Détection des menaces

Les rubriques suivantes décrivent comment configurer les statistiques de détection des menaces et l'analyse de la détection des menaces.

Détection des menaces

La détection des menaces sur l'ASA fournit une défense de première ligne contre les attaques. La détection des menaces fonctionne aux couches 3 et 4 pour développer une référence pour le trafic sur le périphérique, en analysant les statistiques sur les pertes de paquets et en accumulant les rapports « top » en fonction des modèles de trafic. En comparaison, un module qui fournit des services IPS ou IPS de nouvelle génération identifie et atténue les vecteurs d'attaque jusqu'à la couche 7 sur le trafic autorisé par l'ASA, et ne peut pas voir le trafic déjà abandonné par l'ASA. Ainsi, la détection des menaces et l'IPS peuvent fonctionner ensemble pour fournir une défense contre les menaces plus complète.

La détection des menaces comprend les éléments suivants :

- Différents niveaux de collecte de statistiques pour diverses menaces.

  Les statistiques de détection des menaces peuvent vous aider à gérer les menaces qui pèsent sur votre ASA; par exemple, si vous activez la détection des menaces par analyse, l'affichage des statistiques peut vous aider à analyser la menace. Vous pouvez configurer deux types de statistiques de détection des menaces :

  - Statistiques de détection des menaces de base : comprennent des informations sur l'activité des attaques pour le système dans son ensemble. Les statistiques de détection des menaces de base sont activées par défaut et n'ont aucune incidence sur les performances. Consultez Statistiques de détection des menaces de base, à la page 2.
  - Statistiques avancées de détection des menaces : permettent de suivre l'activité au niveau de l'objet, afin que l'ASA puisse signaler l'activité des hôtes, des ports, des protocoles ou des ACL individuels. Les statistiques de détection avancée des menaces peuvent avoir un impact majeur sur les

performances, en fonction des statistiques recueillies, de sorte que seules les statistiques d'ACL sont activées par défaut. Consultez Statistiques de détection avancée des menaces, à la page 2.

- La fonction de détection des menaces par analyse détermine quand un hôte effectue une analyse. Vous pouvez éventuellement bloquer tout hôte identifié comme constituant une menace d'analyse. Consultez Détection des menaces par analyse, à la page 3.

Statistiques de détection des menaces de base

À l'aide des statistiques de détection des menaces de base, l'ASA surveille le taux d'abandons de paquets et les événements de sécurité pour les raisons suivantes :

- Déni par les listes de contrôle d'accès.
- Mauvais format de paquet (comme invalid-ip-header ou invalid-tcp-hdr-length).
- Limites de connexion dépassées (limites de ressources à l'échelle du système et limites définies dans la configuration).
- Attaque DoS détectée (comme un SPI non valide, échec de vérification de pare-feu avec état).
- Échec des vérifications de base du pare-feu. Cette option est un débit combiné qui inclut tous les abandons de paquets liés au pare-feu dans cette liste. Il n'inclut pas les abandons non liés au pare-feu, tels que la surcharge d'interface, les échecs de paquets lors de l'inspection de l'application et les attaques par analyse détectées.
- Paquets ICMP suspects détectés.
- Paquets ayant échoué à l'inspection de l'application.
- Surcharge de l'interface.
- Attaque par analyse détectée. Cette option surveille les attaques par analyse; par exemple, le premier paquet TCP n'est pas un paquet SYN, ou la connexion TCP a échoué dans l'établissement de liaison à 3 voies. La détection des menaces d'analyse complète prend ces informations de taux d'attaque d'analyse et agit en classant les hôtes comme agresseurs et en les contournant automatiquement, par exemple.
- Session incomplète détectée, comme l'attaque TCP SYN détectée ou la session UDP sans retour de données détectée.

Lorsque l'ASA détecte une menace, il envoie immédiatement un message de journal système (733100). L'ASA suit deux types de taux : le taux moyen d'événements sur un intervalle, et le taux d'événements en rafale sur un intervalle de rafale plus court. L'intervalle de débit en rafale est de 1/30 de l'intervalle de débit moyen ou de 10 secondes, selon le plus élevé des deux. Pour chaque événement reçu, l'ASA vérifie les limites de débit moyen et de rafale; si les deux débits sont dépassés, l'ASA envoie deux messages système distincts, avec un maximum d'un message pour chaque type de débit par période de rafale.

La détection des menaces de base affecte les performances uniquement en cas d'abandon ou de menace potentielle; même dans ce scénario, l'incidence sur les performances est négligeable.

Statistiques de détection avancée des menaces

Les statistiques de détection avancée des menaces affichent les débits de trafic autorisés et abandonnés pour les objets individuels tels que les hôtes, les ports, les protocoles ou les listes de contrôle d'accès.

Mise en garde L'activation des statistiques avancées peut affecter les performances de l'ASA, selon le type de statistiques activées. L'activation des statistiques sur l'hôte a une incidence importante sur les performances ; si vous avez une charge de trafic élevée, vous pouvez envisager d'activer temporairement ce type de statistiques. Les statistiques de port ont cependant une incidence faible.

Détection des menaces par analyse

Une attaque par analyse typique se compose d'un hôte qui teste l'accessibilité de chaque adresse IP d'un sous-réseau (en analysant de nombreux hôtes dans le sous-réseau ou en balayage de nombreux ports dans un hôte ou un sous-réseau). La fonction de détection des menaces par analyse détermine quand un hôte effectue une analyse. Contrairement à la détection d'analyse IPS qui est basée sur les signatures de trafic, la fonction de détection des menaces par analyse ASA gère une base de données étendue qui contient des statistiques d'hôte pouvant être analysées pour l'activité d'analyse.

La base de données d'hôtes suit les activités suspectes telles que les connexions sans activité de retour, l'accès à des ports de service fermés, les comportements TCP vulnérables tels que les IPID non aléatoires, etc.

Si le taux de menace d'analyse est dépassé, l'ASA envoie un message syslog (733101) et bloque éventuellement l'agresseur. L'ASA suit deux types de taux : le taux moyen d'événements sur un intervalle, et le taux d'événements en rafale sur un intervalle de rafale plus court. Le taux d'événements en rafale est de 1/30 de l'intervalle de débit moyen ou de 10 secondes, selon le plus élevé des deux. Pour chaque événement détecté et considéré comme faisant partie d'une attaque par analyse, l'ASA vérifie les limites de débit moyen et de rafale. Si l'un ou l'autre de ces débits est dépassé pour le trafic envoyé par un hôte, cet hôte est considéré comme un agresseur. Si l'un ou l'autre de ces débits est dépassé pour le trafic reçu par un hôte, cet hôte est considéré comme une cible.

Le tableau suivant répertorie les limites de débit par défaut pour la détection des menaces d'analyse.

Tableau 1 : Limites de débit par défaut pour la détection des menaces par analyse

Débit moyen	Taux de rafale
5 abandons/s au cours des 600 dernières secondes.	10 abandons/s au cours des 20 dernières secondes.
5 abandons/s au cours des 3 600 dernières secondes.	10 abandons/s au cours de la dernière période de 120 secondes.

Mise en garde La fonction de détection des menaces par analyse peut affecter de manière significative les performances et la mémoire de l'ASA pendant qu'elle crée et recueille une structure de données et des informations basées sur l'hôte et le sous-réseau.

Lignes directrices pour la détection des menaces

Lignes directrices relatives au contexte de sécurité

À l'exception des statistiques sur les menaces avancées, la détection des menaces est prise en charge en mode unique uniquement. En mode multiple, les statistiques d'interception TCP sont les seules statistiques prises en charge.

Types de trafic surveillés

- Pour les statistiques, seul le trafic traversant la boîte est surveillé; le trafic vers le boîtier n'est pas surveillé.
- Le trafic refusé par une liste de contrôle d'accès ne déclenche pas la détection des menaces par analyse; seul le trafic autorisé par l'ASA et qui crée un flux est affecté par la détection des menaces d'analyse.

Paramètres par défaut pour la détection des menaces

Les statistiques de détection des menaces de base sont activées par défaut.

Le tableau suivant répertorie les paramètres par défaut. Vous pouvez afficher tous ces paramètres par défaut à l'aide de la commande **show running-config all threat-detection** dans Outils > Interface de ligne de commande.

Pour les statistiques avancées, par défaut, les statistiques pour les listes de contrôle d'accès sont activées.

Tableau 2 : Paramètres par défaut de détection de base des menaces

Raison de l'abandon du paquet	Paramètres de déclenchement	
	Taux moyen	**Taux de rafale**
• Attaque par déni de service détectée	100 abandons/s au cours des 600 dernières secondes.	400 abandons/s au cours de la dernière période de 20 secondes.
• Mauvais format de paquet • Limite de connexion dépassée • Paquets ICMP suspects détectés	80 abandons/s au cours des 3 600 dernières secondes.	320 abandons/s au cours de la dernière période de 120 secondes.
Attaque par analyse détectée.	5 abandons/s au cours des 600 dernières secondes.	10 abandons/s au cours des 20 dernières secondes.
	4 abandons/s au cours des 3 600 dernières secondes.	8 abandons/s au cours des 120 dernières secondes.
Session incomplète détectée, comme une attaque TCP SYN détectée ou une session UDP sans retour de données détectée (combinées)	100 abandons/s au cours des 600 dernières secondes.	200 abandons/s au cours des 20 dernières secondes.
	80 abandons/s au cours des 3 600 dernières secondes.	160 abandons/s au cours des 120 dernières secondes.

Raison de l'abandon du paquet	Paramètres de déclenchement	
	Taux moyen	**Taux de rafale**
Refus par les listes de contrôle d'accès	400 abandons/s au cours des 600 dernières secondes.	800 abandons/s au cours des 20 dernières secondes.
	320 abandons/s au cours des 3 600 dernières secondes.	640 abandons/s au cours des 120 dernières secondes.
• Échec des vérifications de base du pare-feu	400 abandons/s au cours des 600 dernières secondes.	1 600 abandons/s au cours des 20 dernières secondes.
• Paquets ayant échoué à l'inspection de l'application.	320 abandons/s au cours des 3 600 dernières secondes.	1 280 abandons/s au cours des 120 dernières secondes.
Surcharge d'interface	2 000 abandons/s au cours des 600 dernières secondes.	8 000 abandons/s au cours des 20 dernières secondes.
	1 600 abandons/s au cours des 3 600 dernières secondes.	6 400 abandons/s au cours de la dernière période de 120 secondes.

Configurer la détection des menaces

Les statistiques de détection des menaces de base sont activées par défaut et peuvent être le seul service de détection des menaces dont vous avez besoin. Utilisez la procédure suivante si vous souhaitez mettre en œuvre des services de détection des menaces supplémentaires.

Procédure

Étape 1 Configurer les statistiques de base sur la détection des menaces, à la page 5.

Les statistiques de détection de base des menaces comprennent les activités qui peuvent être liées à une attaque, comme une attaque DoS.

Étape 2 Configurer les statistiques de détection avancée des menaces, à la page 6.

Étape 3 Configurer l'analyse de détection des menaces, à la page 7.

Configurer les statistiques de base sur la détection des menaces

Les statistiques de détection des menaces de base sont activées par défaut. Vous pouvez les désactiver ou les réactiver si vous les avez désactivées.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Threat Detection (Détection des menaces)**

Étape 2 Sélectionnez ou désélectionnez **la fonction Enable Basic Threat Détection (activer la détection des menaces de base)** comme vous le souhaitez.

Étape 3 Cliquez sur **Apply** (Appliquer).

Configurer les statistiques de détection avancée des menaces

Vous pouvez configurer l'ASA pour collecter des statistiques détaillées. Par défaut, les statistiques pour les listes de contrôle d'accès sont activées. Pour activer d'autres statistiques, procédez comme suit.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Threat Detection (Détection des menaces)**

Étape 2 Dans la zone Scanning Threat Statistics (Statistiques des menaces d'analyse), choisissez l'une des options suivantes :

- **Enable All Statistics (Activer toutes les statistiques)**.
- **Disable All Statistics (Désactiver toutes les statistiques)**.
- **Enable Only Following Statistics (Activer uniquement les statistiques suivantes)**.

Étape 3 Si vous avez choisi **Enable Only Following Statistics (Activer uniquement les statistiques suivantes)**, sélectionnez une ou plusieurs des options suivantes :

- **Hosts (Hôtes)** : active les statistiques de l'hôte. Les statistiques sur l'hôte s'accumulent tant que l'hôte est actif et dans la base de données de l'hôte de menace d'analyse. L'hôte est supprimé de la base de données (et les statistiques effacées) après 10 minutes d'inactivité.
- **Access Rules (Règles d'accès)** (activé par défaut) : active les statistiques pour les règles d'accès.
- **Port** : active les statistiques pour les ports TCP et UDP.
- **Protocol** : active les statistiques pour les protocoles IP non TCP/UDP.
- **TCP-Intercept** : active les statistiques pour les attaques interceptées par TCP Intercept (pour activer l'interception TCP, consultez Protéger les serveurs contre une attaque DoS par inondation SYN (interception de TCP)).

Étape 4 Pour les statistiques d'hôte, de port et de protocole, vous pouvez modifier le nombre d'intervalles de débit collectées. Dans la zone Intervalles de débit, choisissez **1 heure**, **1 et 8 heures**, ou **1, 8 et 24 heures** pour chaque type de statistique. L'intervalle par défaut est **1 heure**, ce qui réduit l'utilisation de la mémoire.

Étape 5 Pour les statistiques d'interception TCP, vous pouvez définir les options suivantes dans la zone de détection des menaces d'interception TCP :

- **Monitoring Window Size** : définit la taille de la fenêtre de surveillance de l'historique, entre 1 et 1 440 minutes. La valeur par défaut est de 30 minutes. L'ASA échantillonne le nombre d'attaques 30 fois au cours de l'intervalle de débit ; ainsi, pour la période par défaut de 30 minutes, des statistiques sont collectées toutes les 60 secondes.
- **Burst Threshold Rate** : définit le seuil de génération de messages syslog, entre 25 et 2 147 483 647. La valeur par défaut est de 400 par seconde. Lorsque le débit en rafale est dépassé, le message syslog 733104 est généré.
- **Average Threshold Rate** : définit le seuil de débit moyen pour la génération de messages syslog, entre 25 et 2 147 483 647. La valeur par défaut est de 200 par seconde. Lorsque le débit moyen est dépassé, le message syslog 733105 est généré.

Cliquez sur **Set Default** (Rétablir les valeurs par défaut) pour rétablir les valeurs par défaut.

Étape 6 Cliquez sur **Apply** (Appliquer).

Configurer l'analyse de détection des menaces

Vous pouvez configurer la détection des menaces par analyse pour identifier les agresseurs et, éventuellement, les contourner.

Vous pouvez configurer l'ASA pour envoyer des messages de journal système sur un agresseur ou vous pouvez banir automatiquement l'hôte. Par défaut, le message de journal système 730101 est généré lorsqu'un hôte est identifié comme agresseur. Assurez-vous d'exclure les adresses du bannissement lorsque vous attendez beaucoup de messages de la part de l'hôte. Par exemple, si vous avez activé la multidiffusion PIM, exemptez les routeurs PIM ou les messages PIM seront abandonnés.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Threat Detection (Détection des menaces)**

Étape 2 Sélectionnez **Enable Scanning Threat Detection** (Activer la détection des menaces par analyse).

Étape 3 (Facultatif) Pour mettre fin automatiquement à une connexion d'hôte lorsque l'ASA identifie l'hôte comme un agresseur, sélectionnez **Shun Hosts detected by scanning threat** (Bloquer les hôtes détectés par la détection des menaces par analyse) et complétez ces options si vous le souhaitez :

- Pour exempter les adresses IP d'hôte d'être contournées, saisissez une adresse ou le nom d'un objet réseau dans le champ **Réseaux exclus du contournement**. Il est possible d'entrer des adresses multiples, séparées par des virgules. Pour choisir un réseau dans la liste des objets d'adresse IP, cliquez sur le bouton **...** .
- Pour définir la durée d'un bannissement pour un hôte attaquant, sélectionnez **Définir la durée du bannissement** et saisissez une valeur comprise entre 10 et 2 592 000. La durée par défaut est de 3 600 secondes (1 heure). Pour rétablir la valeur par défaut, cliquez sur **Set Default** (Rétablir les valeurs par défaut).

Étape 4 Cliquez sur **Apply** (Appliquer).

Surveillance de la détection des menaces

Les rubriques suivantes expliquent comment surveiller la détection des menaces et afficher les statistiques de trafic.

Surveillance des statistiques de détection de base des menaces

Choisissez **Home (Accueil) > Firewall Dashboard (Tableau de bord du pare-feu) > Traffic Overview (Aperçu du trafic)** pour afficher les statistiques de détection des menaces de base.

Surveillance des statistiques de détection avancée des menaces

Vous pouvez surveiller les statistiques avancées sur les menaces à l'aide des tableaux de bord suivants :

- **Accueil > Tableau de bord du pare-feu > 10 principaux critères d'accès** : affiche les critères d'accès les plus sollicités. Les autorisations et les refus ne sont pas distingués dans ce graphique. Vous pouvez suivre le trafic refusé dans le graphique **Aperçu du trafic > Taux de paquets abandonnés**.
- **Accueil > Tableau de bord du pare-feu > Statistiques d'utilisation** : les onglets **10 principales sources** et **10 principales destinations** affichent les statistiques sur les hôtes. En raison de l'algorithme de détection des menaces, une interface utilisée comme combinaison de basculement et de lien d'état peut apparaître dans les 10 principaux hôtes; il s'agit du comportement attendu, et vous pouvez ignorer cette adresse IP dans l'affichage.

  L'onglet **Top 10 Services** (10 principaux services) affiche les statistiques pour les ports et les protocoles (les deux doivent être activés pour l'affichage) et affiche les statistiques combinées des types de ports TCP/UDP et de protocoles IP. TCP (protocole 6) et UDP (protocole 17) ne sont pas inclus dans l'affichage pour les protocoles IP; cependant, les ports TCP et UDP sont inclus dans l'affichage pour les ports. Si vous n'activez les statistiques que pour l'un de ces types, port ou protocole, vous ne pourrez afficher que les statistiques activées.
- **Accueil > Tableau de bord du pare-feu > Les dix principaux serveurs protégés sous l'attaque SYN** : affiche les statistiques d'interception TCP. Cliquez sur le bouton **Detail** (Détails) pour afficher les données d'échantillonnage de l'historique. L'ASA échantillonne le nombre d'attaques 30 fois au cours de l'intervalle de débit ; ainsi, pour la période par défaut de 30 minutes, des statistiques sont collectées toutes les 60 secondes.

Historique de la détection des menaces

Nom de la caractéristique	Versions de plateforme	Description
Statistiques de détection de base et avancée des menaces, détection des menaces par analyse	8.0(2)	Statistiques de détection de base et avancée des menaces, la détection des menaces d'analyse a été introduite. Les écrans suivants ont été introduits : **Configuration > Firewall (Pare-feu) > Threat Detection (Détection des menaces)**, **Home (Accueil) > Firewall Dashboard (Tableau de bord du pare-feu) > Traffic Overview (Aperçu du trafic)**, **Home (Accueil) > Firewall Dashboard (Tableau de bord du pare-feu) > Top 10 Access Rules (10 principales règles d'accès)**, **Home (Accueil) > Firewall Dashboard (Tableau de bord du pare-feu) > Top Usage Status (État de l'utilisation la plus élevée)**, **Home (Accueil) > Firewall Dashboard (Tableau de bord du pare-feu) > Top 10 Protected Servers Under SYN Attack (10 principaux serveurs protégés sous attaque SYN)**.
Durée du bannissement	8.0(4)/8.1(2)	Vous pouvez maintenant définir la durée du blocage, L'écran suivant a été modifié : **Configuration > Firewall (Pare-feu) > Threat Detection (Détection des menaces)**.
Statistiques TCP Intercept	8.0(4)/8.1(2)	Les statistiques TCP Intercept ont été introduites. Les écrans suivants ont été introduits ou modifiés : **Configuration > Firewall (Pare-feu) > Threat Detection (Détection des menaces)**, **Home (Accueil) > Firewall Dashboard (Tableau de bord du pare-feu) > Top 10 Protected Servers Under SYN Attack (10 principaux serveurs protégés sous attaque SYN)**.
Personnaliser les intervalles de débit des statistiques d'hôte	8.1(2)	Vous pouvez maintenant personnaliser le nombre d'intervalles de débit pour lesquels les statistiques sont recueillies. Le nombre de débits par défaut a été modifié de 3 à 1. L'écran suivant a été modifié : **Configuration > Firewall (Pare-feu) > Threat Detection (Détection des menaces)**.
L'intervalle de débit de rafale a été modifié à 1/30 du débit moyen.	8.2(1)	Dans les versions précédentes, l'intervalle de débit en rafale était de 1/60 du débit moyen. Pour maximiser l'utilisation de la mémoire, l'intervalle d'échantillonnage a été réduit à 30 pendant le débit moyen.
Personnaliser les intervalles de débit des statistiques de port et de protocole	8.3(1)	Vous pouvez maintenant personnaliser le nombre d'intervalles de débit pour lesquels les statistiques sont recueillies. Le nombre de débits par défaut a été modifié de 3 à 1. L'écran suivant a été modifié : **Configuration > Firewall (Pare-feu) > Threat Detection (Détection des menaces)**.

Nom de la caractéristique	Versions de plateforme	Description
Amélioration de l'utilisation de la mémoire	8.3(1)	L'utilisation de la mémoire pour la détection des menaces a été améliorée.

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.