Consultez Configurer une règle de politique de service pour obtenir de plus amples renseignements.

Fenêtre TCP maximale

Spécifie la taille maximale de la fenêtre TCP entre 1 et 1073725440 octets, autorisée comme spécifié par un hôte de réception. La définition de la valeur 0 désactive la vérification de la taille de la fenêtre TCP.

Mise en garde La limite supérieure est la taille de fenêtre maximale autorisée par la RFC et est destinée à empêcher un agresseur de se soustraire à la détection, mais la définition d'une taille de fenêtre maximale beaucoup plus grande peut entraîner un déni de service auto-imposé.

Lorsque **les anomalies d'inspection dynamique** sont activées, vous pouvez activer la règle 129:6 de générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Limite de chevauchement

Spécifie que lorsque le nombre configuré entre 0 (illimité) et 255 de segments qui se chevauchent dans une session a été détecté, le réassemblage des segments s'arrête pour cette session et, si les **anomalies d'inspection dynamique** sont activées et la règle de préprocesseur associée est activée, un événement est généré.

Vous pouvez activer la règle 129:7 de générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Facteur de purge

Dans un déploiement en ligne, le modèle précise que lorsqu'un segment de taille réduite a été détecté à la suite du nombre configuré entre 1 et 2 048 de segments de taille non décroissante, le système purge les données de segment accumulées pour la détection. La définition de la valeur 0 désactive la détection de ce modèle de segment, ce qui peut indiquer la fin d'une demande ou d'une réponse. Notez que l'option de normalisation en ligne **Normaliser la charge utile TCP** doit être activée pour que cette option soit effective.

Anomalies dans le filtrage dynamique de paquets

Détecte les comportements anormaux dans la pile TCP. L'activation des règles de préprocesseur associées peut générer de nombreux événements si les piles TCP/IP sont mal écrites.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Vous pouvez activer les règles suivantes pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option :

- 129:1 à 129:5
- 129:6 (Mac OS uniquement)
- 129:8 à 129:11
- 129:13 à 129:19

Tenez compte des points suivants :

- pour que la règle 129:6 se déclenche, vous devez également configurer une valeur supérieure à 0 pour **la Fenêtre TCP maximale**.
- pour que les règles 129:9 et 129:10 se déclenchent, vous devez également activer **le déroutement de session TCP**.

Détournement de session TCP

Détecte le détournement de session TCP en validant les adresses matérielles (MAC) détectées des deux côtés d'une connexion TCP lors de l'établissement de liaison tridirectionnelle par rapport aux paquets suivants reçus au cours de la session. Lorsque l'adresse MAC pour un côté ou l'autre ne correspond pas, si **les anomalies d'inspection dynamique** sont activées et que l'une des deux règles de préprocesseur correspondantes est activée, le système génère des événements.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Vous pouvez activer les règles 129:9 et 129:10 de générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Notez que pour que l'une de ces règles génère des événements, vous devez également activer les **anomalies d'inspection dynamique**.

Petits segments consécutifs

Lorsque **les anomalies d'inspection dynamique** sont activées, spécifie un nombre maximal de 1 à 2048 petits segments TCP consécutifs autorisés. La définition de la valeur 0 désactive la vérification des petits segments consécutifs.

Vous devez définir cette option avec l'option **Taille des petits segments**, soit en désactivant les deux, soit en définissant une valeur non nulle pour les deux. Notez que recevoir jusqu'à 2 000 segments consécutifs, même si chaque segment fait 1 octet, sans accusé de réception (ACK) constituerait beaucoup plus de segments consécutifs que ce à quoi vous vous attendez normalement.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Vous pouvez activer la règle 129:12 de générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Petit segment

Lorsque les **anomalies d'inspection dynamique** sont activées, précise la taille de segment TCP de 1 à 2048 octets qui est considérée comme petite. La définition de la valeur 0 désactive la spécification de la taille d'un petit segment.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Vous devez définir cette option avec l'option **Petits Segments consécutifs**, soit en désactivant les deux, soit en définissant une valeur non nulle pour les deux. Notez qu'un segment TCP de 2048 octets est plus grand qu'une trame Ethernet normale de 1500 octets.

Ports ignorant les petits segments

Lorsque **les anomalies d'inspection dynamique**, **les petits segments consécutifs** et la **Taille des petits segments** sont activés, spécifie une liste séparée par des virgules d'un ou de plusieurs ports qui ignorent la détection des petits segments TCP. Si vous laissez cette option à blanc, aucun port n'est ignoré.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Vous pouvez ajouter n'importe quel port à la liste, mais la liste n'affecte que les ports spécifiés dans l'une des listes de ports **Réaliser le réassemblage des flux sur** de la politique TCP.

Exiger une connexion TCP en 3 temps

Spécifie que les sessions sont traitées comme établies uniquement à l'achèvement d'une prise de contact TCP tridirectionnelle. Désactivez cette option pour augmenter les performances, vous protéger contre les attaques par inondation SYN et permettre le fonctionnement dans un environnement partiellement asynchrone. Activez-la pour éviter les attaques qui tentent de générer des faux positifs en envoyant des informations qui ne font pas partie d'une session TCP établie.

Vous pouvez activer la règle 129:20 de générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Expiration du délai de la connexion en 3 temps

Spécifie le nombre de secondes entre 0 (illimité) et 86 400 (vingt-quatre heures) avant que l'établissement de liaison ne soit terminé lorsque l'option **Exiger l'établissement de la liaison TCP tridirectionnelle** est activée. Vous devez activer l'option **Exiger l'établissement d'une liaison TCP tridirectionnelle** pour modifier la valeur de cette option.

Pour les périphériques logiciels Firepower et les interfaces défense contre les menaces en ligne, Tap en ligne et passives, la valeur par défaut est 0. Pour les interfaces routées et transparentes défense contre les menaces , le délai d'expiration est toujours de 30 secondes; la valeur configurée ici est ignorée.

Amélioration de la performance des tailles de paquet

Définit le préprocesseur pour ne pas mettre en file d'attente de paquets volumineux dans la mémoire tampon de réassemblage. Cette amélioration des performances pourrait se traduire par des attaques manquées. Désactivez cette option pour vous protéger contre les tentatives d'évitement à l'aide de petits paquets de un à vingt octets. Activez-la lorsque vous êtes assuré qu'il n'y a pas de telles attaques, car tout le trafic est composé de très gros paquets.

Réassemblage de l'héritage

Définit le préprocesseur de flux 4 pour émuler le préprocesseur obsolète du flux 4 lors du réassemblage des paquets, ce qui vous permet de comparer les événements réassemblés par le préprocesseur de flux avec les événements basés sur le même flux de données réassemblé par le préprocesseur de flux 4.

Réseau asynchrone

Spécifie si le réseau surveillé est un réseau asynchrone, c'est-à-dire un réseau où le système ne voit que la moitié du trafic. Lorsque cette option est activée, le système ne rassemble pas les flux TCP pour augmenter les performances.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Effectuer le réassemblage de flux sur les ports client

Active le réassemblage du flux en fonction des ports pour le côté client de la connexion. En d'autres termes, il réassemble les flux destinés aux serveurs Web, aux serveurs de messagerie ou à d'autres adresses IP généralement définies par les adresses IP spécifiées dans $Home_NET. Utilisez cette option lorsque vous vous attendez à ce que le trafic malveillant provienne des clients.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Effectuer le réassemblage de flux sur les services client

Active le réassemblage du flux en fonction des services pour le côté client de la connexion. Utilisez cette option lorsque vous vous attendez à ce que le trafic malveillant provienne des clients.

Au moins un détecteur client doit être activé pour chaque service client que vous sélectionnez. Par défaut, tous les détecteurs fournis par Cisco sont activés. Si aucun détecteur n'est activé pour une application client associée, le système active automatiquement tous les détecteurs fournis par Cisco pour l'application; s'il n'en existe aucun, le système active le détecteur défini par l'utilisateur modifié le plus récemment pour l'application.

Cette fonctionnalité nécessite des licences de protection et de contrôle.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Effectuer le réassemblage de flux sur les ports du serveur

Active le réassemblage du flux en fonction des ports pour le côté du serveur de la connexion uniquement. En d'autres termes, il réassemble les flux provenant de serveurs Web, de serveurs de messagerie ou d'autres adresses IP généralement définies par les adresses IP spécifiées dans $EXTERNAL_NET. Utilisez cette option

lorsque vous souhaitez surveiller les attaques côté serveur. Vous pouvez désactiver cette option en ne précisant pas les ports.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Remarque Pour une inspection approfondie d'un service, ajoutez le nom du service dans le champ Perform Stream Reassembly on Server Services (Effectuer le réassemblage des flux sur les services du serveur) en plus d'ajouter le numéro de port dans le champ Perform Stream Reassembly on Server Ports (Effectuer le réassemblage des flux sur les ports du serveur). Par exemple, ajoutez le service **« `HTTP` »** dans le champ Perform Stream Reassembly on Server Services pour inspecter le service HTTP en plus d'ajouter le port numéro 80 dans le champ Perform Stream Reassembly on Server Ports.

Effectuer le réassemblage de flux sur les services de serveur

Active le réassemblage des flux en fonction des services pour le côté serveur de la connexion uniquement. Utilisez cette option lorsque vous souhaitez surveiller les attaques côté serveur. Vous pouvez désactiver cette option en ne précisant pas de services.

Au moins un détecteur doit être activé. Par défaut, tous les détecteurs fournis par Cisco sont activés. Si aucun détecteur n'est activé pour un service, le système active automatiquement tous les détecteurs fournis par Cisco pour le protocole d'application associé; S'il n'en existe aucun, le système active le détecteur défini par l'utilisateur modifié le plus récemment pour le protocole d'application.

Cette fonctionnalité nécessite des licences de protection et de contrôle.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Effectuer le réassemblage de flux sur les deux ports

Active le réassemblage du flux en fonction des ports pour les côtés client et serveur de la connexion. Utilisez cette option lorsque vous prévoyez que le trafic malveillant pour les mêmes ports pourra se déplacer dans les deux sens entre les clients et les serveurs. Vous pouvez désactiver cette option en ne précisant pas les ports.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Effectuer le réassemblage de flux sur les deux services

Active le réassemblage du flux en fonction des services pour les côtés client et serveur de la connexion. Utilisez cette option lorsque vous vous attendez à ce que le trafic malveillant pour les mêmes services puisse se déplacer dans les deux sens entre les clients et les serveurs. Vous pouvez désactiver cette option en ne précisant pas de services.

Au moins un détecteur doit être activé. Par défaut, tous les détecteurs fournis par Cisco sont activés. Si aucun détecteur n'est activé pour une application cliente ou un protocole d'application associé, le système active automatiquement tous les détecteurs fournis par Cisco pour l'application ou le protocole d'application; S'il n'en existe aucun, le système active le dernier détecteur défini par l'utilisateur modifié pour l'application ou le protocole d'application.

Cette fonctionnalité nécessite des licences de protection et de contrôle.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Options de dépannage : nombre maximal d'octets en file d'attente

Le service d'assistance peut vous demander, lors d'un appel de dépannage, de préciser la quantité de données qui peut être mise en file d'attente d'un côté d'une connexion TCP. La valeur 0 spécifie un nombre illimité d'octets.

Mise en garde La modification du paramètre de cette option de dépannage affectera les performances et doit être effectuée uniquement avec les conseils du soutien.

Options de dépannage : nombre maximal de segments en file d'attente

Le service d'assistance peut vous demander, lors d'un appel de dépannage, de préciser le nombre maximal d'octets de segments de données qui peuvent être mis en file d'attente d'un côté d'une connexion TCP. La valeur 0 spécifie un nombre illimité d'octets de segments de données.

Mise en garde La modification du paramètre de cette option de dépannage affectera les performances et doit être effectuée uniquement avec les conseils du soutien.

Sujets connexes

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

Configuration du prétraitement du flux TCP

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 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 le paramètre **TCP Stream Configuration** (Configuration des flux TCP) est désactivé dans **les préprocesseurs de transport/couche réseau**, activez-le en cliquant sur **Enabled** (Activé).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Configuration des flux TCP**.

Étape 7 Cochez ou décochez la case **Packet Type Performance Boost** (Amélioration des performances des types de paquets) dans la section **Global Settings** (paramètres globaux).

Étape 8 Vous pouvez réaliser les actions suivantes :

- Ajouter une politique basée sur la cible – Cliquez sur **Ajouter** (+) à côté de **Hosts** (hôtes) dans la section Targets (Cibles). Précisez une ou plusieurs adresses IP dans le champ **Host Address (** adresse de l'hôte). Vous pouvez spécifier une adresse IP unique ou un bloc d'adresses. Vous pouvez créer un total de 255 politiques basées sur la cible, y compris la politique par défaut. Lorsque vous avez terminé, cliquez sur **OK**.
- Modifier une politique basée sur la cible existante – Sous **Hôtes**, cliquez sur l'adresse de la politique que vous souhaitez modifier ou sur par défaut pour modifier les valeurs de configuration **par défaut**.
- Modifier les options de prétraitement du flux TCP – Voir Options de prétraitement du flux TCP, à la page 27.

  Mise en garde Ne modifiez pas le **nombre maximal d'octets en file d'attente** ou le **nombre maximal de segments en file d'attente**, à moins que le service d'assistance ne vous le demande.

  Astuces Pour modifier les paramètres de réassemblage des flux en fonction du client, du serveur ou des deux services, cliquez dans le champ que vous souhaitez modifier ou cliquez sur **Edit** (modifier) à côté du champ. Utilisez la flèche pour déplacer les services entre les listes **Disponible** et **Activé** dans la fenêtre contextuelle, puis cliquez sur **OK**.

- Supprimer une politique basée sur la cible existante – Cliquez sur **Supprimer** (🗑) à côté de la politique que vous souhaitez supprimer.

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 événements et, dans un déploiement en ligne, supprimer les paquets incriminés, activez les règles de préprocesseur de flux TCP (GID 129). Pour plus de renseignements, consultez les sections Définition des états des règles d'intrusion et Options de prétraitement du flux TCP, à la page 27.
- Déployer les changements de configuration.

Sujets connexes

Gestion des couches

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

Prétraitement du flux UDP

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 prétraitement du flux UDP se produit lorsque le moteur de règles traite des paquets en fonction d'une règle UDP qui comprend le mot-clé `flow` en utilisant l'un des arguments suivants :

- `Établi`
- `Au client`
- `Du client`
- `Vers le serveur`
- `À partir du serveur`

Les flux de données UDP ne sont généralement pas considérés en termes de *sessions*. UDP est un protocole sans connexion qui ne permet pas à deux points terminaux d'établir un canal de communication, d'échanger des données et de fermer le canal. Cependant, le préprocesseur de flux utilise les champs d'adresse IP source et de destination dans l'en-tête du datagramme IP d'encapsulation et les champs de port dans l'en-tête UDP pour déterminer la direction du flux et identifier une session. Une session se termine lorsqu'une minuterie configurable est dépassée ou lorsqu'un terminal reçoit un message ICMP indiquant que l'autre terminal est inaccessible ou que le service demandé n'est pas disponible.

Notez que le système ne génère pas d'événements liés au prétraitement du flux UDP; cependant, vous pouvez activer les règles de décodeur de paquets associées pour détecter les anomalies de l'en-tête de protocole UDP.

Sujets connexes

Valeurs d'en-tête TCP et taille du flux

Options de prétraitement de flux UDP

Délai d'expiration

Spécifie la durée de secondes pendant laquelle le préprocesseur conserve un flux inactif dans la table d'état. Si des datagrammes supplémentaires ne sont pas vus dans le délai spécifié, le préprocesseur supprime le flux de la table d'état.

Les périphériques Défense contre les menaces ignorent cette option et utilisent plutôt les paramètres de la politique de service de contrôle d'accès avancé **(Threat Defense Service Policy)**. Consultez Configurer une règle de politique de service pour obtenir de plus amples renseignements.

Amélioration de la performance de type de paquet

Définit sur le préprocesseur pour ignorer le trafic UDP pour tous les ports et protocoles d'application qui ne sont pas spécifiés dans les règles activées, sauf lorsqu'une règle UDP avec les ports source et de destination définis sur `any` a une option de `flow` ou `flowbits`. Cette amélioration des performances pourrait se traduire par des attaques manquées.

Configuration du prétraitement de flux UDP

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 de flux UDP** sous **Transport/Network Layer Preprocessors** (Préprocesseurs de la couche transport/réseau) est désactivée, cliquer sur **Enabled** (Activée).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Configuration des flux UDP**.

Étape 7 Définissez les options décrites dans Options de prétraitement de flux UDP, à la page 37.

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 décodeur de paquets associées (GID 116). Pour plus de renseignements, consultez les sections Définition des états des règles d'intrusion et Le décodeur de paquets, à la page 20.
- Déployer les changements de configuration.

Sujets connexes

Gestion des couches

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

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.