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 de détection avancée des menaces : effectue le suivi de 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. Elle 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 des applications
- 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 attaque de 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**.

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 de la dernière période de 20 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 8.

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 Activez les statistiques de détection des menaces de base (si vous les avez désactivées précédemment).

threat-detection basic-threat

Exemple :

```
hostname(config)# threat-detection basic-threat
```

La détection des menaces de base est activée par défaut. Utilisez **no threat-detection basic-threat** pour la désactiver.

Étape 2 (Facultatif) Modifiez les paramètres par défaut pour un ou plusieurs types d'événement.

threat-detection rate {**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**} **rate-interval** *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

Pour obtenir une description de chaque type d'événement, consultez Statistiques de base sur la détection des menaces, page 8-1.

Lorsque vous utilisez cette commande avec le mot-clé **scanning-threat**, elle est également utilisée dans la détection des menaces d'analyse. Si vous ne configurez pas la détection des menaces de base, vous pouvez toujours utiliser cette commande avec le mot-clé **scanning-threat** pour configurer les limites de débit pour la détection des menaces d'analyse.

Vous pouvez configurer jusqu'à trois intervalles de débit différents pour chaque type d'événement.

Exemple :

```
hostname(config)# threat-detection rate dos-drop rate-interval 600 average-rate 60 burst-rate
 100
```

Configurer les statistiques de détection avancée des menaces

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

Procédure

Étape 1 (Facultatif) Activez *toutes* les statistiques.

statistiques de détection des menaces

Pour activer uniquement certaines statistiques, saisissez cette commande pour chaque type de statistique (montré plus loin dans cette procédure), et ne saisissez pas également la commande sans option. Vous pouvez saisir **statistiques de détection des menaces** (sans option), puis personnaliser certaines statistiques en entrant

la commande avec des options spécifiques aux statistiques (par exemple, **statistiques de détection des menaces host number-of-rate 2**). Si vous saisissez **statistiques de détection des menaces** (sans aucune option), puis saisissez une commande pour des statistiques spécifiques, mais sans option spécifique à la statistique, cette commande n'a aucun effet, car elle est déjà activée.

Si vous saisissez la forme **no** de cette commande, elle supprime toutes les commandes **statistiques de détection des menaces**, y compris la commande **statistiques de détection des menaces access-list**, qui est activée par défaut.

Exemple :

```
hostname(config)# threat-detection statistics
```

Étape 2 (Facultatif) Activez les statistiques pour les ACL (si elles ont été désactivées précédemment).

statistiques de détection des menaces access-list

Les statistiques pour les listes de contrôle d'accès sont activées par défaut. Les statistiques d'ACL ne sont affichées qu'à l'aide de la commande **show threat-detection top access-list**.

Exemple :

```
hostname(config)# threat-detection statistics access-list
```

Étape 3 (Facultatif) Configurez les statistiques pour les hôtes (mot clé **host**), les ports TCP et UDP (mot clé **port**) ou les protocoles IP non TCP/UDP (mot clé **protocol**).

statistiques de détection des menaces {**host** | **port** | **protocol**} [**number-of-rate** {**1** | **2** | **3**}]

Le mot-clé **number-of-rate** définit le nombre d'intervalles de débit gérés pour les statistiques. Le nombre d'intervalles de débit par défaut est **1**, ce qui réduit l'utilisation de la mémoire. Pour afficher davantage d'intervalles de débit, définissez la valeur à **2** ou **3**. Par exemple, si vous définissez la valeur à **3**, vous affichez les données des dernières 1 heure, 8 heures et 24 heures. Si vous définissez ce mot-clé à **1** (par défaut), seules les statistiques d'intervalle de débit les plus courts sont conservées. Si vous définissez la valeur à **2**, les deux intervalles les plus courts sont conservés.

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.

Exemple :

```
hostname(config)# threat-detection statistics host number-of-rate 2

hostname(config)# threat-detection statistics port number-of-rate 2

hostname(config)# threat-detection statistics protocol number-of-rate 3
```

Étape 4 (Facultatif) Configurez les statistiques pour les attaques interceptées par TCP Intercept.

statistiques de détection des menaces tcp-intercept [**rate-interval** *minutes*] [**burst-rate** *attacks_per_sec*] [**average-rate** *attacks_per_sec*]

Lieu :

- **rate-interval** 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. Pendant cet intervalle, le système échantillonne le nombre d'attaques 30 fois.

- **burst-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-rate** : définit le seuil de débit moyen pour la génération des 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.

Pour activer l'interception TCP, consultez Protéger les serveurs contre une attaque DoS par inondation SYN (interception de TCP).

Remarque
Cette commande est disponible en mode de contexte multiple, contrairement aux autres commandes de détection des menaces.

Exemple :

```
hostname(config)# threat-detection statistics tcp-intercept rate-interval 60
burst-rate 800 average-rate 600
```

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 Activer la détection des menaces par analyse.

threat-detection scanning-threat [**shun** [**except** {**ip-address** *ip_address mask* | **object-group** *network_object_group_id*}]]

Par défaut, le message de journal système 733101 est généré lorsqu'un hôte est identifié comme agresseur. Entrez cette commande plusieurs fois pour identifier plusieurs adresses IP ou groupes d'objets réseau à exempter du bannissement.

Exemple :

```
hostname(config)# threat-detection scanning-threat shun except
ip-address 10.1.1.0 255.255.255.0
```

Étape 2 (Facultatif) Définissez la durée du contournement pour les hôtes attaquants.

threat-detection scanning-threat shun duration *seconds*

Exemple :

```
hostname(config)# threat-detection scanning-threat shun duration 2000
```

Étape 3 (Facultatif) Modifiez la limite d'événements par défaut lorsque l'ASA identifie un hôte comme agresseur ou comme cible.

threat-detection rate scanning-threat rate-interval *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

Si vous avez déjà configuré cette commande dans le cadre de la configuration de base de détection des menaces, ces paramètres sont partagés avec la fonctionnalité de détection des menaces par analyse; vous ne pouvez pas configurer des débits distincts pour la détection des menaces de base et la détection des menaces par analyse. Si vous ne définissez pas les débits à l'aide de cette commande, les valeurs par défaut sont utilisées pour la fonctionnalité de détection des menaces par analyse et la fonctionnalité de détection des menaces de base. Vous pouvez configurer jusqu'à trois intervalles de débit différents en entrant des commandes distinctes.

Exemple :

```
hostname(config)# threat-detection rate scanning-threat rate-interval 1200
average-rate 10 burst-rate 20

hostname(config)# threat-detection rate scanning-threat rate-interval 2400
average-rate 10 burst-rate 20
```

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 base de la détection des menaces

Pour afficher les statistiques de base sur la détection des menaces, utilisez la commande suivante :

show threat-detection rate [**min-display-rate** *min_display_rate*] [**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**]

L'argument **min-display-rate** *min_display_rate* limite l'affichage aux statistiques qui dépassent le taux d'affichage minimal en événements par seconde. Vous pouvez définir le *min_display_rate* entre 0 et 2147483647.

Les autres arguments vous permettent de limiter l'affichage à des catégories spécifiques. Pour une description de chaque type d'événement, consultez Statistiques de détection des menaces de base, à la page 2.

Le résultat affiche le débit moyen en événements/s sur deux périodes fixes : les 10 dernières minutes et la dernière heure. Il affiche également : le débit de rafale actuel en événements/s sur le dernier intervalle de rafale terminé, qui est 1/30 de l'intervalle de débit moyen ou 10 secondes, selon le plus élevé des deux; le nombre de fois que les débits ont été dépassés (déclenchés); et le nombre total d'événements au fil des périodes.

L'ASA stocke le nombre à la fin de chaque période de rafale, pour un total de 30 intervalles de rafale terminés. L'intervalle de rafale inachevée qui se produit actuellement n'est pas inclus dans le débit moyen. Par exemple, si l'intervalle de débit moyen est de 20 minutes, l'intervalle de rafale est de 20 secondes. Si le dernier intervalle

de rafale a été compris entre 3:00:00 et 3:00:20 et que vous utilisez la commande **afficher** à 3:00:25, les 5 dernières secondes ne sont pas incluses dans la sortie.

La seule exception à cette règle est si le nombre d'événements dans l'intervalle de rafale inachevé dépasse déjà le nombre d'événements dans l'intervalle de rafale le plus ancien (n° 1 sur 30) lors du calcul du nombre total d'événements. Dans ce cas, l'ASA calcule le nombre total d'événements comme les 29 derniers intervalles complets, plus les événements jusqu'à présent dans l'intervalle de rafale inachevé. Cette exception vous permet de surveiller une augmentation importante des événements en temps réel.

Vous pouvez effacer les statistiques à l'aide de la commande **clear threat-detection rate**.

Voici un exemple de sortie de la commande **show threat-detection rate** :

```
hostname# show threat-detection rate

                        Average(eps)    Current(eps) Trigger         Total events
  10-min ACL  drop:                0               0       0                   16
  1-hour ACL  drop:                0               0       0                  112
  1-hour SYN attck:                5               0       2                21438
  10-min  Scanning:                0               0      29                  193
  1-hour  Scanning:              106               0      10               384776
  1-hour Bad  pkts:               76               0       2               274690
  10-min  Firewall:                0               0       3                   22
  1-hour  Firewall:               76               0       2               274844
  10-min DoS attck:                0               0       0                    6
  1-hour DoS attck:                0               0       0                   42
  10-min Interface:                0               0       0                  204
  1-hour Interface:               88               0       0               318225
```

Surveillance des statistiques de détection avancée des menaces

Pour surveiller les statistiques de détection avancée des menaces, utilisez les commandes affichées dans le tableau suivant. La sortie d'affichage affiche les éléments suivants :

- Le débit moyen en événements/s sur des périodes fixes.
- Le débit de rafale actuel en événements/s sur le dernier intervalle de rafale terminé, qui est de 1/30 de l'intervalle de débit moyen ou de 10 secondes, selon le plus élevé des deux.
- Le nombre de fois que les débits ont été dépassés (pour les statistiques de trafic abandonnées uniquement).
- Le nombre total d'événements sur les périodes de temps fixes.

L'ASA stocke le nombre à la fin de chaque période de rafale, pour un total de 30 intervalles de rafale terminés. L'intervalle de rafale inachevée qui se produit actuellement n'est pas inclus dans le débit moyen. Par exemple, si l'intervalle de débit moyen est de 20 minutes, l'intervalle de rafale est de 20 secondes. Si le dernier intervalle de rafale a été compris entre 3:00:00 et 3:00:20 et que vous utilisez la commande **afficher** à 3:00:25, les 5 dernières secondes ne sont pas incluses dans la sortie.

La seule exception à cette règle est si le nombre d'événements dans l'intervalle de rafale inachevé dépasse déjà le nombre d'événements dans l'intervalle de rafale le plus ancien (n° 1 sur 30) lors du calcul du nombre total d'événements. Dans ce cas, l'ASA calcule le nombre total d'événements comme les 29 derniers intervalles complets, plus les événements jusqu'à présent dans l'intervalle de rafale inachevé. Cette exception vous permet de surveiller une augmentation importante des événements en temps réel.

Commande	Objectif
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top** [[**access-list** | **host** | **port-protocol**] [**rate-1** | **rate-2** | **rate-3**] | **tcp-intercept** [**all**] **detail**]]	Affiche les 10 principales statistiques. Si vous ne saisissez aucune option, les 10 principales statistiques sont affichées pour toutes les catégories. L'argument **min-display-rate** *min_display_rate* limite l'affichage aux statistiques qui dépassent le taux d'affichage minimal en événements par seconde. Vous pouvez définir le *min_display_rate* entre 0 et 2147483647. Les lignes suivantes expliquent les mots-clés facultatifs.
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top access-list** [**rate-1** | **rate-2** | **rate-3**]	Pour afficher les 10 principaux ACE correspondant aux paquets, y compris les ACE d'autorisation et de refus, utilisez le mot-clé **access-list**. Le trafic autorisé et refusé ne sont pas distincts dans cet affichage. Si vous activez la détection des menaces de base à l'aide de la commande **threat-detection basic-threat**, vous pouvez suivre les refus d'ACL à l'aide de la commande **show threat-detection rate acl-drop**. Le mot-clé **rate-1** affiche les statistiques pour les plus petits intervalles de débit fixe disponibles dans l'affichage ; **rate-2** affiche l'intervalle de débit suivant le plus important ; et **rate-3**, si vous avez défini trois intervalles, affiche le plus grand intervalle de débit. Par exemple, l'affichage présente les statistiques de la dernière heure, des 8 dernières heures et des 24 dernières heures. Si vous définissez le mot-clé **rate-1**, l'ASA affiche uniquement l'intervalle de temps d'1 heure.
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top host** [**rate-1** | **rate-2** | **rate-3**]	Pour afficher uniquement les statistiques d'hôte, utilisez le mot-clé **host**. **Remarque** : 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.
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top port-protocol** [**rate-1** | **rate-2** | **rate-3**]	Pour afficher les statistiques sur les ports et les protocoles, utilisez le mot-clé **port-protocol**. Le mot-clé **port-protocol** 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.
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top tcp-intercept** [**all**] **detail**]]	Pour afficher les statistiques d'interception TCP, utilisez le mot-clé **tcp-intercept**. L'affichage inclut les 10 principaux serveurs protégés sous attaque. Le mot-clé **all** affiche les données historiques de tous les serveurs suivis. Le mot-clé **detail** affiche 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.
show threat-detection statistics [**min-display-rate** *min_display_rate*] **host** [*ip_address* [*mask*]]	Affiche les statistiques pour tous les hôtes ou pour un hôte ou un sous-réseau spécifique.
show threat-detection statistics [**min-display-rate** *min_display_rate*] **port** [*start_port*[-*end_port*]]	Affiche les statistiques pour tous les ports ou pour un port ou une plage de ports spécifique.

Commande	Objectif
show threat-detection statistics [**min-display-rate** *min_display_rate*] **protocol** [*protocol_number* | *protocol*]	Affiche les statistiques pour tous les protocoles IP ou pour un protocole spécifique. L'argument *protocol_number* est un entier compris entre 0 et 255. L'argument du *protocole* peut être l'un des suivants : **ah**, **eigrp**, **esp**, **gre**, **icmp**, **icmp6**, **igmp**, **igrp**, **ip**, **ipinip**, **ipsec**, **nos**, **ospf**, **pcp**, **pim**, **pptp**, **snp**, **tcp**, **udp**.

Évaluation des statistiques de détection des menaces de l'hôte

Voici un exemple de résultat de la commande **show threat-detection statistics host** :

```
hostname# show threat-detection statistics host

                        Average(eps)    Current(eps) Trigger         Total events
Host:10.0.0.1: tot-ses:289235 act-ses:22571 fw-drop:0 insp-drop:0 null-ses:21438 bad-acc:0
  1-hour Sent byte:               2938               0       0             10580308
  8-hour Sent byte:                367               0       0             10580308
 24-hour Sent byte:                122               0       0             10580308
  1-hour Sent pkts:                 28               0       0               104043
  8-hour Sent pkts:                  3               0       0               104043
 24-hour Sent pkts:                  1               0       0               104043
  20-min Sent drop:                  9               0       1                10851
  1-hour Sent drop:                  3               0       1                10851
  1-hour Recv byte:               2697               0       0              9712670
  8-hour Recv byte:                337               0       0              9712670
 24-hour Recv byte:                112               0       0              9712670
  1-hour Recv pkts:                 29               0       0               104846
  8-hour Recv pkts:                  3               0       0               104846
 24-hour Recv pkts:                  1               0       0               104846
  20-min Recv drop:                 42               0       3                50567
  1-hour Recv drop:                 14               0       1                50567
Host:10.0.0.0: tot-ses:1 act-ses:0 fw-drop:0 insp-drop:0 null-ses:0 bad-acc:0
  1-hour Sent byte:                  0               0       0                  614
  8-hour Sent byte:                  0               0       0                  614
 24-hour Sent byte:                  0               0       0                  614
  1-hour Sent pkts:                  0               0       0                    6
  8-hour Sent pkts:                  0               0       0                    6
 24-hour Sent pkts:                  0               0       0                    6
  20-min Sent drop:                  0               0       0                    4
  1-hour Sent drop:                  0               0       0                    4
  1-hour Recv byte:                  0               0       0                  706
  8-hour Recv byte:                  0               0       0                  706
 24-hour Recv byte:                  0               0       0                  706
  1-hour Recv pkts:                  0               0       0                    7
```

Le tableau suivant explique la sortie.

Tableau 3 : show threat-detection statistics host

Champ	Description
Hébergement	Adresse IP de l'hôte
tot-ses	Le nombre total de sessions pour cet hôte depuis son ajout à la base de données.

Champ	Description
act-ses	Le nombre total de sessions actives dans lesquelles l'hôte est actuellement impliqué.
fw-drop	Le nombre d'abandons de pare-feu. Les abandons de pare-feu sont un taux combiné qui inclut tous les abandons de paquets liés au pare-feu suivis dans la détection des menaces de base, y compris les refus d'ACL, les paquets incorrects, les limites de connexion dépassées, les paquets d'attaques DoS, les paquets ICMP suspects, les paquets d'attaques TCP SYN et les paquets d'attaques par session UDP sans données de retour. 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.
insp-drop	Le nombre de paquets abandonnés en raison d'un échec de l'inspection de l'application.
null-ses	Le nombre de sessions nulles, qui sont des sessions TCP SYN qui ne se sont pas terminées dans le délai d'expiration de 3 secondes, et les sessions UDP qui n'ont fait l'objet d'aucune donnée envoyée par son serveur 3 secondes après le début de la session.
bad-acc	Le nombre de tentatives d'accès incorrectes aux ports d'hôte fermés. Lorsqu'il est déterminé qu'un port se trouve dans une session nulle (voir la description du champ null-ses), l'état du port de l'hôte est défini à HOST_PORT_CLOSE. Tout client qui accède au port de l'hôte est immédiatement classé comme un mauvais accès sans qu'il soit nécessaire d'attenter un délai d'expiration.
Moyenne (eps)	Le débit moyen en événements/s sur chaque période. L'ASA stocke le nombre à la fin de chaque période de rafale, pour un total de 30 intervalles de rafale terminés. L'intervalle de rafale inachevée qui se produit actuellement n'est pas inclus dans le débit moyen. Par exemple, si l'intervalle de débit moyen est de 20 minutes, l'intervalle de rafale est de 20 secondes. Si le dernier intervalle de rafale a été compris entre 3:00:00 et 3:00:20 et que vous utilisez la commande **afficher** à 3:00:25, les 5 dernières secondes ne sont pas incluses dans la sortie. La seule exception à cette règle est si le nombre d'événements dans l'intervalle de rafale inachevé dépasse déjà le nombre d'événements dans l'intervalle de rafale le plus ancien (n° 1 sur 30) lors du calcul du nombre total d'événements. Dans ce cas, l'ASA calcule le nombre total d'événements comme les 29 derniers intervalles complets, plus les événements jusqu'à présent dans l'intervalle de rafale inachevé. Cette exception vous permet de surveiller une augmentation importante des événements en temps réel.
Actuel (eps)	Le débit de rafale actuel en événements/s sur le dernier intervalle de rafale terminé, qui est de 1/30 de l'intervalle de débit moyen ou de 10 secondes, selon le plus élevé des deux. Pour l'exemple spécifié dans la description de la moyenne (eps), le taux actuel est le taux de 3:19:30 à 3:20:00
initiales	Le nombre de fois que les limites de débit de paquets abandonnés ont été dépassées. Pour le trafic valide identifié dans les lignes des octets et des paquets envoyés et reçus, cette valeur est toujours 0, car il n'y a aucune limite de débit à déclencher pour le trafic valide.

Champ	Description
Nombre total d'événements	Le nombre total d'événements sur chaque intervalle de débit. L'intervalle de rafale inachevée qui se produit actuellement n'est pas inclus dans le nombre total d'événements. La seule exception à cette règle est si le nombre d'événements dans l'intervalle de rafale inachevé dépasse déjà le nombre d'événements dans l'intervalle de rafale le plus ancien (n° 1 sur 30) lors du calcul du nombre total d'événements. Dans ce cas, l'ASA calcule le nombre total d'événements comme les 29 derniers intervalles complets, plus les événements jusqu'à présent dans l'intervalle de rafale inachevé. Cette exception vous permet de surveiller une augmentation importante des événements en temps réel.
20 min, 1 heure, 8 heures et 24 heures	Statistiques pour ces intervalles de débit fixe. Pour chaque intervalle : • Octets envoyés : le nombre d'octets envoyés par l'hôte. • Paquets envoyés : le nombre de paquets envoyés par l'hôte. • Envoyés abandonnés : le nombre de paquets envoyés par l'hôte qui ont été abandonnés en raison d'une attaque par analyse. • Octets reçus : le nombre d'octets reçus par l'hôte. • Paquets reçus : le nombre de paquets reçus par l'hôte. • Réception de l'abandon : le nombre de paquets reçus par l'hôte qui ont été abandonnés en raison d'une attaque par analyse.

Surveillance de la détection des menaces, des hôtes contournés, des agresseurs et des cibles

Pour surveiller et gérer les hôtes et les attaquants bloqués, ainsi que les cibles pour la détection des menaces d'analyse, utilisez les commandes suivantes. Ces commandes sont destinées uniquement à la détection des menaces d'analyse et ne s'appliquent pas à d'autres services.

- **show threat-detection shun**

  Affiche les hôtes actuellement bloqués. Par exemple :

```
hostname# show threat-detection shun

Shunned Host List:
(outside) src-ip=10.0.0.13 255.255.255.255
(inside) src-ip=10.0.0.13 255.255.255.255
```

- **clear threat-detection shun** [*ip_address* [*mask*]]

  Libère un hôte de la liste de blocage. Si vous ne spécifiez pas d'adresse IP, tous les hôtes sont effacés de la liste de blocage.

  Par exemple, pour libérer l'hôte à l'adresse 10.1.1.6, entrez la commande suivante :

```
hostname# clear threat-detection shun 10.1.1.6
```

- **show threat-detection scanning-threat** [**attacker** | **target**]

  Affiche les hôtes que l'ASA considère comme des attaquants (y compris les hôtes dans la liste de blocage) et affiche les hôtes qui sont la cible d'une attaque. Si vous ne saisissez pas d'option, les attaquants et les hôtes cibles sont affichés. Par exemple :

```
hostname# show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0 (l2l)
    192.168.1.249 (l2l)
Latest Attacker Host & Subnet List:
    192.168.10.234 (outside)
    192.168.10.0 (outside)
    192.168.10.2 (outside)
    192.168.10.3 (outside)
    192.168.10.4 (outside)
    192.168.10.5 (outside)
    192.168.10.6 (outside)
    192.168.10.7 (outside)
    192.168.10.8 (outside)
    192.168.10.9 (outside)
```

Exemples pour la détection des menaces

L'exemple suivant configure les statistiques de détection des menaces de base et modifie les paramètres de taux d'attaque DoS. Toutes les statistiques de détection avancée des menaces sont activées, avec le nombre d'intervalles de taux des statistiques d'hôte réduit à 2. L'intervalle de débit d'interception TCP est également personnalisé. La détection des menaces d'analyse est activée avec le blocage automatique pour toutes les adresses, à l'exception de 10.1.1.0/24. Les intervalles de taux de menace d'analyse sont personnalisés.

```
threat-detection basic-threat
threat-detection rate dos-drop rate-interval 600 average-rate 60 burst-rate 100
threat-detection statistics
threat-detection statistics host number-of-rate 2
threat-detection statistics tcp-intercept rate-interval 60 burst-rate 800 average-rate 600
threat-detection scanning-threat shun except ip-address 10.1.1.0 255.255.255.0
threat-detection rate scanning-threat rate-interval 1200 average-rate 10 burst-rate 20
threat-detection rate scanning-threat rate-interval 2400 average-rate 10 burst-rate 20
```

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 commandes suivantes ont été introduites : **threat-detection basic-threat**, **threat-detection rate**, **show threat-detection rate**, **clear threat-detection rate, threat-detection statistics**, **show threat-detection statistics**, **threat-detection scanning-threat**, **threat-detection rate scanning-threat**, **show threat-detection scanning-threat**, **show threat-detection shun**, **clear threat-detection shun**.
Durée du bannissement	8.0(4)/8.1(2)	Vous pouvez maintenant définir la durée du blocage, La commande suivante a été introduite : **threat-detection scanning-threat shun duration**.
Statistiques TCP Intercept	8.0(4)/8.1(2)	Les statistiques TCP Intercept ont été introduites. Les commandes suivantes ont été modifiées ou introduites : **threat-detection statistics tcp-intercept**, **show threat-detection statistics top tcp-intercept**, **clear threat-detection statistics**.
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. La commande suivante a été modifiée : **threat-detection statistics host number-of-rates**.
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. Les commandes suivantes ont été modifiées : **threat-detection statistics port number-of-rates**, **threat-detection statistics protocol number-of-rates**.
Amélioration de l'utilisation de la mémoire	8.3(1)	L'utilisation de la mémoire pour la détection des menaces a été améliorée. La commande suivante a été introduite : **show threat-detection memory**.

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.

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.

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.

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.

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.