ASA/PIX 7.x y posterior: Atenuación de los ataques a la red

Contenido

Introducción

Este documento describe cómo mitigar los diversos ataques a la red, tales como servicios negados (DoS), mediante Cisco Security Appliance (ASA/PIX).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en el dispositivo de seguridad adaptable (ASA) de la serie 5500 de Cisco que ejecuta la versión de software 7.0 y posteriores.

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.

Productos Relacionados

Este documento también se puede utilizar con Cisco 500 Series PIX que ejecuta la versión de software 7.0 y posterior.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Protección contra ataques SYN

¿Cómo mitiga los ataques de sincronización/inicio (SYN) del protocolo de control de transmisión (TCP) en ASA/PIX?

Ataque TCP SYN

El ataque TCP SYN es un tipo de ataque DoS en el que un remitente transmite un volumen de conexiones que no se pueden completar. Esto provoca que las colas de conexión se llenen y denieguen el servicio para usuarios TCP legítimos.

Cuando se inicia una conexión TCP normal, un host de destino recibe un paquete SYN de un host de origen y devuelve un mensaje de confirmación de sincronización (SYN ACK). El host de destino debe escuchar un ACK del SYN ACK antes de que se establezca la conexión. Esto se denomina entrada en contacto de tres vías TCP.

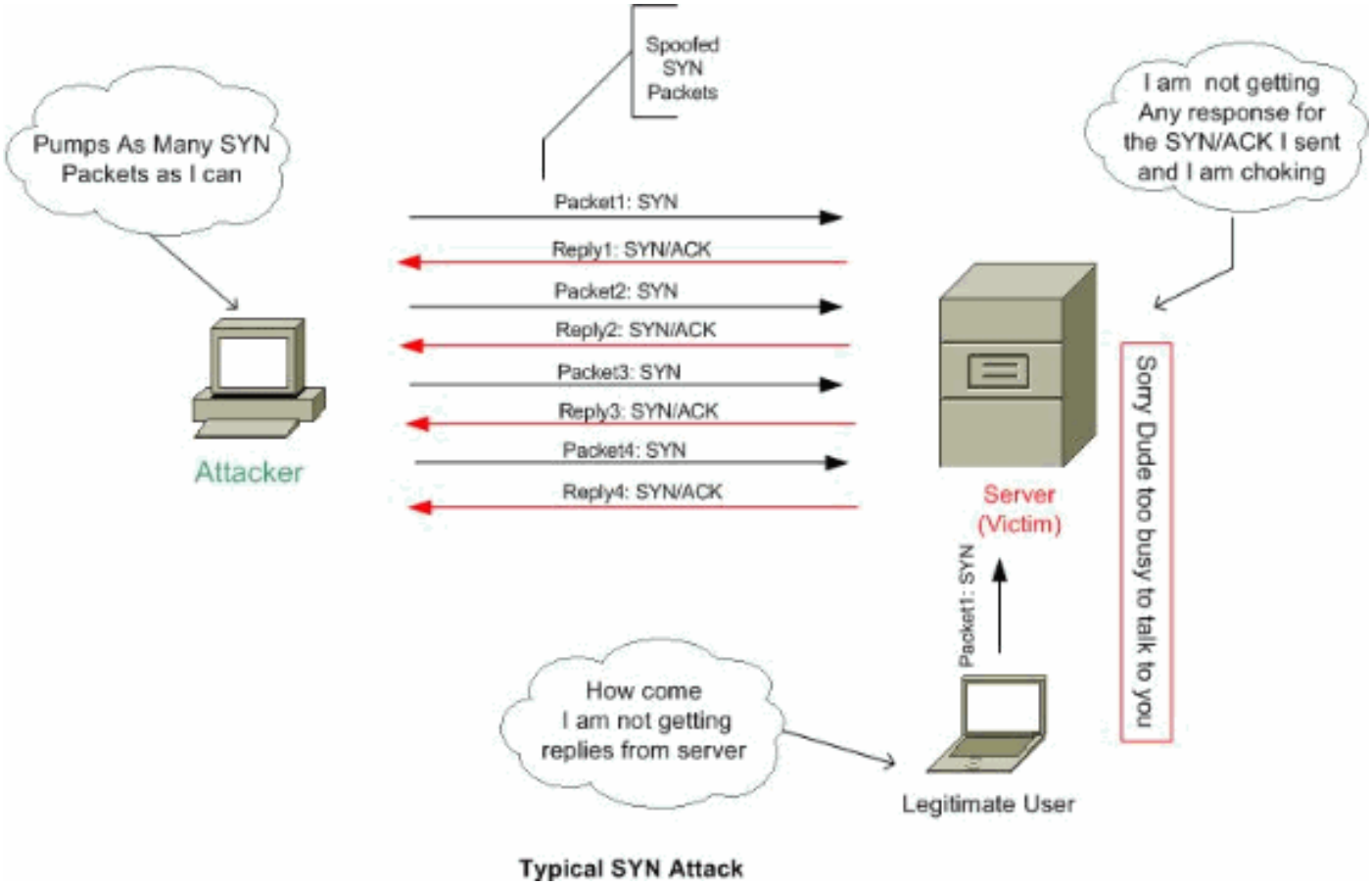
Mientras se espera el ACK en el ACK SYN, una cola de conexión de tamaño finito en el host de destino realiza el seguimiento de las conexiones que están por finalizar. Esta cola normalmente se vacía rápidamente porque se espera que el ACK llegue unos milisegundos después de SYN ACK.

El ataque TCP SYN explota este diseño haciendo que un host de origen atacante genere paquetes TCP SYN con direcciones de origen aleatorias hacia un host víctima. El host víctima de destino envía un SYN ACK de regreso la dirección de origen aleatoria y le agrega una entrada a la cola de conexión. Debido a que SYN ACK está destinado a un host incorrecto o inexistente, la última parte del "intercambio de señales en tres direcciones" nunca se completa y la entrada permanece en la cola de conexión hasta que un temporizador caduca, normalmente durante aproximadamente un minuto. Al generar paquetes SYN TCP falsos de direcciones IP aleatorias a una velocidad rápida, es posible llenar la cola de conexión y denegar los servicios TCP (como correo electrónico, transferencia de archivos o WWW) a usuarios legítimos.

No hay una manera fácil de rastrear el autor del ataque porque la dirección IP del origen está falsificada.

Las manifestaciones externas del problema incluyen la incapacidad de obtener correo electrónico, la incapacidad de aceptar conexiones a WWW o servicios FTP, o un gran número de conexiones TCP en su host en el estado SYN_RCVD.

Consulte Defenses Against TCP SYN Flooding Attacks para obtener más información sobre los ataques TCP SYN.



Typical SYN Attack

Mitigación

Esta sección describe cómo mitigar los ataques SYN estableciendo las conexiones TCP y UDP (protocolo de datagramas de usuario) máximas, las conexiones embrionarias máximas, los tiempos de espera de conexión y cómo deshabilitar la aleatorización de secuencias TCP.

Si se alcanza el límite de conexión embrionaria, el dispositivo de seguridad responde a cada paquete SYN enviado al servidor con un SYN+ACK y no pasa el paquete SYN al servidor interno. Si el dispositivo externo responde con un paquete ACK, el dispositivo de seguridad sabe que es una solicitud válida (y no parte de un posible ataque SYN). A continuación, el dispositivo de seguridad establece una conexión con el servidor y se une a las conexiones. Si el dispositivo de seguridad no obtiene un ACK del servidor, desconecta de forma agresiva esa conexión embrionaria.

Cada conexión TCP tiene dos números de secuencia inicial (ISN): uno generado por el cliente y otro generado por el servidor. El dispositivo de seguridad aleatoriza el ISN del TCP SYN pasando tanto en las direcciones de entrada como de salida.

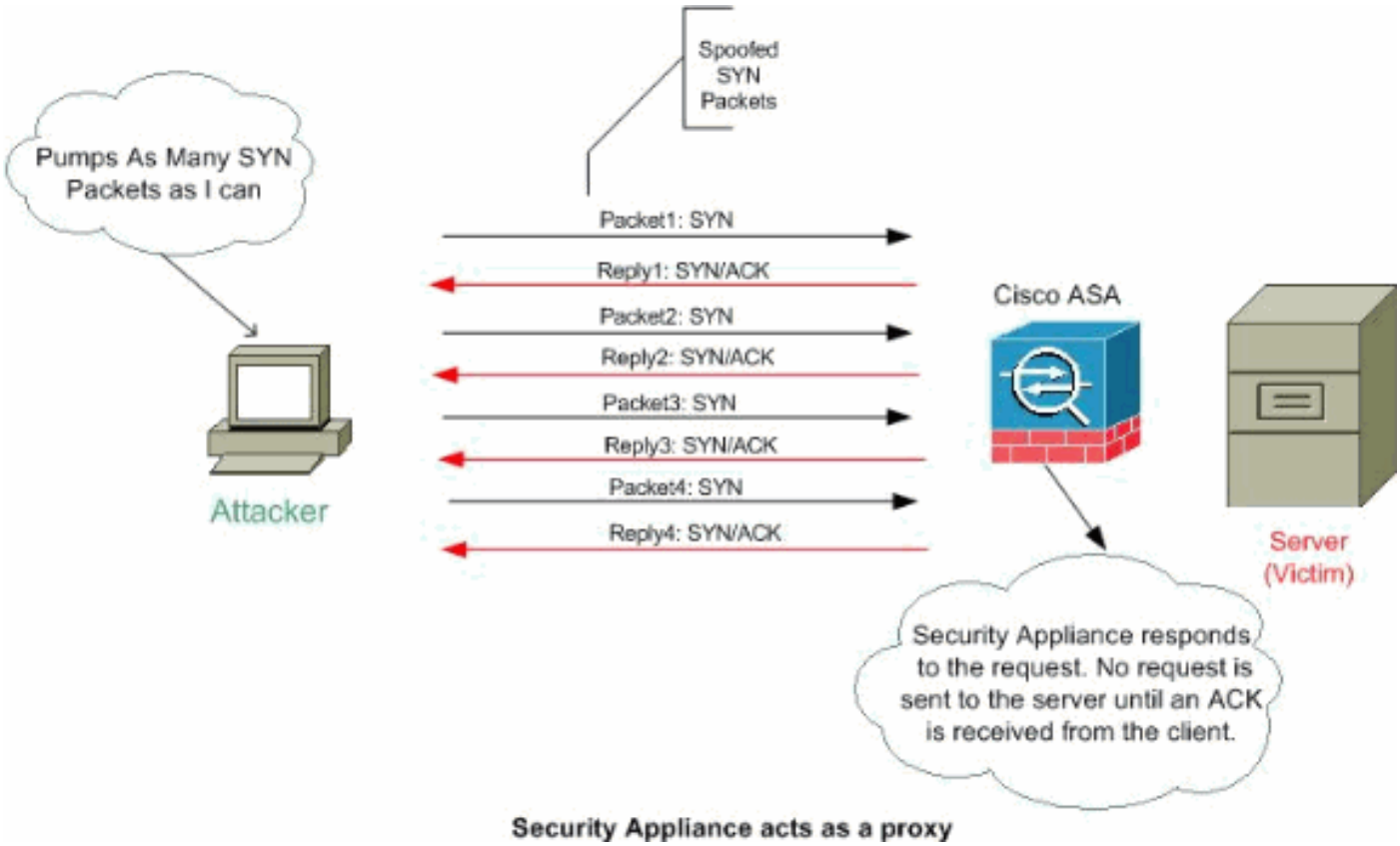
Al aleatorizar el ISN del host protegido, se evita que un atacante prediga el siguiente ISN para una nueva conexión y posiblemente secuestre la nueva sesión.

La aleatorización del número de secuencia inicial de TCP se puede inhabilitar si es necesario. Por ejemplo:

- Si otro firewall en línea también está randomizando los números de secuencia iniciales, no es necesario que ambos firewalls realicen esta acción, aunque esta acción no afecte al tráfico.
- Si utiliza un salto múltiple BGP externo (eBGP) a través del dispositivo de seguridad y los peers eBGP utilizan MD5, la aleatorización interrumpe la suma de comprobación MD5.

- Se utiliza un dispositivo de servicios Wide Area Application Services (WAAS) que requiere que el dispositivo de seguridad no aleatorice los números de secuencia de conexiones.

Nota: También puede configurar conexiones máximas, conexiones embrionarias máximas y aleatorización de secuencia TCP en la configuración NAT. Si configura estos parámetros para el mismo tráfico utilizando ambos métodos, el dispositivo de seguridad utiliza el límite inferior. Para la aleatorización de la secuencia TCP, si se inhabilita mediante cualquiera de los métodos, el dispositivo de seguridad inhabilita la aleatorización de la secuencia TCP.



Security Appliance acts as a proxy

Complete estos pasos para establecer los límites de conexión:

1. Para identificar el tráfico, agregue un mapa de clase usando el comando **class-map** según Using Modular Policy Framework.
2. Para agregar o editar un **policy map** que establezca las acciones a realizar con el tráfico de class map, ingrese este comando:
   ```
   hostname(config)#policy-map name
   ```
3. Para identificar el mapa de clase (desde el paso 1) al que desea asignar una acción, ingrese este comando:
   ```
   hostname(config-pmap)#class class_map_name
   ```
4. Para establecer las conexiones máximas (tanto TCP como UDP), las conexiones embrionarias máximas, per-client-embrionic-max, per-client-max o si inhabilitar la aleatorización de secuencia TCP, ingrese este comando:
   ```
   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}}
   ```
   Donde number es un entero entre 0 y 65535. El valor predeterminado es 0, lo que significa que no hay límite en las conexiones.Puede ingresar este comando todo en una línea (en

cualquier orden) o puede ingresar cada atributo como un comando independiente. El comando se combina en una línea en la configuración en ejecución.

5. Para establecer el tiempo de espera para las conexiones, conexiones embrionarias (semirabiertas) y conexiones semicerradas, ingrese este comando:
   ```
   hostname(config-pmap-c)#set connection {[embryonic hh[:mm[:ss]]]
   [half-closed hh[:mm[:ss]]] [tcp hh[:mm[:ss]]]}
   ```
   Donde **embrionario** hh[:mm[:ss] es un tiempo entre 0:0:5 y 1192:59:59. El valor predeterminado es 0:0:30. También puede establecer este valor en 0, lo que significa que la conexión nunca se agota el tiempo de espera.Los valores **semicerrados** hh[:mm[:ss] y **tcp** hh[:mm[:ss] son un tiempo entre 0:5:0 y 1192:59:59. El valor predeterminado para **semicerrado** es 0:10:0 y el valor predeterminado para **tcp** es 1:0:0. También puede establecer estos valores en 0, lo que significa que la conexión nunca se agota el tiempo de espera.Puede ingresar este comando todo en una línea (en cualquier orden) o puede ingresar cada atributo como un comando independiente. El comando se combina en una línea en la configuración en ejecución.**Conexión embrionaria (semiabierta)**: una conexión embrionaria es una solicitud de conexión TCP que no ha finalizado el intercambio de señales necesario entre el origen y el destino.**Conexión semicerrada**: la mitad de conexión cerrada se cierra cuando la conexión sólo se cierra en una dirección mediante el envío de FIN. Sin embargo, la sesión TCP aún se mantiene por el peer.**Per-client-embrionic-max**: el número máximo de conexiones embrionarias simultáneas permitidas por cliente, entre 0 y 65535. El valor predeterminado es 0, que permite conexiones ilimitadas.**Per-client-max**: el número máximo de conexiones simultáneas permitidas por cliente, entre 0 y 65535. El valor predeterminado es 0, que permite conexiones ilimitadas.
6. Para activar el policy map en una o más interfaces, ingrese este comando:
   ```
   hostname(config)#service-policy policymap_name {global | interface interface_name}
   ```

   Donde **global** aplica el policy map a todas las interfaces, y **la interfaz** aplica la política a una interfaz. Sólo se permite una política global. Puede invalidar la política global en una interfaz aplicando una política de servicio a esa interfaz. Sólo puede aplicar un policy map a cada interfaz.

Ejemplo:

```
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
```

Nota: Para verificar el número total de sesiones semirabiertas para cualquier host en particular, utilice este comando:

```
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
```

Nota: La línea, `recuento embrionario TCP para host`, muestra el número de sesiones semirabiertas.

Protección frente a ataques de suplantación de IP

¿Puede el PIX/ASA bloquear los ataques de simulación IP?

Suplantación de IP

Para obtener acceso, los intrusos crean paquetes con direcciones IP de origen simuladas. Esto explota las aplicaciones que utilizan la autenticación basada en direcciones IP y conduce a usuarios no autorizados y posiblemente a acceso raíz en el sistema de destino. Algunos ejemplos son los servicios rsh y rlogin.

Es posible rutear paquetes a través de firewalls de router de filtrado si no están configurados para filtrar paquetes entrantes cuya dirección de origen está en el dominio local. Es importante tener en cuenta que el ataque descrito es posible incluso si ningún paquete de respuesta puede llegar al atacante.

Entre los ejemplos de configuraciones potencialmente vulnerables se incluyen:

- Firewalls de proxy donde las aplicaciones de proxy utilizan la dirección IP de origen para la autenticación
- Routers a redes externas que admiten varias interfaces internas
- Routers con dos interfaces que admiten la división en subredes en la red interna

Mitigación

Unicast Reverse Path Forwarding (uRPF) protege contra la suplantación de IP (un paquete utiliza una dirección IP de origen incorrecta para ocultar su origen verdadero) al asegurarse de que todos los paquetes tienen una dirección IP de origen que coincide con la interfaz de origen correcta según la tabla de routing.

Normalmente, el dispositivo de seguridad sólo mira la dirección de destino cuando determina dónde reenviar el paquete. Unicast RPF indica al dispositivo de seguridad que también consulte la dirección de origen. Esta es la razón por la que se denomina **Reenvío de Trayectoria Inversa**. Para cualquier tráfico que desee permitir a través del dispositivo de seguridad, la tabla de ruteo

del dispositivo de seguridad debe incluir una ruta de regreso a la dirección de origen. Consulte RFC 2267 para obtener más información.

Nota: El `:- %PIX-1-106021: Denegar la verificación de trayectoria inversa del protocolo de src_addr a dest_addr en el` mensaje de registro `int_name de la interfaz` se puede ver cuando se habilita la verificación de trayectoria inversa. Inhabilite la verificación de trayectoria inversa con el comando **no ip verify reverse-path interface (nombre de la interfaz)** para resolver este problema:

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

Para el tráfico externo, por ejemplo, el dispositivo de seguridad puede utilizar la ruta predeterminada para satisfacer la protección RPF unidifusión. Si el tráfico ingresa desde una interfaz externa y la dirección de origen no es conocida por la tabla de ruteo, el dispositivo de seguridad utiliza la ruta predeterminada para identificar correctamente la interfaz externa como la interfaz de origen.

Si el tráfico ingresa a la interfaz externa desde una dirección que es conocida por la tabla de ruteo pero está asociada con la interfaz interna, entonces el dispositivo de seguridad descarta el paquete. De manera similar, si el tráfico ingresa a la interfaz interna desde una dirección de origen desconocida, el dispositivo de seguridad descarta el paquete porque la ruta coincidente (la ruta predeterminada) indica la interfaz externa.

RPF unidifusión se implementa como se muestra:

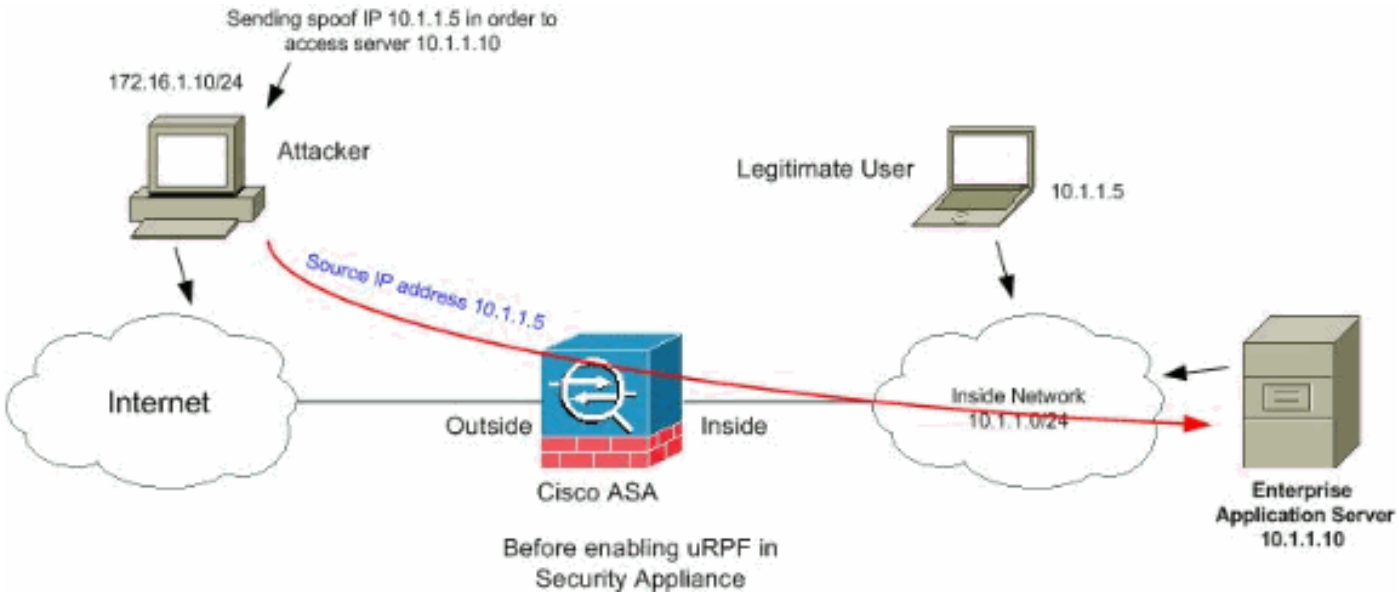
- Los paquetes ICMP no tienen sesión, por lo que se verifica cada paquete.
- UDP y TCP tienen sesiones, por lo que el paquete inicial requiere una búsqueda de ruta inversa. Los paquetes subsiguientes que llegan durante la sesión se comprueban usando un estado existente mantenido como parte de la sesión. Los paquetes no iniciales se comprueban para asegurarse de que llegaron a la misma interfaz utilizada por el paquete inicial.

Para habilitar Unicast RPF, ingrese este comando:

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

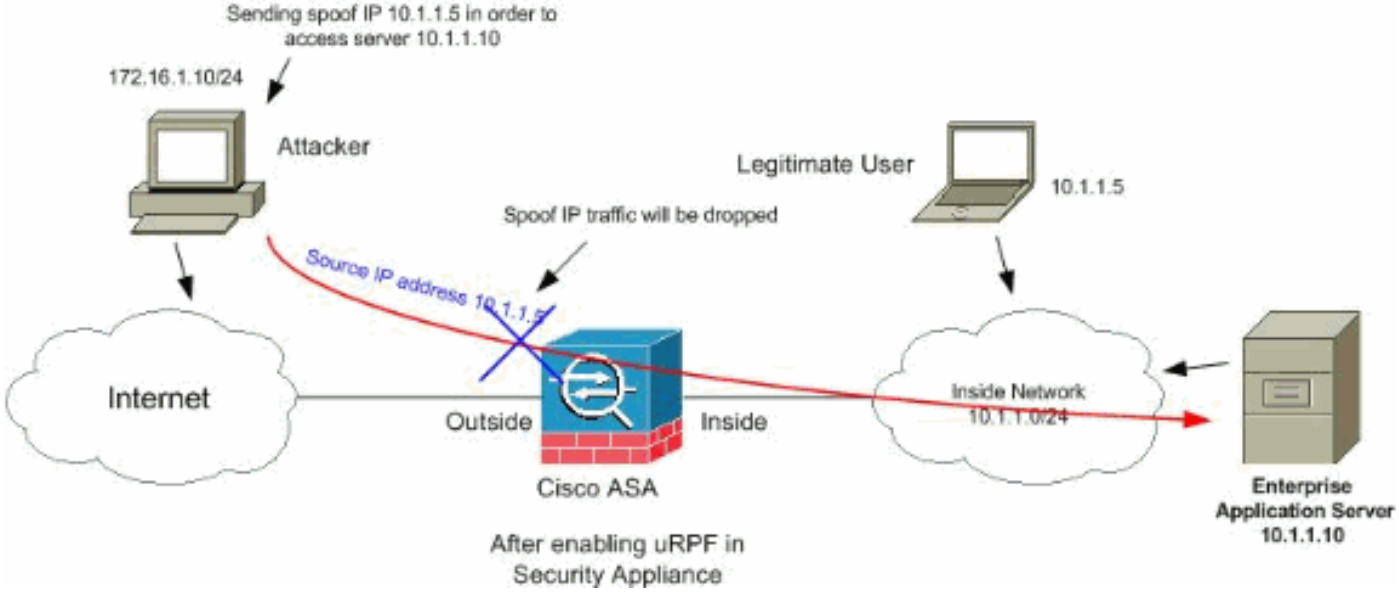
Ejemplo:

Como se muestra en esta figura, el PC atacante origina una solicitud al servidor de aplicaciones 10.1.1.10 enviando un paquete con una dirección IP de origen falsificada 10.1.1.5/24, y el servidor envía un paquete a la dirección IP real 10.1.1.5/24 en respuesta a la solicitud. Este tipo de paquete ilegal atacará tanto al servidor de aplicaciones como al usuario legítimo en la red interna.



RPF unidifusión puede evitar ataques basados en la suplantación de dirección de origen. Debe configurar uRPF en la interfaz exterior del ASA como se muestra aquí:

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



Identificación de simulación mediante mensajes Syslog

El dispositivo de seguridad sigue recibiendo mensajes de error syslog como se muestra. Esto indica ataques potenciales que utilizan paquetes simulados o que podrían desencadenarse debido al ruteo asimétrico.

1.

```
%PIX|ASA-2-106001: Inbound TCP connection denied from IP_address/port
to IP_address/port flags tcp_flags on interface interface_name
```

ExplicaciónEsto es un mensaje relacionado con la conexión. Este mensaje se produce cuando la política de seguridad definida para el tipo de tráfico especificado niega un intento de conexión con una dirección interna. Los valores posibles *tcp_flag* corresponden a los indicadores del encabezado TCP que estaban presentes cuando se denegó la conexión. Por

ejemplo, llegó un paquete TCP para el que no existe ningún estado de conexión en el dispositivo de seguridad y se descartó. Los *indicadores_tcp* en este paquete son FIN y ACK.Los *indicadores_tcp* son los siguientes:ACK: el número de reconocimiento se recibió.FIN: se enviaron datos.PSH: el receptor ha pasado los datos a la aplicación.RST: se restableció la conexión.SYN: los números de secuencia se sincronizaron para iniciar una conexión.URG: el puntero urgente se declaró válido.Hay muchas razones para que la traducción estática falle en el PIX/ASA. Pero, una razón común es si la interfaz de zona desmilitarizada (DMZ) se configura con el mismo nivel de seguridad (0) que la interfaz externa.Para resolver este problema, asigne un nivel de seguridad diferente a todas las interfacesConsulte Configuración de Parámetros de Interfaz para obtener más información.Este mensaje de error también aparece si un dispositivo externo envía un paquete IDENT al cliente interno, que es descartado por el Firewall PIX. Refiérase a Problemas de Rendimiento PIX Causados por el Protocolo IDENT para obtener más información

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

   ExplicaciónEsto es un mensaje relacionado con la conexión. Este mensaje se muestra si la conexión especificada falla debido a un comando **outbound deny**. La variable de protocolo puede ser ICMP, TCP o UDP.**Acción Recomendada:** Utilice el comando **show outbound** para verificar las listas salientes.

3. `%PIX|ASA-3-106014: Deny inbound icmp src interface_name: IP_address dst interface_name: IP_address (type dec, code dec)`

   ExplicaciónEl dispositivo de seguridad negó cualquier acceso de paquete ICMP entrante. De forma predeterminada, se deniega el acceso a todos los paquetes ICMP a menos que se lo permita específicamente.

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

   ExplicaciónEste mensaje se genera cuando un paquete llega a la interfaz del dispositivo de seguridad que tiene una dirección IP de destino de 0.0.0.0 y una dirección MAC de destino de la interfaz del dispositivo de seguridad. Además, este mensaje se genera cuando el dispositivo de seguridad descartó un paquete con una dirección de origen no válida, que puede incluir una de las siguientes direcciones o alguna otra dirección no válida:Red de bucle invertido (127.0.0.0)Difusión (limitada, dirigida a la red, dirigida a la subred y dirigida a todas las subredes)El host de destino (land.c)Para mejorar aún más la detección de paquetes de suplantación, utilice el comando **icmp** para configurar el dispositivo de seguridad para descartar paquetes con direcciones de origen que pertenecen a la red interna. Esto se debe a que el comando **access-list** ha quedado obsoleto y ya no se garantiza que funcione correctamente.**Acción Recomendada:** Determine si un usuario externo está intentando poner en peligro la red protegida. Verifique si hay clientes mal configurados.

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

   ExplicaciónEl dispositivo de seguridad recibió un paquete con la dirección IP de origen igual al destino IP y el puerto de destino igual al puerto de origen. Este mensaje indica un paquete

suplantado que está diseñado para atacar sistemas. Este ataque se denomina ataque terrestre.**Acción Recomendada:** Si este mensaje persiste, es posible que haya un ataque en curso. El paquete no proporciona suficiente información para determinar dónde se origina el ataque.

6.
```
%PIX|ASA-1-106021: Deny protocol reverse path check from
source_address to dest_address on interface interface_name
```
ExplicaciónUn ataque está en curso. Alguien está intentando falsificar una dirección IP en una conexión entrante. RPF unidifusión, también conocido como búsqueda de ruta inversa, detectó un paquete que no tiene una dirección de origen representada por una ruta y asume que es parte de un ataque a su dispositivo de seguridad.Este mensaje aparece cuando ha habilitado Unicast RPF con el comando **ip verify reverse-path**. Esta función funciona en la entrada de paquetes a una interfaz. Si se configura en el exterior, el dispositivo de seguridad verifica los paquetes que llegan desde el exterior.El dispositivo de seguridad busca una ruta basada en la dirección de origen. Si no se encuentra una entrada y no se ha definido una ruta, aparecerá este mensaje de registro del sistema y se eliminará la conexión.Si hay una ruta, el dispositivo de seguridad verifica qué interfaz corresponde. Si el paquete llegó a otra interfaz, es una simulación o hay un entorno de ruteo asimétrico que tiene más de un trayecto a un destino. El dispositivo de seguridad no admite routing asimétrico.Si el dispositivo de seguridad está configurado en una interfaz interna, verifica las sentencias de comando **route** estáticas o RIP. Si no se encuentra la dirección de origen, un usuario interno está simulando su dirección.**Acción Recomendada:** Aunque hay un ataque en curso, si esta función está activada, no se requiere ninguna acción por parte del usuario. El dispositivo de seguridad repele el ataque.**Nota:** El comando **show asp drop** muestra los paquetes o conexiones perdidos por la ruta de seguridad acelerada (asp), lo que podría ayudarle a resolver un problema. También indica cuándo se borraron los contadores de caídas asp por última vez. Utilice el comando **show asp drop rpf-break** en el que se incrementa el contador cuando se configura **ip verify reverse-path** en una interfaz y el dispositivo de seguridad recibe un paquete para el cual la búsqueda de ruta de la IP de origen no produjo la misma interfaz que la en la que se recibió el paquete.
```
ciscoasa#show asp drop frame rpf-violated
  Reverse-path verify failed                       2
```
Nota: Recomendación: Realice un seguimiento del origen del tráfico basado en la IP de origen impresa en este siguiente mensaje del sistema e investigue por qué está enviando tráfico suplantado.**Nota: Mensajes de registro del sistema:** 106021

7.
```
%PIX|ASA-1-106022: Deny protocol connection spoof from source_address
to dest_address on interface interface_name
```
ExplicaciónUn paquete que coincide con una conexión llega a una interfaz diferente de la interfaz donde comenzó la conexión.Por ejemplo, si un usuario inicia una conexión en la interfaz interna, pero el dispositivo de seguridad detecta la misma conexión que llega a una interfaz perimetral, el dispositivo de seguridad tiene más de una ruta a un destino. Esto se conoce como ruteo asimétrico y no se soporta en el dispositivo de seguridad.Un atacante también podría intentar agregar paquetes de una conexión a otra como una forma de entrar en el dispositivo de seguridad. En cualquier caso, el dispositivo de seguridad muestra este mensaje y descarta la conexión.**Acción de recomendación:** Este mensaje aparece cuando el comando **ip verify reverse-path** no está configurado. Verifique que el ruteo no sea asimétrico.

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
```

ExplicaciónLa ACL denegó un paquete IP. Este mensaje se muestra incluso si no tiene la opción **log** habilitada para una ACL.**Acción de recomendación:** Si los mensajes persisten desde la misma dirección de origen, los mensajes pueden indicar un intento de impresión a pie o de escaneo de puertos. Póngase en contacto con los administradores de host remotos.

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.
```

ExplicaciónEste mensaje de registro del sistema indica que el establecimiento de una nueva conexión a través del dispositivo de firewall dará como resultado que se supere al menos uno de los límites máximos de conexión configurados. El mensaje de registro del sistema se aplica tanto a los límites de conexión configurados mediante un comando estático como a los configurados mediante Cisco Modular Policy Framework. La nueva conexión no se permitirá a través del dispositivo de firewall hasta que se desactive una de las conexiones existentes, con lo que el recuento de conexiones actual se sitúa por debajo del máximo configurado.*cnt*: recuento de conexiones actual*limit*: límite de conexión configurado*dir*: dirección del tráfico, entrante o saliente*sip*: dirección IP de origen*sport*: puerto de origen*dip*: dirección IP de destino*dport*: puerto de destino*if_name*: nombre de la interfaz en la que se recibe la unidad de tráfico, principal o secundario.**Acción de recomendación:** Debido a que los límites de conexión se configuran por una buena razón, este mensaje de registro del sistema podría indicar un posible ataque de DoS, en cuyo caso el origen del tráfico podría ser probablemente una dirección IP falsa. Si la dirección IP de origen no es totalmente aleatoria, identificar el origen y bloquearlo mediante una lista de acceso podría ayudar. En otros casos, obtener rastros de sabueso y analizar el origen del tráfico ayudaría a aislar el tráfico no deseado del tráfico legítimo.

Función básica de detección de amenazas en ASA 8.x

Cisco Security Appliance ASA/PIX soporta la función llamada detección de amenazas de la versión de software 8.0 y posteriores. Mediante la detección básica de amenazas, el dispositivo de seguridad monitorea la velocidad de paquetes perdidos y eventos de seguridad debido a estas razones:

- Denegación por listas de acceso
- Formato de paquete incorrecto (como invalid-ip-header o invalid-tcp-hdr-length)
- Se excedieron los límites de conexión (tanto los límites de recursos de todo el sistema como los límites establecidos en la configuración)
- Se ha detectado un ataque DoS (como un SPI no válido, fallo de comprobación de Stateful Firewall)
- Fallaron las comprobaciones básicas del firewall (esta opción es una velocidad combinada que incluye todas las caídas de paquetes relacionadas con el firewall en esta lista con viñetas. No incluye caídas no relacionadas con el firewall, como la sobrecarga de la interfaz, los paquetes fallados en la inspección de la aplicación y el ataque de análisis detectado.)
- Paquetes ICMP sospechosos detectados

- Inspección de aplicación fallida de paquetes
- Sobrecarga de interfaz
- Se ha detectado un ataque de escaneo (esta opción monitorea los ataques de escaneo; por ejemplo, el primer paquete TCP no es un paquete SYN o la conexión TCP falló en el intercambio de señales de 3 vías. La detección de amenazas de escaneo completo (consulte Configuración de Escaneo de la Detección de Amenazas para obtener más información) toma esta información de velocidad de ataque de escaneo y actúa sobre ella clasificando los hosts como atacantes y evitándolos automáticamente, por ejemplo).
- Detección de sesión incompleta como el ataque TCP SYN detectado o no se ha detectado ningún ataque de sesión UDP de datos.

Cuando el dispositivo de seguridad detecta una amenaza, envía inmediatamente un mensaje de registro del sistema (730100).

La detección básica de amenazas afecta al rendimiento sólo cuando hay caídas o amenazas potenciales. Incluso en este escenario, el impacto en el rendimiento es insignificante.

El comando **show threat-detection rate** se utiliza para identificar ataques potenciales cuando se inicia sesión en el dispositivo de seguridad.

```
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
```

Consulte la sección Configuración de la Detección Básica de Amenazas de la Guía de Configuración de ASA 8.0 para obtener más información sobre la parte de configuración.

Mensaje Syslog 733100

Mensaje de error:

```
%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
```

El objeto especificado en el mensaje de registro del sistema ha superado la velocidad de umbral de ráfaga o la velocidad de umbral promedio especificada. El objeto puede ser actividad de descarte de un host, puerto TCP/UDP, protocolo IP o varias caídas debido a ataques potenciales. Indica que el sistema se encuentra en un ataque potencial.

Nota: Estos mensajes de error con resolución sólo se aplican a ASA 8.0 y posteriores.

1. Object: el origen general o particular de un recuento de velocidad de caída, que puede incluir lo siguiente:FirewallPkts incorrectosLímite de velocidadAtaque DoScaída de ACLLímite de

connataque ICMPExploraciónSYN AttackInspeccionarInterfaz
2. rate_ID: la velocidad configurada que se está excediendo. La mayoría de los objetos se pueden configurar con hasta tres velocidades diferentes para intervalos diferentes.
3. rate_val: un valor de velocidad determinado.
4. total_cnt: recuento total desde que se creó o borró el objeto.

Estos tres ejemplos muestran cómo se producen estas variables:

- Para una caída de interfaz debido a una limitación de CPU o 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
```
- Para una caída de la exploración debido a posibles ataques:
```
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)
```
- Para paquetes defectuosos debido a ataques potenciales:
```
%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
```

Acción Recomendada:

Realice estos pasos según el tipo de objeto especificado que aparece en el mensaje:

1. Si el objeto en el mensaje syslog es uno de estos:FirewallPkts incorrectosLímite de velocidadataque DoScaída de ACLLímite de connataque ICMPExploraciónSYN AttackInspeccionarInterfazCompruebe si la velocidad de descarte es aceptable para el entorno en ejecución.
2. Ajuste la velocidad del umbral de la caída en particular a un valor apropiado ejecutando el comando **Threat-Detection Rate *xxx, donde xxx*** es uno de estos:acl-dropbad-packet-dropconn-limit-dropdos caídasfw-dropicmp-dropinspección-descarteinterface-dropamenaza de exploraciónsyn-attack
3. Si el objeto en el mensaje syslog es un puerto TCP o UDP, un protocolo IP o una caída de host, verifique si la velocidad de descarte es aceptable para el entorno en ejecución.
4. Ajuste la velocidad de umbral de la caída en particular a un valor apropiado ejecutando el comando **threat-detection rate bad-packet-drop**. Refiérase a la sección Configuración de la Detección Básica de Amenazas de la Guía de Configuración de ASA 8.0 para obtener más información.

Nota: Si no desea que aparezca la advertencia de exceso de velocidad de descarte, puede desactivarla ejecutando el comando **no threat-detection basic-threat**.

Información Relacionada

- Página de soporte de Cisco 5500 Series Adaptive Security Appliances
- Página de soporte de PIX de la serie 500 de Cisco
- Defensas frente a ataques de inundación TCP SYN
- Boletín de mitigación aplicada de Cisco: Identificación y mitigación de vulnerabilidades de denegación de servicio en el módulo de switching de contenido

- Boletín de mitigación aplicada de Cisco: Identificación y Mitigación de la Explotación de Varias Vulnerabilidades en Cisco PIX y ASA Appliances y Firewall Services Module
- Suplantación de IP
- Soporte Técnico y Documentación - Cisco Systems