ASA/PIX 7.x et versions ultérieures : Atténuation des attaques réseau

Contenu

Introduction

Ce document décrit comment atténuer les diverses attaques réseau, telles que les dénis de service (DoS), en utilisant le dispositif de sécurité Cisco (ASA/PIX).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur l'appliance de sécurité adaptable de gamme Cisco 5500 (ASA) cette version de logiciel 7.0 de passages et plus tard.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-

vous que vous comprenez l'effet potentiel de toute commande.

Produits connexes

Ce document peut également être utilisé avec la gamme Cisco 500 PIX qui exécute la version de logiciel 7.0 et plus tard.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Protection contre des attaques de synchronisation

Comment atténuez-vous le Protocole TCP (Transmission Control Protocol) synchronisez-vous/attaques de début (synchronisation) sur l'ASA/PIX ?

Attaque de synchronisation de TCP

L'attaque de synchronisation de TCP est un type d'attaque DoS dans lequel un expéditeur transmet un volume de connexions qui ne peuvent pas être terminées. Ceci fait remplir les files d'attente de connexion, refusant de ce fait le service pour légitimer des utilisateurs de TCP.

Quand les débuts normaux d'une connexion TCP, une destination host reçoit un paquet de synchronisation d'un hôte de source et renvoie un synchroniser reconnaissez (synchronisation ACK). La destination host doit alors entendre un ACK de la synchronisation ACK avant que la connexion soit établie. Ceci désigné sous le nom du connexion TCP à trois.

Tout en attendant l'ACK à la synchronisation ACK, une file d'attente de connexion de taille finie sur la destination host maintient des connexions attendant d'être terminé. Cette file d'attente vide typiquement rapidement parce qu'on s'attend à ce que l'ACK arrive quelques millisecondes après la synchronisation ACK.

L'attaque de synchronisation de TCP exploite cette conception en ayant un hôte de attaque de source génèrent des paquets de synchronisation de TCP avec des adresses sources aléatoires vers un hôte victime. Le hôte de destination victime envoie une synchronisation ACK de nouveau à l'adresse source aléatoire et ajoute une entrée à la file d'attente de connexion. Puisque la synchronisation ACK est destinée à un hôte incorrect ou inexistant, la dernière partie de la « connexion en trois étapes » n'est jamais terminée et l'entrée demeure dans la file d'attente de connexion jusqu'à ce qu'un temporisateur expire, typiquement pour environ une minute. En générant de faux paquets de synchronisation de TCP des adresses IP aléatoires à une vitesse rapide, il est possible de remplir la file d'attente de connexion et de refuser des services de TCP (tels que le courrier électronique, le transfert de fichiers, ou le WWW) aux utilisateurs légitimes.

Il n'y a aucune méthode facile de tracer le créateur de l'attaque parce que l'adresse IP de la source est modifiée.

Les manifestations externes du problème incluent l'incapacité d'obtenir le courrier électronique, l'incapacité de recevoir des connexions aux services de WWW ou de FTP, ou un grand nombre de connexions TCP sur votre hôte dans l'état SYN_RCVD.

Référez-vous aux défenses contre des attaques par inondation SYN de TCP pour plus d'informations sur des attaques de synchronisation de TCP.

Réduction

Cette section décrit comment atténuer les attaques de synchronisation en plaçant le TCP et les connexions maximum de Protocole UDP (User Datagram Protocol), les connexions embryonnaires maximum, des délais d'attente de connexion, et comment désactiver la randomisation d'ordre de TCP.

Si la limite embryonnaire de connexion est atteinte, alors les dispositifs de sécurité répondent à chaque paquet de synchronisation envoyé au serveur avec un SYN+ACK, et ne passent pas le paquet de synchronisation au serveur interne. Si le périphérique externe répond avec un paquet ACK, alors les dispositifs de sécurité savent que c'est une demande valide (et pas une partie d'une attaque potentielle de synchronisation). Les dispositifs de sécurité alors établissent une connexion avec le serveur et joignent les connexions ensemble. Si les dispositifs de sécurité ne récupèrent pas un ACK du serveur, ils chronomètrent agressivement cette connexion embryonnaire.

Chaque connexion TCP a le nombre de deux séquences initiales (ISNs) : un généré par le client et un généré par le serveur. Les dispositifs de sécurité sélectionnent de façon aléatoire l'ISN de la synchronisation de TCP passant dans le d'arrivée et des directions sortantes.

Sélectionner de façon aléatoire l'ISN de l'hôte protégé empêche un attaquant de prévoir le prochain ISN pour une nouvelle connexion et de détourner potentiellement la nouvelle session.

La randomisation de nombre de séquence initiale de TCP peut être désactivée s'il y a lieu. Exemple :

- Si un autre Pare-feu intégré sélectionne de façon aléatoire également les nombres de séquence initiale, il n'y a aucun besoin des deux Pare-feu d'exécuter cette action, quoique cette action n'affecte pas le trafic.
- Si vous utilisez la connexion multiple entre deux noeuds de BGP externe (eBGP) par les dispositifs de sécurité, et les pairs d'eBGP utilisent le MD5, la randomisation casse la somme de contrôle de MD5.
- Vous utilisez un périphérique des Services d'applications de réseau étendu Cisco (WAAS) qui exige des dispositifs de sécurité de ne pas sélectionner de façon aléatoire les numéros de séquence de connexions.

Remarque: Vous pouvez également randomisation configurer des nombres maximaux de connexions, des connexions embryonnaires maximum, et de TCP ordre dans la configuration NAT. Si vous configurez ces configurations pour le même trafic suivre les deux méthodes, alors les dispositifs de sécurité utilisent la limite inférieure. Pour la randomisation d'ordre de TCP, s'ils sont désactivés suivre l'un ou l'autre de méthode, puis les dispositifs de sécurité désactivent la randomisation d'ordre de TCP.

Terminez-vous ces étapes afin de fixer des limites de connexion :

1. Afin d'identifier le trafic, ajoutez un class map utilisant la commande de **class-map** selon utiliser le cadre de stratégie modulaire.
2. Afin d'ajouter ou éditer une **stratégie tracez** qui place les actions de prendre avec le class map trafiquent, sélectionnent cette commande :`hostname(config)#`**`policy-map name`**

3. Afin d'identifier le class map (de l'étape 1) auquel vous voulez assigner une action, sélectionnent cette commande :`hostname(config-pmap)#`**`class class_map_name`**
4. Afin de placer les nombres maximaux de connexions (les deux TCP et UDP), les connexions embryonnaires, par-client-embryonnaire-maximum maximum, par-client-maximum ou si désactiver la randomisation d'ordre de TCP, sélectionnent cette commande :`hostname(config-pmap-c)#`**`set connection`** {[**`conn-max`** number] [**`embryonic-conn-max`** number] [**`per-client-embryonic-max`** number] [**`per-client-max`** number][**`random-sequence-number`** {**`enable`** | **`disable`**}} Là où le nombre est un entier entre 0 et 65535. Le par défaut est 0, qui ne signifie aucune limite sur des connexions.Vous pouvez sélectionner cette commande toute sur une ligne (dans toute commande), ou vous pouvez écrire chaque attribut pendant qu'une commande distincte. La commande est combinée sur une ligne en configuration en cours.
5. Afin de placer le délai d'attente pour des connexions, les connexions embryonnaires (entrouvertes) et les connexions à moitié fermées, sélectionnent cette commande :`hostname(config-pmap-c)#`**`set connection`** {[**`embryonic`** hh[:mm[:ss]]] [**`half-closed`** hh[:mm[:ss]]] [**`tcp`** hh[:mm[:ss]]]} Là où hh **embryonnaire** [: millimètre [: les solides solubles] est un moment entre 0:0:5 et 1192:59:59. Le par défaut est 0:0:30. Vous pouvez également placer cette valeur à 0, qui signifie que la connexion ne chronomètre jamais.Le hh **à moitié fermé** [: millimètre [: solides solubles] et hh de **TCP** [: millimètre [: les valeurs solides solubles] sont un moment entre 0:5:0 et 1192:59:59. Le par défaut pour **à moitié fermé** est 0:10:0 et le par défaut pour le **TCP** est 1:0:0. Vous pouvez également placer ces valeurs à 0, qui signifie que la connexion ne chronomètre jamais.Vous pouvez sélectionner cette commande toute sur une ligne (dans toute commande), ou vous pouvez écrire chaque attribut pendant qu'une commande distincte. La commande est combinée sur une ligne en configuration en cours.**Connexion (entrouverte) embryonnaire** — Une connexion embryonnaire est une demande de connexion TCP qui n'a pas terminé la prise de contact nécessaire entre la source et la destination.**Connexion à moitié fermée** — La connexion à moitié fermée est quand la connexion est seulement fermée dans une direction en envoyant la FIN. Cependant, la session TCP est encore mise à jour par le pair.**Par-client-embryonnaire-maximum** — Le nombre maximal de connexions embryonnaires simultanées a autorisé par client, entre 0 et 65535. Le par défaut est 0, qui permet les connexions illimitées.**Par-client-maximum** — Le nombre maximal de connexions simultanées a autorisé par client, entre 0 et 65535. Le par défaut est 0, qui permet les connexions illimitées.
6. Afin de lancer la carte de stratégie sur un ou plusieurs interfaces, sélectionnez cette commande :`hostname(config)#`**`service-policy policymap_name`** *`{global | interface interface_name}`* Là où **global** applique la carte de stratégie à toutes les interfaces, et l'**interface** s'applique la stratégie à une interface. On permet seulement une stratégie globale. Vous pouvez ignorer la stratégie globale sur une interface en s'appliquant une stratégie de service à cette interface. Vous pouvez seulement appliquer une carte de stratégie à chaque interface.

Exemple :

```
ciscoasa(config)#class-map tcp_syn ciscoasa(config-cmap)#match port tcp eq 80 ciscoasa(config-cmap)#exit ciscoasa(config)#policy-map tcpmap ciscoasa(config-pmap)#class tcp_syn ciscoasa(config-pmap-c)#set connection conn-max 100 ciscoasa(config-pmap-c)#set connection embryonic-conn-max 200 ciscoasa(config-pmap-c)#set connection per-client-embryonic-max 10 ciscoasa(config-pmap-c)#set connection per-client-max 5 ciscoasa(config-pmap-c)#set connection random-sequence-number enable ciscoasa(config-pmap-c)#set connection timeout embryonic 0:0:45 ciscoasa(config-pmap-c)#set connection timeout half-closed 0:25:0 ciscoasa(config-pmap-c)#set connection timeout tcp 2:0:0 ciscoasa(config-pmap-c)#exit ciscoasa(config-pmap)#exit ciscoasa(config)#service-policy tcpmap global
```

Remarque: Afin de vérifier le nombre total de sessions entrouvertes pour n'importe quel hôte spécifique, utilisez cette commande :

```
ASA-5510-8x# show local-host all Interface dmz: 0 active, 0 maximum active, 0 denied Interface
management: 0 active, 0 maximum active, 0 denied Interface xx: 0 active, 0 maximum active, 0
denied Interface inside: 7 active, 18 maximum active, 0 denied local host: <10.78.167.69>, TCP
flow count/limit = 2/unlimited TCP embryonic count to host = 0 TCP intercept watermark =
unlimited UDP flow count/limit = 0/unlimited
```

Remarque: La ligne, `compte embryonnaire de TCP à héberger`, affiche le nombre de sessions entrouvertes.

Protection contre des attaques d'usurpation d'adresse IP

Le PIX/ASA peut-il bloquer des attaques de détournement de trafic IP ?

Usurpation d'adresse IP

Afin d'accéder, les intrus créent des paquets avec les adresses IP charriées de source. Ceci exploite les applications qui utilisent l'authentification basée sur des adresses IP et mène à l'utilisateur non autorisé et enracine probablement l'accès sur le système visé. Les exemples sont le rsh et des services de rlogin.

Il est possible de conduire des paquets par des Pare-feu de routeur de filtrage s'ils ne sont pas configurés pour filtrer les paquets entrant dont l'adresse source est dans le domaine local. Il est important de noter que l'attaque décrite est possible même si aucun paquet de réponse ne peut atteindre l'attaquant.

Les exemples des configurations qui sont potentiellement vulnérables incluent :

- Pare-feu de proxy où les applications de proxy utilisent l'adresse IP source pour l'authentification
- Routeurs aux réseaux externes qui prennent en charge de plusieurs interfaces internes
- Routeurs avec deux interfaces qui prennent en charge le sous-réseautage sur le réseau interne

Réduction

Le Fonction Unicast Reverse Path Forwarding (uRPF) garde contre l'usurpation d'adresse IP (un paquet emploie une adresse IP source incorrecte pour obscurcir sa source vraie) en s'assurant que tous les paquets ont une adresse IP source qui apparie l'interface correcte de source selon la table de routage.

Normalement, les dispositifs de sécurité regardent seulement l'adresse de destination en déterminant où expédier le paquet. Unicast RPF demande aux dispositifs de sécurité de regarder également l'adresse source. C'est pourquoi ce s'appelle le **Reverse Path Forwarding**. Pour n'importe quel trafic que vous voulez permettre par les dispositifs de sécurité, la table de routage de dispositifs de sécurité doit inclure une route de retour vers l'adresse source. Voir le pour en savoir plus RFC 2267.

Remarque: `: - %PIX-1-106021 : Refusez le contrôle de chemin inverse de protocole du src_addr au dest_addr sur le` message de log d'`int_name d'interface` peut être vu quand le contrôle de chemin

inverse est activé. Désactivez le contrôle de chemin inverse avec l'**aucun IP vérifient la** commande d'**interface de chemin inverse (nom d'interface)** afin de résoudre ce problème :

`no ip verify reverse-path interface (interface name)`

Pour le trafic d'extérieur, par exemple, les dispositifs de sécurité peuvent employer le default route pour satisfaire la protection d'Unicast RPF. Si le trafic entre d'une interface extérieure, et l'adresse source n'est pas connue à la table de routage, les dispositifs de sécurité emploient le default route pour identifier correctement l'interface extérieure comme interface de source.

Si le trafic écrit l'interface extérieure d'une adresse qui est connue à la table de routage, mais est associé avec l'interface interne, alors les dispositifs de sécurité relâchent le paquet. De même, si le trafic écrit l'interface interne d'une adresse de provenance inconnue, les dispositifs de sécurité relâchent le paquet parce que l'artère assortie (le default route) indique l'interface extérieure.

Unicast RPF est mis en application comme affiché :

- Les paquets d'ICMP n'ont aucune session, ainsi chaque paquet est vérifié.
- L'UDP et le TCP ont des sessions, ainsi le paquet initial exige une recherche de route inverse. Des paquets suivants arrivant pendant la session sont vérifiés utilisant un état existant mis à jour en tant qu'élément de la session. des paquets de Non-initiale sont vérifiés pour s'assurer qu'ils sont arrivés sur la même interface utilisée par le paquet initial.

Afin d'activer Unicast RPF, sélectionnez cette commande :

`hostname(config)#`**`ip verify reverse-path interface`** *`interface_name`*

Exemple :

Comme affiché cette figure, le PC d'attaquant lance une demande au serveur d'applications 10.1.1.10 en envoyant un paquet avec une adresse IP source modifiée 10.1.1.5/24, et le serveur envoie un paquet à la vraie adresse IP 10.1.1.5/24 en réponse à la demande. Ce type de paquet illégal attaquera le serveur d'applications et l'utilisateur légitime dans le réseau intérieur.

Unicast RPF peut empêcher des attaques basées sur le détournement de l'adresse source. Vous devez configurer l'uRPF dans l'interface extérieure de l'ASA comme affiché ici :

`ciscoasa(config)#`**`ip verify reverse-path interface`** `outside`

Charrier l'identification utilisant des messages de Syslog

Les dispositifs de sécurité continuent à recevoir des messages d'erreur de Syslog comme affichés. Ceci indique que les attaques potentielles utilisant les paquets charriés ou celle pourraient déclencher en raison du routage asymétrique.

1. **`%PIX|ASA-2-106001: Inbound TCP connection denied from IP_address/port to IP_address/port flags tcp_flags on interface interface_name`** **Explication**C'est un message lié à la connexion. Ce message se produit quand une tentative de se connecter à une adresse intérieure est refusée par la stratégie de sécurité qui est définie pour le type du trafic indiqué. Les valeurs possibles de *tcp_flags* correspondent aux indicateurs dans l'en-tête de TCP qui étaient présent quand la connexion a été refusée. Par exemple, un paquet TCP est arrivé pour ce qu'aucun état de connexion n'existe dans les dispositifs de sécurité, et il a été abandonné. *Les tcp_flags* en ce paquet sont FIN et ACK.*Les tcp_flags* sont comme suit :ACK — Le

nombre d'accusé de réception a été reçu.FIN — Des données ont été envoyées.PSH — Le récepteur a passé des données à l'application.RST — La connexion a été remise à l'état initial.synchronisation — Des numéros de séquence ont été synchronisés pour commencer une connexion.URG — Le pointeur d'urgence était valide avoué.Il y a beaucoup de raisons pour que la traduction statique échoue sur le PIX/ASA. Mais, une raison commune est si l'interface de la zone démilitarisée (DMZ) est configurée avec le même niveau de Sécurité (0) que l'interface extérieure.Afin de résoudre ce problème, assignez un niveau de Sécurité différent à toutes les interfacesRéférez-vous à configurer le pour en savoir plus de paramètres d'interface.Ce message d'erreur apparaît également si un périphérique externe envoie un paquet d'IDENT au client interne, qui est lâché par le Pare-feu PIX. Référez-vous aux problèmes de performances PIX provoqués par pour en savoir plus de Protocol d'IDENT

2. **%PIX|ASA-2-106007: Deny inbound UDP from outside address/outside port to inside_address/inside port due to DNS {Response|Query}** **Explication**C'est un message lié à la connexion. Ce message est affiché si la connexion spécifiée échoue en raison d'un **sortant refusent la** commande. La variable de protocole peut être ICMP, TCP, ou UDP.**Action recommandée :** Utilisez la commande **sortante d'exposition** de vérifier les listes sortantes.
3. `%PIX|ASA-3-106014: Deny inbound icmp src interface_name: IP_address dst interface_name: IP_address (type dec, code dec)`**Explication**Les dispositifs de sécurité ont refusé n'importe quel accès de paquet d'ICMP entrant. Par défaut, tous les paquets d'ICMP sont refusés l'accès à moins que spécifiquement permis.
4. `%PIX|ASA-2-106016: Deny IP spoof from (IP_address) to IP_address on interface interface_name.`**Explication**Ce message est généré quand un paquet arrive à l'interface de dispositifs de sécurité qui a une adresse IP de destination de 0.0.0.0 et une adresse MAC de destination de l'interface de dispositifs de sécurité. En outre, ce message est généré quand les dispositifs de sécurité ont jeté un paquet avec une adresse source incorrecte, qui peut inclure un de l'adresse non valide suivante ou autre :Réseau de bouclage (127.0.0.0)Émission (limité, net-dirigé, sous-réseau-dirigé, et tout-sous-réseau-dirigé)La destination host (land.c)Afin d'améliorer plus loin charriez la détection de paquet, utilisent la commande d'**ICMP** de configurer les dispositifs de sécurité pour jeter des paquets avec des adresses sources appartenant au réseau interne. C'est parce que la **commande access-list** a été désapprouvée et n'est plus garanti de fonctionner correctement.**Action recommandée :** Déterminez si un utilisateur externe essaye de compromettre le réseau protégé. Check for misconfigured des clients.
5. `%PIX|ASA-2-106017: Deny IP due to Land Attack from IP_address to IP_address`**Explication**Les dispositifs de sécurité ont reçu un paquet avec l'adresse source IP égale à la destination IP, et la destination port égale au port de source. Ce message indique un paquet charrié qui est conçu pour attaquer des systèmes. Cette attaque est mentionnée comme une attaque de terre.**Action recommandée :** Si ce message persiste, une attaque pourrait être en cours. Le paquet ne fournit pas assez d'informations pour déterminer où l'attaque commence.
6. `%PIX|ASA-1-106021: Deny protocol reverse path check from source_address to dest_address on interface interface_name`**Explication**Une attaque est en cours. Quelqu'un tente de charrier une adresse IP sur une connexion entrante. Unicast RPF, également connu sous le nom de recherche de route inverse, détectée un paquet qui n'a pas une adresse source représentée par une artère et suppose que ce fait partie d'une attaque sur vos dispositifs de sécurité.Ce message apparaît quand vous avez activé Unicast RPF avec l'**IP vérifiez la** commande de **chemin inverse**. Cette caractéristique travaille aux paquets entrés à une interface. S'il est configuré sur l'extérieur, alors les dispositifs de sécurité

vérifient des paquets arrivant de l'extérieur.Les consultations de dispositifs de sécurité un routage en fonction sur l'adresse source. Si une entrée n'est pas trouvée et une artère n'est pas définie, alors ce message du journal système apparaît et la connexion est abandonnée.S'il y a une artère, les dispositifs de sécurité vérifient qui les relient correspondent. Si le paquet arrivait sur une autre interface, c'est ou un charrier ou il y a un environnement asymétrique de routage qui a plus d'un chemin à une destination. Les dispositifs de sécurité ne prennent en charge pas le routage asymétrique.Si les dispositifs de sécurité sont configurés sur une interface interne, ils vérifient les appels de procédure ou le RIP statiques d'**artère**. Si l'adresse source n'est pas trouvée, alors un utilisateur interne charrie leur adresse.**Action recommandée :** Quoiqu'une attaque soit en cours, si cette caractéristique est activée, aucune action de l'utilisateur n'est exigée. Les dispositifs de sécurité repoussent l'attaque.**Remarque:** La commande de **baisse d'asp d'exposition** affiche les paquets ou les connexions abandonnés par le chemin accéléré de Sécurité (asp), qui pourrait vous aider à dépanner un problème. Il indique également quand la dernière fois les compteurs de baisse d'asp ont été effacés. Utilisez la commande RPF-**violée par baisse d'asp d'exposition** dans laquelle le compteur est incrémenté quand l'**IP vérifient le chemin inverse** est configuré sur une interface et les dispositifs de sécurité reçoivent un paquet pour lequel la recherche de route du source ip n'a pas rapporté la même interface comme celle sur laquelle le paquet a été reçu.`ciscoasa#`**`show asp drop frame rpf-violated`** `Reverse-path verify failed 2` **Remarque: Recommandation :** Tracez la source de trafic basée sur le source ip imprimé dans ce prochain message système, et étudiez pourquoi il envoie le trafic charrié.**Remarque: Messages du journal système :** 106021

7. `%PIX|ASA-1-106022: Deny protocol connection spoof from source_address to dest_address on interface interface_name`**Explication**Un paquet appariant une connexion arrive sur une interface différente de l'interface où la connexion a commencé.Par exemple, si un utilisateur commence une connexion sur l'interface interne, mais les dispositifs de sécurité détecte la même connexion arrivant sur une interface de périmètre, les dispositifs de sécurité a plus d'un chemin à une destination. Ceci est connu en tant que routage asymétrique et n'est pas pris en charge sur les dispositifs de sécurité.Un attaquant pourrait également tenter d'ajouter des paquets d'une connexion à l'autre comme manière de diviser en dispositifs de sécurité. Dans l'un ou l'autre de cas, les dispositifs de sécurité affichent ces message et arrêters la connexion.**Action de recommandation :** Ce message apparaît quand l'**IP vérifient la** commande de **chemin inverse** n'est pas configuré. Vérifiez que le routage n'est pas asymétrique.
8. `%PIX|ASA-4-106023: Deny protocol src [interface_name:source_address/source_port] dst interface_name:dest_address/dest_port [type {string}, code {code}] by access_group acl_ID`**Explication**Un paquet IP a été refusé par l'ACL. Affichages de ce message même si vous n'avez pas l'option de **log** activée pour un ACL.**Action de recommandation :** Si les messages persistent de la même adresse source, les messages pourraient indiquer une tentative d'empreinte ou de port-lecture. Contactez les administrateurs de serveur distant.
9. `%PIX|ASA-3-210011: Connection limit exceeded cnt/limit for dir packet from sip/sport to dip/dport on interface if_name.`
10. `%ASA-4-419002: Received duplicate TCP SYN from in_interface:src_address/src_port to out_interface:dest_address/dest_port with different initial sequence number.`**Explication**Ce message du journal système indique que cela l'établissement d'une nouvelle connexion par le périphérique de Pare-feu aura en dépassant au moins une des limites configurées de nombre maximal de connexions. Le message du journal système applique chacun des deux pour des limites de connexion

configurées utilisant une commande statique, ou à ceux configurées utilisant le cadre de stratégie modulaire de Cisco. On ne permettra pas la nouvelle connexion par le périphérique de Pare-feu jusqu'à ce qu'une des connexions existantes soient démolies, apportant de ce fait le compte en cours de connexion au-dessous du maximum configuré.*cnt* — Compte en cours de connexion*limite* — Limite configurée de connexion*dir* — Direction du trafic, d'arrivée ou sortant*sip* — Adresse IP source*sport* — Port de source*immersion* — Adresse IP de destination*dport* — Destination port*if_name* — Nom de l'interface sur laquelle l'unité du trafic est reçue, primaire ou secondaire.**Action de recommandation :** Puisque des limites de connexion sont configurées pour une bonne raison, ce message du journal système pourrait indiquer une attaque DoS possible, dans ce cas la source de trafic pourrait vraisemblablement être une adresse IP charriée. Si l'adresse IP source n'est pas totalement aléatoire, identifier la source et le blocage de elle utilisant une liste d'accès pourraient aider. Dans d'autres cas, obtenir des tracés de renifleur et l'analyse de la source de trafic aideraient en isolant le trafic non désiré du trafic légitime.

Caractéristique de base de détection de menace dans ASA 8.x

L'appliance ASA/PIX de sécurité Cisco prend en charge la caractéristique appelée la détection de menace de la version de logiciel 8.0 et plus tard. Utilisant la détection de base de menace, les dispositifs de sécurité surveillent le débit de paquets lâchés et d'événements de Sécurité dus à ces raisons :

- Refus par des Listes d'accès
- Mauvais format de paquet (tel que la non valide-IP-en-tête ou la non valide-TCP-HDR-longueur)
- Limites de connexion dépassées (les deux au niveau système limites de ressource, et positionnement de limites dans la configuration)
- Attaque DoS détectée (comme un SPI non valide, panne de contrôle de pare-feu dynamique)
- Les contrôles de base de Pare-feu ont manqué (cette option est un débit combiné qui inclut toutes les pertes de paquets liées à la Pare-feu dans cette liste à puces. Il n'inclut pas des baisses liées non Pare-feu telles que la surcharge d'interface, les paquets ont manqué à l'inspection d'application, et à l'attaque de lecture détectée.)
- Paquets méfiants d'ICMP détectés
- Les paquets ont manqué inspection d'application
- Surcharge d'interface
- Attaque de balayage détectée (cette option surveille des attaques de lecture ; par exemple, le premier paquet TCP n'est pas un paquet de synchronisation, ou la connexion TCP a manqué la prise de contact à trois voies. La pleine détection de menace de lecture (référez-vous à configurer le pour en savoir plus de détection de menace de lecture) prend ces informations sur le débit d'attaque de lecture et agit là-dessus en classifiant des hôtes comme attaquants et en les évitant automatiquement, par exemple.)
- Détection inachevée de session telle que l'attaque de synchronisation de TCP détectée ou aucune attaque de session d'UDP de données détectée.

Quand les dispositifs de sécurité détectent une menace, ils envoient immédiatement un message du journal système (730100).

La détection de base de menace affecte la représentation seulement quand il y a des baisses ou des dangers potentiels. Même dans ce scénario, l'incidence des performances est non

significative.

La commande de **débit de menace-détection d'exposition** est utilisée afin d'identifier des attaques potentielles quand vous êtes enregistré dans les dispositifs de sécurité.

```
ciscoasa#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
```

Référez-vous à configurer la section de base de détection de menace du guide de configuration ASA 8.0 pour plus d'informations sur la cloison de configuration.

Message 733100 de Syslog

Message d'erreur :

```
%ASA-4-733100: Object drop rate rate_ID exceeded. Current burst rate is rate_val per second, max
configured rate is rate_val; Current average rate is rate_val per second, max configured rate is
rate_val; Cumulative total count is total_cnt
```

L'objet spécifié dans le message du journal système a dépassé le débit spécifié de seuil de rafale ou le débit moyen de seuil. L'objet peut être activité d'extraction d'un hôte, de port TCP/UDP, de protocole IP, ou de diverses baisses dues aux attaques potentielles. Il indique que le système est soumis aux attaques potentielles.

Remarque: Ces messages d'erreur avec la résolution s'appliquent seulement à ASA 8.0 et plus tard.

1. Objet — La source générale ou particulière de compte de débit de baisse, qui pourrait inclure ces derniers :Pare-feuMauvais paquetsRaté limitAttck DOSBaisse d'ACLLimite conn.Attk d'ICMPBalayageAttck de synchronisationExaminezInterface
2. rate_ID — Le débit configuré qui est dépassé. La plupart des objets peuvent être configurés avec jusqu'à trois débits différents pour différents intervalles.
3. rate_val — Un teneur particulier en débit.
4. total_cnt — Le comptage total puisque l'objet a été créé ou effacé.

Ces trois exemples affichent comment ces variables se produisent :

- Pour une baisse d'interface due à une limite CPU ou de bus :`%ASA-4-733100: [Interface] drop rate 1 exceeded. Current burst rate is 1 per second, max configured rate is 8000; Current average rate is 2030 per second, max configured rate is 2000; Cumulative total count is 3930654`
- Pour une baisse de lecture due au potentiel attaque :`ASA-4-733100: [Scanning] drop rate-1 exceeded. Current burst rate is 10 per second_ max configured rate is 10; Current average rate is 245 per second_ max configured rate is 5; Cumulative total count is 147409 (35 instances received)`
- Pour de mauvais paquets dus aux attaques potentielles :`%ASA-4-733100: [Bad pkts] drop rate 1 exceeded. Current burst rate is 0 per second, max configured rate is 400; Current average rate is 760 per second, max configured rate is 100; Cumulative total count is 1938933`

Action recommandée :

Exécutez ces étapes selon le type d'objet spécifié qui apparaît dans le message :

1. Si l'objet dans le message de Syslog est l'un de ces derniers :Pare-feuMauvais paquetsRaté limitAttaque DoSBaisse d'ACLLimite conn.Attk d'ICMPBalayageAttck de synchronisationExaminezInterfaceVérifiez si le débit de baisse est acceptable pour l'environnement courant.
2. Ajustez le débit de seuil de la baisse particulière à une valeur appropriée en exécutant la commande du **débit** *xxx de menace*-**détection**, où *xxx* est l'un de ces derniers :acl-baissemauvais-paquet-baisseconn.-limite-baisseDOS-baisseFW-baisseICMP-baisseexaminer-baisseinterface-baisselecture-menacesynchronisation-attaque
3. Si l'objet dans le message de Syslog est un TCP ou un port UDP, un protocole IP, ou une baisse d'hôte, contrôle si le débit de baisse est acceptable pour l'environnement courant.
4. Ajustez le débit de seuil de la baisse particulière à une valeur appropriée en exécutant la commande de mauvais-paquet-**baisse de débit de menace-détection**. Référez-vous à la section de base configurante de détection de menace du pour en savoir plus de guide de configuration ASA 8.0.

Remarque: Si vous ne voulez pas le débit de baisse dépassez l'avertissement d'apparaître, vous peut le désactiver en n'exécutant l'**aucune** commande de base-**menace de menace-détection**.

Informations connexes

- Page de support d'appliances de sécurité adaptable de gamme Cisco 5500
- Page de support Cisco 500 gamme PIX
- Les défenses contre des attaques par inondation SYN de TCP
- Cisco a appliqué le bulletin de réduction : Identifiant et exploitation d'atténuation des vulnérabilités de Déni de service dans le module de commutation de contenu
- Cisco a appliqué le bulletin de réduction : Identifiant et exploitation d'atténuation des plusieurs vulnérabilités dans Cisco PIX et les appliances ASA et le Module de services de Pare-feu
- Usurpation d'adresse IP
- Support et documentation techniques - Cisco Systems