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.

Components Used

Les informations de ce document sont basées sur l'appliance de sécurité adaptable (ASA) de la gamme Cisco 5500 qui exécute les versions 7.0 et ultérieures du logiciel.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Produits connexes

Ce document peut également être utilisé avec les PIX de la gamme Cisco 500 qui exécutent les versions 7.0 et ultérieures du logiciel.

Conventions

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

Protection contre les attaques SYN

Comment limitez-vous les attaques SYN (Transmission Control Protocol) sur ASA/PIX ?

Attaque SYN TCP

L'attaque SYN TCP est un type d'attaque DoS dans lequel un expéditeur transmet un volume de connexions qui ne peut pas être terminé. Cela entraîne le remplissage des files d'attente de connexion, refusant ainsi le service aux utilisateurs TCP légitimes.

Lorsqu'une connexion TCP normale démarre, un hôte de destination reçoit un paquet SYN d'un hôte source et renvoie un accusé de réception de synchronisation (SYN ACK). L'hôte de destination doit alors entendre un ACK de l'ACK SYN avant l'établissement de la connexion. Il s'agit de la connexion TCP en trois étapes.

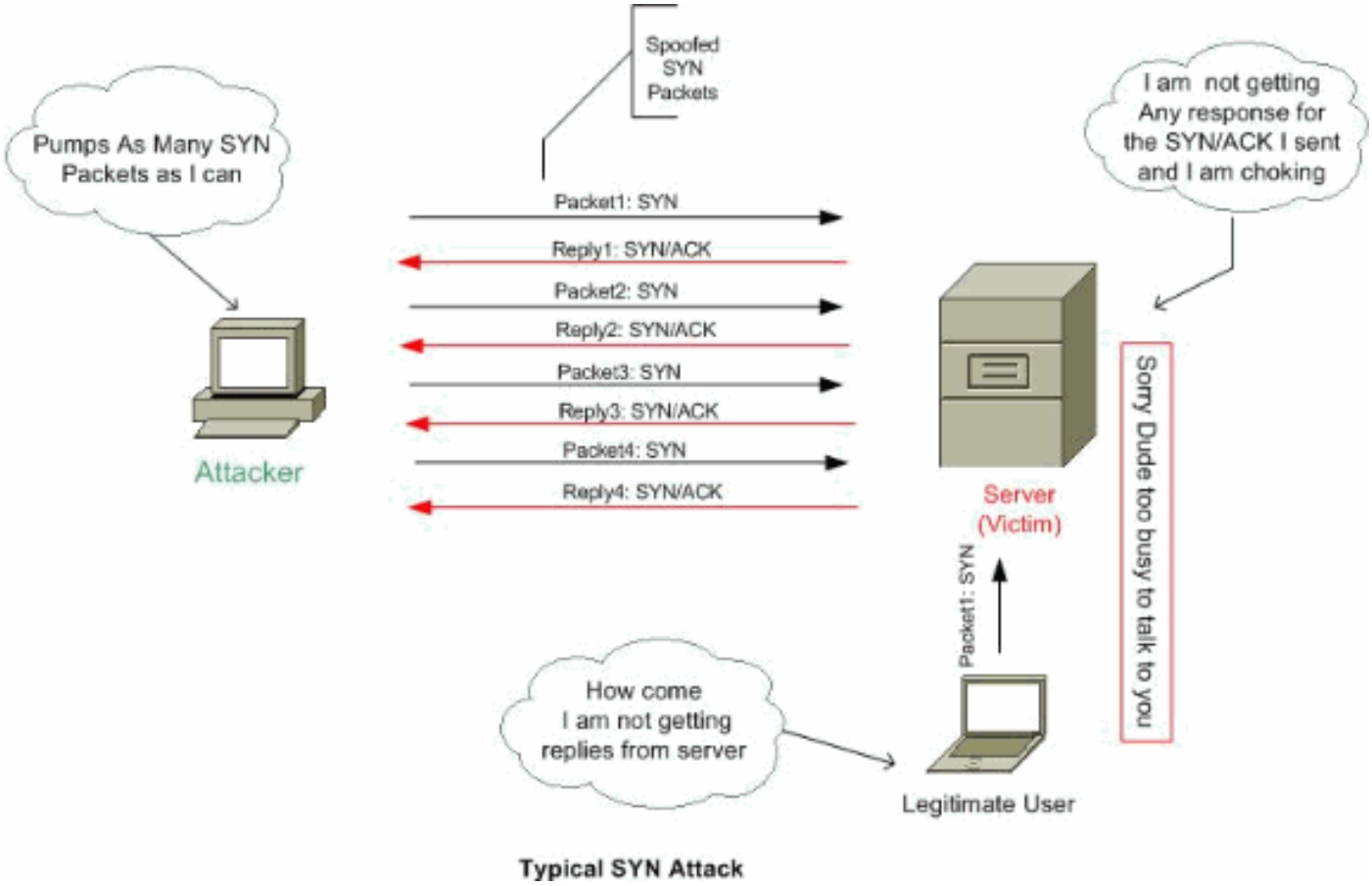
En attendant l'ACK vers l'ACK SYN, une file d'attente de connexion de taille limitée sur l'hôte de destination conserve le suivi des connexions en attente d'achèvement. En règle générale, cette file d'attente se vide rapidement car l'ACK devrait arriver quelques millisecondes après l'ACK SYN.

L'attaque SYN TCP exploite cette conception en demandant à un hôte source d'attaque de générer des paquets SYN TCP avec des adresses source aléatoires vers un hôte victime. L'hôte de destination de la victime renvoie un ACK SYN à l'adresse source aléatoire et ajoute une entrée à la file d'attente de connexion. Comme l'ACK SYN est destiné à un hôte incorrect ou inexistant, la dernière partie de la « connexion en trois étapes » n'est jamais terminée et l'entrée reste dans la file d'attente de connexion jusqu'à l'expiration d'un compteur, généralement pendant environ une minute. En générant rapidement des paquets SYN TCP factices à partir d'adresses IP aléatoires, il est possible de remplir la file d'attente de connexion et de refuser les services TCP (tels que les e-mails, le transfert de fichiers ou le WWW) aux utilisateurs légitimes.

Il n'existe aucun moyen simple de retracer l'auteur de l'attaque car l'adresse IP de la source est falsifiée.

Les manifestations externes du problème incluent l'incapacité d'obtenir des e-mails, l'incapacité d'accepter les connexions aux services WWW ou FTP, ou un grand nombre de connexions TCP sur votre hôte dans l'état SYN_RCVD.

Référez-vous à Défense contre les attaques par inondation TCP SYN pour plus d'informations sur les attaques TCP SYN.



Typical SYN Attack

Atténuation

Cette section décrit comment limiter les attaques SYN en définissant les connexions TCP et UDP maximales, les connexions embryonnaires maximales, les délais d'attente de connexion et comment désactiver la randomisation des séquences TCP.

Si la limite de connexion embryonnaire est atteinte, l'appliance de sécurité répond à chaque paquet SYN envoyé au serveur avec un SYN+ACK et ne transmet pas le paquet SYN au serveur interne. Si le périphérique externe répond avec un paquet ACK, alors le dispositif de sécurité sait qu'il s'agit d'une requête valide (et non d'une attaque SYN potentielle). L'appliance de sécurité établit ensuite une connexion avec le serveur et joint les connexions entre elles. Si l'appliance de sécurité ne récupère pas un ACK du serveur, elle expire agressivement cette connexion embryonnaire.

Chaque connexion TCP comporte deux ISN (Initial Sequence Number) : une générée par le client et une générée par le serveur. L'appliance de sécurité randomise l'ISN du SYN TCP passant dans les directions entrante et sortante.

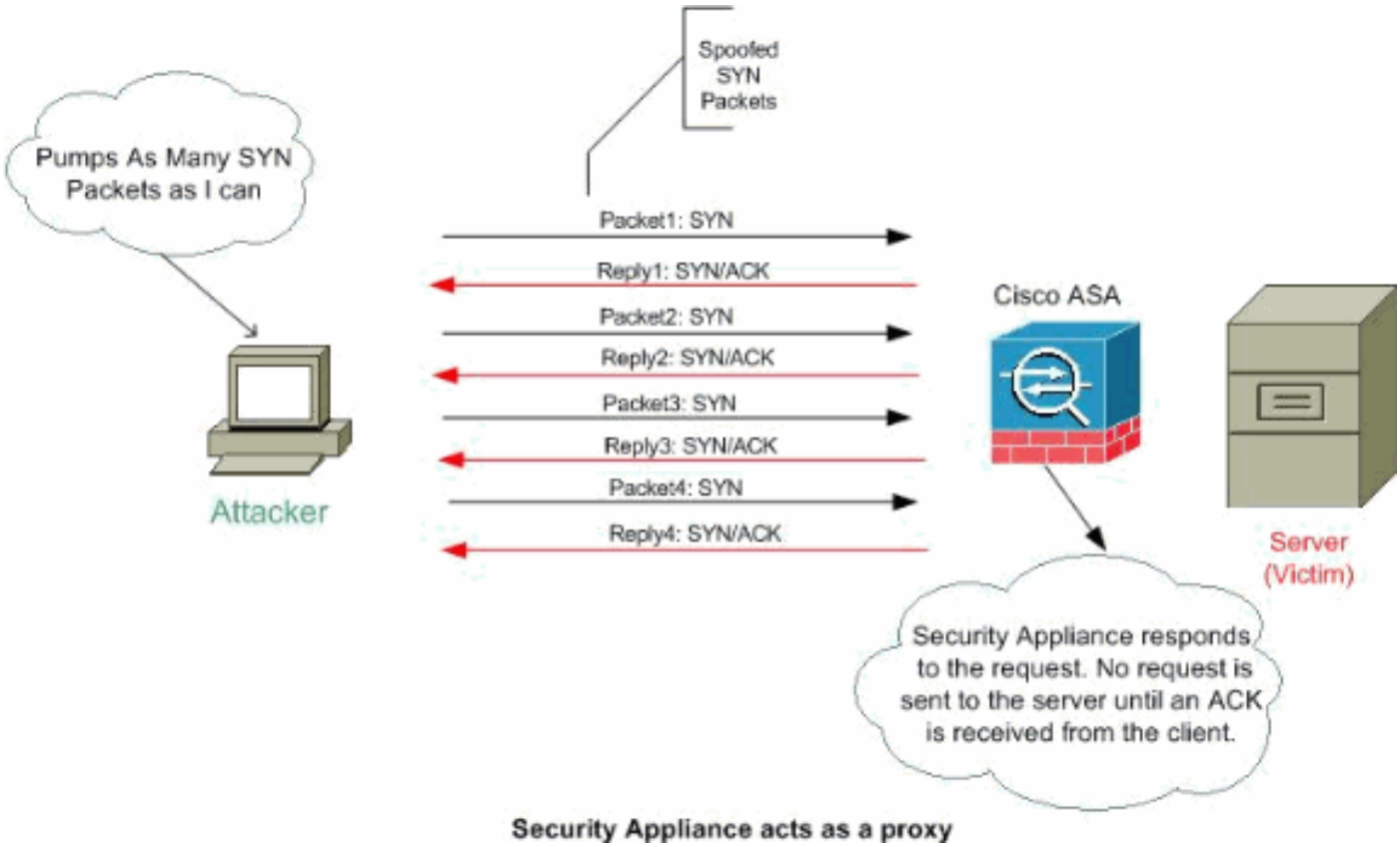
L'aléatoirement du numéro de service intégré de l'hôte protégé empêche un pirate de prédire le prochain numéro de service intégré pour une nouvelle connexion et potentiellement de détourner la nouvelle session.

L'randomisation du numéro de séquence initial TCP peut être désactivée si nécessaire. Exemple :

- Si un autre pare-feu en ligne randomise également les numéros de séquence initiaux, il n'est pas nécessaire que les deux pare-feu exécutent cette action, même si cette action n'affecte pas le trafic.
- Si vous utilisez le multisaut BGP externe (eBGP) via l'appliance de sécurité et que les

homologues eBGP utilisent MD5, la randomisation brise la somme de contrôle MD5.
- Vous utilisez un périphérique WAAS (Wide Area Application Services) qui nécessite que l'appliance de sécurité ne randomise pas les numéros d'ordre des connexions.

Remarque : Vous pouvez également configurer le maximum de connexions, le maximum de connexions embryonnaires et la randomisation des séquences TCP dans la configuration NAT. Si vous configurez ces paramètres pour le même trafic à l'aide des deux méthodes, l'appliance de sécurité utilise la limite inférieure. Pour la randomisation des séquences TCP, si elle est désactivée à l'aide de l'une ou l'autre méthode, l'appliance de sécurité désactive la randomisation des séquences TCP.



Security Appliance acts as a proxy

Complétez ces étapes afin de définir les limites de connexion :

1. Afin d'identifier le trafic, ajoutez une carte de classe à l'aide de la commande **class-map** conformément à Utilisation du cadre de stratégie modulaire.
2. Afin d'ajouter ou de modifier une **carte de stratégie** qui définit les actions à entreprendre avec le trafic de la carte de classe, entrez cette commande :
   ```
   hostname(config)#policy-map name
   ```
3. Afin d'identifier la carte de classe (à partir de l'étape 1) à laquelle vous voulez affecter une action, entrez cette commande :
   ```
   hostname(config-pmap)#class class_map_name
   ```
4. Afin de définir les connexions maximales (TCP et UDP), les connexions embryonnaires maximales, per-client-embryonic-max, per-client-max ou désactiver la randomisation des séquences TCP, entrez 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}}
   ```

Où nombre est un entier compris entre 0 et 65535. La valeur par défaut est 0, ce qui signifie aucune limite sur les connexions.Vous pouvez entrer cette commande sur une seule ligne (dans n'importe quel ordre) ou chaque attribut en tant que commande distincte. La commande est combinée sur une ligne de la configuration en cours.

5. Afin de définir le délai d'attente des connexions, des connexions embryonnaires (semi-ouvertes) et des connexions semi-fermées, entrez cette commande :
   ```
   hostname(config-pmap-c)#set connection {[embryonic hh[:mm[:ss]]]
   [half-closed hh[:mm[:ss]]] [tcp hh[:mm[:ss]]]}
   ```
   Où **embryonnaire** hh[:mm[:ss] est un temps compris entre 0:0:5 et 1192:59:59. La valeur par défaut est 0:0:30. Vous pouvez également définir cette valeur sur 0, ce qui signifie que la connexion ne expire jamais.Les valeurs **semi-fermées** hh[:mm[:ss] et **tcp** hh[:mm[:ss] sont comprises entre 0:5:0 et 1192:59:59. La valeur par défaut pour **semi-fermé** est 0:10:0 et la valeur par défaut pour **tcp** est 1:0:0. Vous pouvez également définir ces valeurs sur 0, ce qui signifie que la connexion ne expire jamais.Vous pouvez entrer cette commande sur une seule ligne (dans n'importe quel ordre) ou chaque attribut en tant que commande distincte. La commande est combinée sur une ligne de la configuration en cours.**Connexion Embryonique (semi-ouverte)** : une connexion embryonnaire est une demande de connexion TCP qui n'a pas terminé la connexion nécessaire entre la source et la destination.**Connexion semi-fermée** : connexion semi-fermée lorsque la connexion est fermée dans une seule direction par l'envoi du FIN. Cependant, la session TCP est toujours gérée par l'homologue.**Per-client-embryonic-max** : nombre maximal de connexions embryonnaires simultanées autorisé par client, compris entre 0 et 65535. La valeur par défaut est 0, ce qui permet des connexions illimitées.**Per-client-max** : nombre maximal de connexions simultanées autorisé par client, compris entre 0 et 65 535. La valeur par défaut est 0, ce qui permet des connexions illimitées.
6. Afin d'activer la carte de stratégie sur une ou plusieurs interfaces, entrez cette commande :
   ```
   hostname(config)#service-policy policymap_name {global | interface interface_name}
   ```

   Où **global** applique la carte de stratégie à toutes les interfaces, et **interface** applique la stratégie à une interface. Une seule politique globale est autorisée. Vous pouvez remplacer la stratégie globale sur une interface en appliquant une stratégie de service à cette interface. Vous ne pouvez appliquer qu'une seule 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 semi-ouvertes pour un hôte particulier,

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, `nombre d'embryons TCP à héberger`, affiche le nombre de sessions semi-ouvertes.

Protection contre les attaques par usurpation d'adresse IP

Le PIX/ASA peut-il bloquer les attaques par usurpation d'adresse IP ?

usurpation d'adresse IP

Afin d'accéder à l'accès, les intrus créent des paquets avec des adresses IP source usurpées. Cela exploite les applications qui utilisent l'authentification basée sur des adresses IP et conduit à un accès non autorisé par l'utilisateur et éventuellement par la racine sur le système cible. Les services rsh et rlogin en sont des exemples.

Il est possible de router les paquets via des pare-feu de routeurs filtrants s'ils ne sont pas configurés pour filtrer les paquets entrants dont l'adresse source se trouve dans le domaine local. Il est important de noter que l'attaque décrite est possible même si aucun paquet de réponse ne peut atteindre le pirate.

Exemples de configurations potentiellement vulnérables :

- Pare-feu proxy dans lequel les applications proxy utilisent l'adresse IP source pour l'authentification
- Routeurs vers réseaux externes prenant en charge plusieurs interfaces internes
- Routeurs avec deux interfaces prenant en charge la création de sous-réseaux sur le réseau interne

Atténuation

Le protocole uRPF (Unicast Reverse Path Forwarding) protège contre l'usurpation d'adresse IP (un paquet utilise une adresse IP source incorrecte pour masquer sa véritable source) en s'assurant que tous les paquets ont une adresse IP source qui correspond à l'interface source correcte conformément à la table de routage.

Normalement, le dispositif de sécurité ne regarde que l'adresse de destination lorsqu'il détermine où transférer le paquet. Le protocole RPF de monodiffusion demande au dispositif de sécurité d'examiner également l'adresse source. C'est pourquoi il s'appelle **Reverse Path Forwarding**. Pour tout trafic que vous souhaitez autoriser via l'appliance de sécurité, la table de routage de l'appliance de sécurité doit inclure une route vers l'adresse source. Voir RFC 2267 pour plus d'informations.

Remarque : Le `: - %PIX-1-106021 : Refuser le contrôle de chemin inverse du protocole de src_addr à dest_addr sur le` message journal `int_name de l'interface` peut être vu lorsque le contrôle de chemin inverse est activé. Désactivez la vérification du chemin inverse à l'aide de la commande **no ip verify inverpath interface (nom d'interface)** afin de résoudre ce problème :

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

Pour le trafic externe, par exemple, l'appliance de sécurité peut utiliser la route par défaut pour satisfaire à la protection RPF de monodiffusion. Si le trafic entre à partir d'une interface externe et que l'adresse source n'est pas connue de la table de routage, l'appliance de sécurité utilise la route par défaut pour identifier correctement l'interface externe en tant qu'interface source.

Si le trafic entre dans l'interface externe à partir d'une adresse connue de la table de routage, mais associée à l'interface interne, alors l'appliance de sécurité abandonne le paquet. De même, si le trafic entre dans l'interface interne à partir d'une adresse source inconnue, le dispositif de sécurité abandonne le paquet parce que la route correspondante (la route par défaut) indique l'interface externe.

Le protocole RPF de monodiffusion est mis en oeuvre comme indiqué :

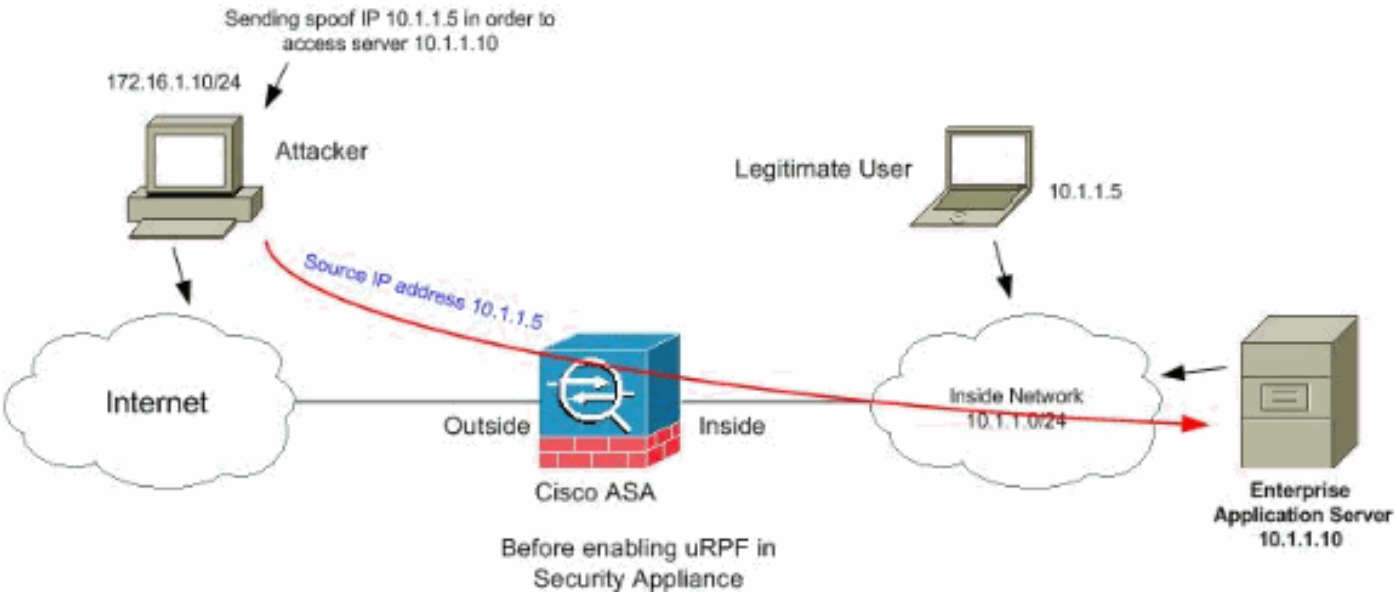
- Les paquets ICMP n'ont pas de session, donc chaque paquet est vérifié.
- UDP et TCP ont des sessions, de sorte que le paquet initial nécessite une recherche de route inverse. Les paquets suivants arrivant pendant la session sont vérifiés à l'aide d'un état existant maintenu dans le cadre de la session. Les paquets non initiaux sont vérifiés pour s'assurer qu'ils sont arrivés sur la même interface utilisée par le paquet initial.

Afin d'activer Unicast RPF, entrez cette commande :

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

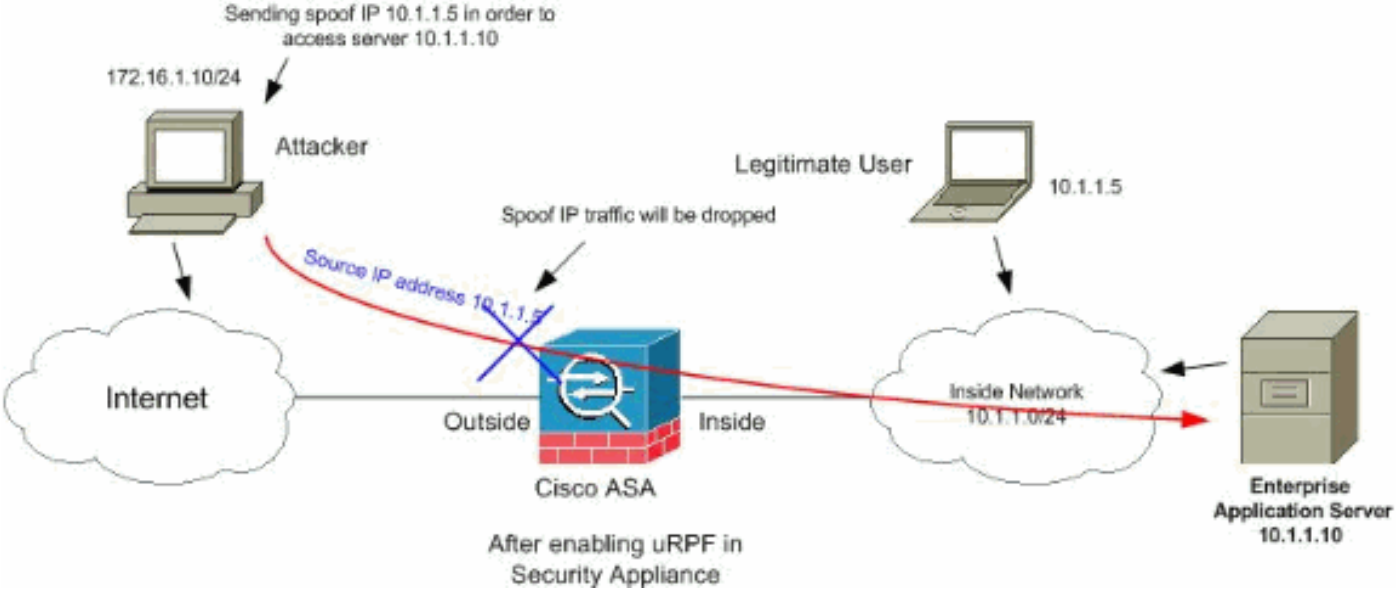
Exemple :

Comme l'illustre cette figure, le PC pirate émet une requête au serveur d'applications 10.1.1.10 en envoyant un paquet avec une adresse IP source falsifiée 10.1.1.5/24, et le serveur envoie un paquet à l'adresse IP réelle 10.1.1.5/24 en réponse à la requête. Ce type de paquet illégal attaque à la fois le serveur d'applications et l'utilisateur légitime dans le réseau interne.



Le protocole RPF de monodiffusion peut empêcher les attaques basées sur l'usurpation d'adresse source. Vous devez configurer le uRPF dans l'interface externe de l'ASA comme indiqué ici :

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



Identification par usurpation à l'aide de messages Syslog

L'appliance de sécurité continue de recevoir des messages d'erreur Syslog comme indiqué. Cela indique des attaques potentielles utilisant des paquets usurpés ou qui peuvent se déclencher en raison d'un 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
```

ExplicationC'est un message lié à la connexion. Ce message se produit lorsqu'une tentative de connexion à une adresse interne est refusée par la stratégie de sécurité définie pour le type de trafic spécifié. Les valeurs *tcp_flags* possibles correspondent aux indicateurs de l'en-tête TCP présents lors du refus de la connexion. Par exemple, un paquet TCP est arrivé pour

lequel aucun état de connexion n'existe dans l'appliance de sécurité, et il a été abandonné. Les *tcp_flags* dans ce paquet sont FIN et ACK.Les *tcp_flags* sont les suivants :ACK : le numéro d'accusé de réception a été reçu.FIN : les données ont été envoyées.PSH : le récepteur a transmis des données à l'application.RST : la connexion a été réinitialisée.SYN : les numéros de séquence ont été synchronisés pour démarrer une connexion.URG : le pointeur urgent a été déclaré valide.Il y a de nombreuses raisons pour lesquelles la traduction statique échoue sur PIX/ASA. Mais une raison courante est que l'interface DMZ (zone démilitarisée) est configurée avec le même niveau de sécurité (0) que l'interface externe.Afin de résoudre ce problème, affectez un niveau de sécurité différent à toutes les interfacesRéférez-vous à Configuration des paramètres d'interface pour plus d'informations.Ce message d'erreur apparaît également si un périphérique externe envoie un paquet IDENT au client interne, qui est abandonné par le pare-feu PIX. Référez-vous à Problèmes de performances PIX causés par le protocole IDENT pour plus d'informations

2. **%PIX|ASA-2-106007: Deny inbound UDP from outside_address/outside_port to inside_address/inside_port due to DNS {Response|Query}**

   ExplicationC'est un message lié à la connexion. Ce message s'affiche si la connexion spécifiée échoue en raison d'une commande **outbound deny**. La variable de protocole peut être ICMP, TCP ou UDP.**Action recommandée :** Utilisez la commande **show outbound** pour 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)`

   ExplicationL'appliance de sécurité a refusé tout accès entrant aux paquets ICMP. Par défaut, tous les paquets ICMP sont refusés à l'accès, sauf autorisation spécifique.

4. `%PIX|ASA-2-106016: Deny IP spoof from (IP_address) to IP_address on interface interface_name.`

   ExplicationCe message est généré lorsqu'un paquet arrive à l'interface de l'appliance de sécurité dont l'adresse IP de destination est 0.0.0.0 et l'adresse MAC de destination de l'interface de l'appliance de sécurité. En outre, ce message est généré lorsque l'appliance de sécurité a rejeté un paquet avec une adresse source non valide, qui peut inclure l'une des adresses suivantes ou une autre adresse non valide :Réseau de bouclage (127.0.0.0)Diffusion (limitée, dirigée par le réseau, dirigée par le sous-réseau et dirigée par tous les sous-réseaux)Hôte de destination (land.c)Afin d'améliorer encore la détection des paquets usurpés, utilisez la commande **icmp** pour configurer l'appliance de sécurité afin de rejeter les paquets dont les adresses source appartiennent au réseau interne. Ceci est dû au fait que la commande **access-list** a été déconseillée et ne fonctionne plus correctement.**Action recommandée :** Déterminez si un utilisateur externe tente de compromettre le réseau protégé. Vérifiez si les clients sont mal configurés.

5. `%PIX|ASA-2-106017: Deny IP due to Land Attack from IP_address to IP_address`

   ExplicationL'appliance de sécurité a reçu un paquet dont l'adresse IP source est égale à la destination IP et le port de destination est égal au port source. Ce message indique un paquet usurpé conçu pour attaquer les systèmes. Cette attaque est appelée attaque terrestre.**Action recommandée :** Si ce message persiste, une attaque peut être en cours. Le paquet ne fournit pas suffisamment d'informations pour déterminer l'origine de l'attaque.

6.

```
%PIX|ASA-1-106021: Deny protocol reverse path check from
source_address to dest_address on interface interface_name
```

ExplicationUne attaque est en cours. Quelqu'un tente d'usurper une adresse IP sur une connexion entrante. Le protocole RPF de monodiffusion, également appelé recherche de route inverse, a détecté un paquet qui n'a pas d'adresse source représentée par une route et suppose qu'il fait partie d'une attaque sur votre appliance de sécurité.Ce message apparaît lorsque vous avez activé Unicast RPF avec la commande **ip verify inverpath**. Cette fonctionnalité fonctionne sur les paquets entrés dans une interface. Si elle est configurée sur l'extérieur, l'appliance de sécurité vérifie les paquets qui arrivent de l'extérieur.L'appliance de sécurité recherche une route en fonction de l'adresse source. Si une entrée est introuvable et qu'une route n'est pas définie, ce message du journal système s'affiche et la connexion est abandonnée.S'il existe une route, le dispositif de sécurité vérifie l'interface qu'il correspond. Si le paquet est arrivé sur une autre interface, il s'agit soit d'une usurpation, soit d'un environnement de routage asymétrique comportant plusieurs chemins vers une destination. Le dispositif de sécurité ne prend pas en charge le routage asymétrique.Si le dispositif de sécurité est configuré sur une interface interne, il vérifie les instructions de commande **route** statique ou RIP. Si l'adresse source est introuvable, un utilisateur interne usurpe son adresse.**Action recommandée :** Même si une attaque est en cours, si cette fonctionnalité est activée, aucune action de l'utilisateur n'est requise. Le dispositif de sécurité repousse l'attaque.**Remarque :** La commande **show asp drop** affiche les paquets ou les connexions abandonnés par le chemin de sécurité accéléré (asp), ce qui peut vous aider à résoudre un problème. Elle indique également le moment où les compteurs de perte asp ont été effacés pour la dernière fois. Utilisez la commande **show asp drop rpf-Violé** dans laquelle le compteur est incrémenté lorsque **ip verify inverse-path** est configuré sur une interface et que l'appliance de sécurité reçoit un paquet pour lequel la recherche de route de l'IP source n'a pas généré la même interface que celle sur laquelle le paquet a été reçu.

```
ciscoasa#show asp drop frame rpf-violated
  Reverse-path verify failed                       2
```

Note : Recommandation : Suivez la source du trafic en fonction de l'adresse IP source imprimée dans ce message système suivant et examinez pourquoi il envoie du trafic usurpé.**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
```

ExplicationUn paquet correspondant à une connexion arrive sur une interface différente de celle de l'interface où la connexion a commencé.Par exemple, si un utilisateur démarre une connexion sur l'interface interne, mais que l'appliance de sécurité détecte la même connexion arrivant sur une interface de périmètre, l'appliance de sécurité a plusieurs chemins vers une destination. Il s'agit d'un routage asymétrique qui n'est pas pris en charge sur l'appliance de sécurité.Un pirate peut également tenter d'ajouter des paquets d'une connexion à une autre afin d'entrer dans l'appliance de sécurité. Dans les deux cas, le dispositif de sécurité affiche ce message et supprime la connexion.**Recommandation Action :** Ce message apparaît lorsque la commande **ip verify inverpath** n'est pas configurée. 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
```

ExplicationUn paquet IP a été refusé par la liste de contrôle d'accès. Ce message s'affiche même si vous n'avez pas l'option **log** activée pour une liste de contrôle d'accès.**Recommandation Action :** Si les messages persistent à partir de la même adresse source, ils peuvent indiquer une tentative d'impression au pied ou d'analyse de port. Contactez les administrateurs de l'hôte 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.
```

ExplicationCe message du journal système indique que l'établissement d'une nouvelle connexion via le périphérique de pare-feu entraînera le dépassement d'au moins une des limites de connexion maximales configurées. Le message du journal système s'applique à la fois aux limites de connexion configurées à l'aide d'une commande statique ou à celles configurées à l'aide de Cisco Modular Policy Framework. La nouvelle connexion ne sera pas autorisée via le périphérique pare-feu tant qu'une des connexions existantes n'est pas désactivée, ce qui fait passer le nombre de connexions en cours sous le maximum configuré.*cnt* : nombre de connexions en cours*limit* : limite de connexion configurée*dir* : direction du trafic, entrant ou sortant*sip* : adresse IP source*sport* - Port source*dip* : adresse IP de destination*dport* - Port de destination*if_name* : nom de l'interface sur laquelle l'unité de trafic est reçue, primaire ou secondaire.**Recommandation Action :** Comme les limites de connexion sont configurées pour une bonne raison, ce message du journal système peut indiquer une attaque DoS possible, auquel cas la source du trafic pourrait être une adresse IP usurpée. Si l'adresse IP source n'est pas totalement aléatoire, l'identification de la source et le blocage à l'aide d'une liste d'accès peuvent aider. Dans d'autres cas, obtenir des traces de renifleur et analyser la source du trafic permettrait d'isoler le trafic indésirable du trafic légitime.

Fonctionnalité de base de détection des menaces dans ASA 8.x

Cisco Security Appliance ASA/PIX prend en charge la fonctionnalité appelée détection des menaces à partir des versions 8.0 et ultérieures du logiciel. Grâce à la détection de base des menaces, l'appliance de sécurité surveille le taux de paquets abandonnés et d'événements de sécurité pour les raisons suivantes :

- Refuser par listes d'accès
- Format de paquet incorrect (tel que 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 (par exemple un SPI non valide, échec de vérification du pare-feu dynamique)
- Échec des vérifications de pare-feu de base (cette option est un taux combiné qui inclut toutes les pertes de paquets liées au pare-feu dans cette liste à puces. Il n'inclut pas les pertes non liées au pare-feu telles que la surcharge de l'interface, l'échec des paquets lors de l'inspection des applications et l'attaque d'analyse détectée.)
- Paquets ICMP suspects détectés
- Échec de l'inspection des applications des paquets

- Surcharge d'interface
- Attaque d'analyse détectée (cette option surveille les attaques d'analyse ; par exemple, le premier paquet TCP n'est pas un paquet SYN, ou la connexion TCP a échoué à la connexion en trois étapes. La détection complète des menaces (reportez-vous à Configuration de l'analyse de la détection des menaces pour plus d'informations) prend ces informations sur le taux d'attaque d'analyse et agit sur elles en classant les hôtes en tant qu'attaquants et en les ignorant automatiquement, par exemple.)
- Détection de session incomplète (attaque SYN TCP, par exemple) détectée ou aucune attaque de session UDP de données détectée.

Lorsque le dispositif de sécurité détecte une menace, il envoie immédiatement un message de journal système (730100).

La détection de base des menaces affecte les performances uniquement en cas de perte ou de menace potentielle. Même dans ce scénario, l'impact sur les performances est négligeable.

La commande **show menaces-detection rate** est utilisée afin d'identifier les attaques potentielles lorsque vous êtes connecté à l'appliance 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 la section Configuration de base de la détection des menaces du guide de configuration ASA 8.0 pour plus d'informations sur la partie configuration.

Message Syslog 733100

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 taux de seuil de rafale spécifié ou le taux de seuil moyen. L'objet peut être une activité de suppression d'un hôte, d'un port TCP/UDP, d'un protocole IP ou de plusieurs abandons en raison d'attaques potentielles. Il indique que le système est menacé.

Remarque : Ces messages d'erreur avec résolution ne s'appliquent qu'à ASA 8.0 et versions ultérieures.

1. Objet : source générale ou particulière d'un décompte de taux d'abandon, qui peut inclure les éléments suivants :Pare-feuPaquets défectueuxLimite de débitAttaque DoSListe déroulante

ACLLimite de connAttaque ICMPAnalyseAttaque SYNInspecterInterface
2. rate_ID : débit configuré dépassé. La plupart des objets peuvent être configurés avec jusqu'à trois débits différents pour différents intervalles.
3. rate_val : valeur de taux spécifique.
4. total_cnt : nombre total depuis la création ou l'effacement de l'objet.

Ces trois exemples montrent comment ces variables se produisent :

- Pour une perte d'interface due à une limitation de 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 perte d'analyse due à des attaques potentielles :
```
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 les paquets défectueux en raison d'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 :

Effectuez ces étapes en fonction du type d'objet spécifié qui apparaît dans le message :

1. Si l'objet du message syslog est l'un des suivants :Pare-feuPaquets défectueuxLimite de débitAttaque DoSListe déroulante ACLLimite de connAttaque ICMPAnalyseAttaque SYNInspecterInterfaceVérifiez si le taux de chute est acceptable pour l'environnement en cours d'exécution.
2. Ajustez le taux de seuil de la perte particulière à une valeur appropriée en exécutant la commande **de taux de détection de menace *xxx, où xxx*** est l'une des suivantes :acl-dropbad-packet-dropconn-limit-dropdos-dropfw-dropicmp-dropinspect-dropinterface-dropanalyse-menaceattaque syn
3. Si l'objet du message syslog est un port TCP ou UDP, un protocole IP ou une perte d'hôte, vérifiez si la vitesse de suppression est acceptable pour l'environnement en cours d'exécution.
4. Ajustez le taux de seuil de la perte particulière à une valeur appropriée en exécutant la commande **de détection de menace bad-packet-drop rate**. Référez-vous à la section Configuration de base de la détection des menaces du Guide de configuration ASA 8.0 pour plus d'informations.

Remarque : Si vous ne voulez pas que l'avertissement de dépassement de la vitesse de chute apparaisse, vous pouvez le désactiver en exécutant la commande **no menace-detection basic-menace**.

Informations connexes

- Page d'assistance relative aux appareils de sécurité adaptatifs de la gamme Cisco 5500
- Page de support Cisco 500 gamme PIX
- Défense contre les attaques par inondation TCP SYN

- Bulletin d'atténuation appliquée de Cisco : Identification et réduction de l'exploitation des vulnérabilités de déni de service dans le module de commutation de contenu
- Bulletin d'atténuation appliquée de Cisco : Identification et réduction de l'exploitation des vulnérabilités multiples dans le module de services de pare-feu et d'appliances Cisco PIX et ASA
- usurpation d'adresse IP
- Support et documentation techniques - Cisco Systems