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).

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en el dispositivo de seguridad adaptante de las Cisco 5500 Series (ASA) esa versión de software 7.0 de los funcionamientos y posterior.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando,

asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

Este documento se puede también utilizar con las Cisco 500 Series PIX que funciona con 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 los Ataques SYN

¿Cómo usted atenúa el Transmission Control Protocol (TCP) sincroniza/los ataques del comienzo (SYN) en ASA/PIX?

Ataque SYN TCP

El Ataque SYN TCP es un tipo de ataque DOS en quien un remitente transmite un volumen de conexiones que no pueda ser completado. Esto provoca que las colas de conexión se llenen y denieguen el servicio para usuarios TCP legítimos.

Cuando una conexión TCP normal comienza, una computadora principal de destino recibe un paquete SYN de un host de origen y envía detrás una sincronización reconoce (SYN ACK). La computadora principal de destino debe entonces oír un ACK del SYN ACK antes de que se establezca la conexión. Esto se refiere como la entrada en contacto de tres vías TCP.

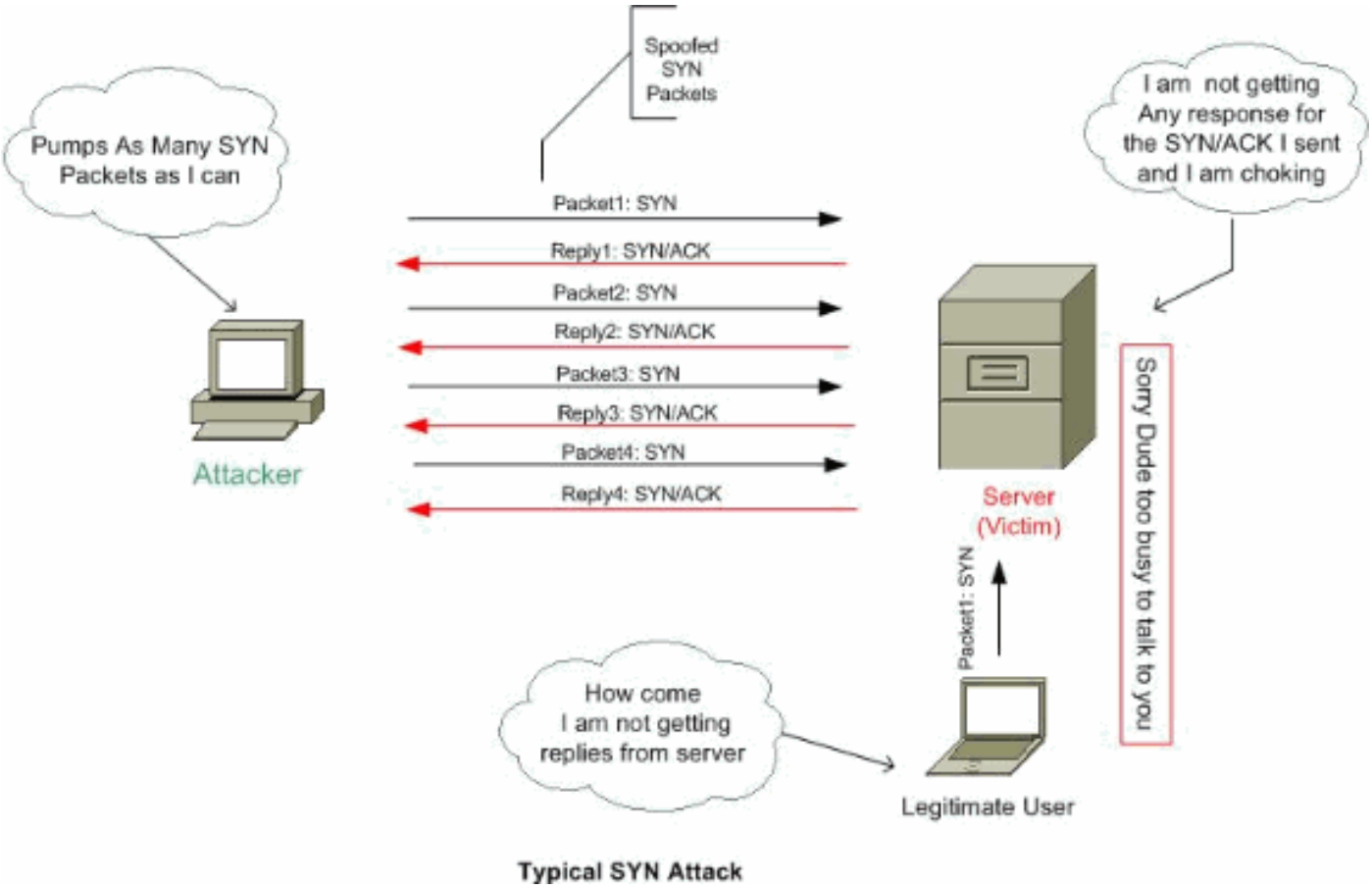
Mientras se espera el ACK en el ACK SYN, una cola de conexión de tamaño finito en el host de destino realiza el seguimiento de las conexiones que están por finalizar. Esta cola vacia típicamente rápidamente porque se espera que llegue el ACK algunos milisegundos después del SYN ACK.

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. Porque el SYN ACK es destinado para un host incorrecto o inexistente, nunca completan a la parte de más reciente la “entrada en contacto de tres vías” y sigue habiendo la entrada en la cola de conexión hasta que un temporizador expire, típicamente para cerca de un minuto. Generando los falsos paquetes SYN TCP de los IP Addresses al azar a una velocidad tan rápida, es posible llenar la cola de conexión y negar los servicios TCP (tales como email, transferencia de archivos, o WWW) a los usuarios legítimos.

No hay forma sencilla de localizar al terminal original del ataque porque la dirección IP de la fuente se forja.

Las manifestaciones externas del problema incluyen la incapacidad para conseguir el email, la incapacidad para validar las conexiones al WWW o a los servicios FTP, o un gran número de conexiones TCP en su host en el estado SYN_RCVD.

Refiera a las defensas contra los ataques de inundación SYN TCP para más información en los Ataques SYN TCP.



Typical SYN Attack

Mitigación

Esta sección describe cómo atenuar los Ataques SYN fijando el máximo TCP y las conexiones del User Datagram Protocol (UDP), las conexiones embrionarias máximas, los tiempos de espera de la conexión, y cómo inhabilitar la distribución aleatoria de la secuencia TCP.

Si se alcanza el límite de la conexión embrionaria, después 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, después el dispositivo de seguridad sabe que es una petición válida (y no parte de un Ataque SYN potencial). El dispositivo de seguridad después establece una conexión con el servidor y se une a las conexiones juntas. Si el dispositivo de seguridad no consigue un ACK detrás del servidor, mide el tiempo agresivamente hacia fuera de esa conexión embrionaria.

Cada conexión TCP tiene dos números de secuencia inicial (ISN): uno generado por el cliente y uno generado por el servidor. El dispositivo de seguridad selecciona al azar el ISN del TCP SYN que pasa en el entrante y las direcciones salientes.

La selección al azar del ISN del host protegido evita que un atacante predecir el ISN siguiente para una nueva conexión y potencialmente secuestre la nueva sesión.

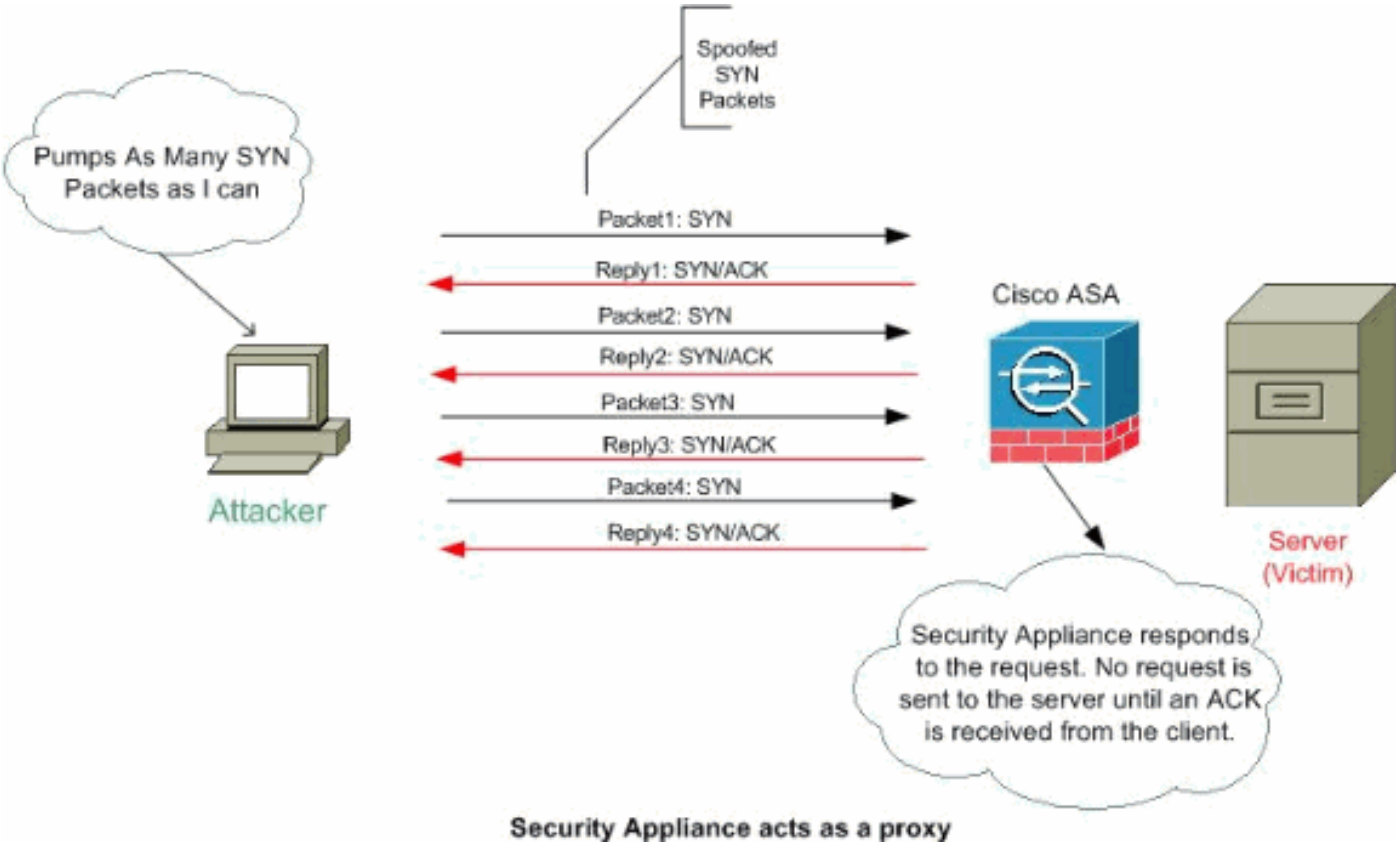
La distribución aleatoria del número de secuencia inicial TCP se puede inhabilitar si procede. Por ejemplo:

- Si otro Firewall en línea también está seleccionando al azar los números de secuencia inicial,

no hay necesidad de ambos Firewall de realizar esta acción, aunque esta acción no afecta al tráfico.

- Si usted utiliza el multi-salto del BGP externo (eBGP) a través del dispositivo de seguridad, y los pares del eBGP están utilizando el MD5, la distribución aleatoria rompe la suma de comprobación MD5.
- Usted utiliza un dispositivo del Wide Area Application Services (WAAS) que requiera el dispositivo de seguridad no seleccionar al azar los números de secuencia de conexiones.

Nota: Usted puede también configurar las cantidades máximas de conexiones, las conexiones embrionarias máximas, y distribución aleatoria de la secuencia TCP en la configuración del NAT. Si usted configura estas configuraciones para el mismo tráfico usando ambos métodos, después el dispositivo de seguridad utiliza el límite más bajo. Para la distribución aleatoria de la secuencia TCP, si se inhabilita usando cualquier método, después el dispositivo de seguridad inhabilita la distribución aleatoria de la secuencia TCP.



Security Appliance acts as a proxy

Complete estos pasos para establecer los límites de la conexión:

1. Para identificar el tráfico, agregue una correspondencia de la clase usando el **comando class-map** según usar el Marco de políticas modular.
2. Para agregar o editar una **correspondencia de políticas** que fije las acciones para tomar con el tráfico de la correspondencia de la clase, ingrese este comando:`hostname(config)#`**`policy-map name`**
3. Para identificar la correspondencia de la clase (del paso 1) a que usted quiere asignar una acción, ingresan este comando:`hostname(config-pmap)#`**`class class_map_name`**
4. Para fijar las cantidades máximas de conexiones (TCP y UDP), las conexiones embrionarias máximas, por-cliente-embrionario-MAX, por-cliente-MAX o si inhabilitar la distribución aleatoria de la secuencia TCP, ingresan 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 está un número

entero el número entre 0 y 65535. El valor por defecto es 0, que no significa ningún límite en las conexiones.Usted puede ingresar este comando all en una línea (en cualquier orden), o usted puede ingresar cada atributo mientras que un comando separado. El comando se combina en una línea en la configuración corriente.

5. Para fijar el descanso para las conexiones, las conexiones embrionarias (mitad-abiertas) y las conexiones semicerradas, ingresan este comando:`hostname(config-pmap-c)#` **`set connection`** `{[` **`embryonic`** `hh[:mm[:ss]]] [` **`half-closed`** `hh[:mm[:ss]]] [` **`tcp`** `hh[:mm[:ss]]]}` Donde hh **embrionario** [: milímetro [: los ss] son una época entre 0:0:5 y 1192:59:59. El valor por defecto es 0:0:30. Usted puede también fijar este valor a 0, que significa que la conexión nunca mide el tiempo hacia fuera.El hh **semicerrado** [: milímetro [: ss] y hh **tcp** [: milímetro [: los valores ss] son una época entre 0:5:0 y 1192:59:59. El valor por defecto para **semicerrado** es 0:10:0 y el valor por defecto para el **tcp** es 1:0:0. Usted puede también fijar estos valores a 0, que significa que la conexión nunca mide el tiempo hacia fuera.Usted puede ingresar este comando all en una línea (en cualquier orden), o usted puede ingresar cada atributo mientras que un comando separado. El comando se combina en una línea en la configuración corriente.**Conexión (medio abierta) embrionaria** — Una conexión embrionaria es una petición de conexión TCP que no ha acabado el apretón de manos necesario entre la fuente y el destino.**Conexión semicerrada** — La conexión semicerrada es cuando la conexión es cerrada solamente en una dirección enviando el FIN. Sin embargo, al par todavía mantiene a la sesión TCP.**Por-cliente-embrionario-MAX** — El número máximo de conexiones embrionarias simultáneas permitidas por el cliente, entre 0 y 65535. El valor por defecto es 0, que permite las conexiones ilimitadas.**Por-cliente-MAX** — El número máximo de conexiones simultáneas permitidas por el cliente, entre 0 y 65535. El valor por defecto es 0, que permite las conexiones ilimitadas.
6. Para activar la correspondencia de políticas en una o más interfaces, ingrese este comando:`hostname(config)#` **`service-policy policymap_name`** *`{global | interface interface_name}`* Cuando sea **global** aplica la correspondencia de políticas a todas las interfaces, y la **interfaz** aplica la directiva a una interfaz. Se permite solamente una política global. Usted puede reemplazar la política global en una interfaz aplicando una política de servicio a esa interfaz. Usted puede aplicar solamente una correspondencia de políticas 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 medio abiertas para cualquier host determinado, 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, `cuenta embrionaria TCP a recibir`, visualiza el número de sesiones medio abiertas.

Protección contra los ataques del IP spoofing

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

IP spoofing

Para acceder, los intrusos crean los paquetes con las dirección IP de origen del spoofed. Esto explota las aplicaciones que utilizan la autenticación basada en los IP Addresses y lleva al usuario no autorizado y posiblemente al acceso a raíz en el sistema objetivo. Los ejemplos son los servicios rsh y de rlogin.

Es posible a los paquetes de Routes con los Firewall del router de filtrado si no se configuran para filtrar los paquetes entrantes cuya dirección de origen está en el dominio local. Es importante observar que el ataque descrito es posible incluso si ningunos paquetes de respuesta pueden alcanzar el atacante.

Los ejemplos de configuraciones que son potencialmente vulnerables incluyen:

- Firewall del proxy donde las aplicaciones del proxy utilizan la dirección IP de origen para la autenticación
- Routers a las redes externas que soportan las interfaces internas múltiples
- El Routers con dos interfaces que soportan subnetting en la red interna

Mitigación

El Unicast Reverse Path Forwarding (uRPF) guarda contra el IP spoofing (un paquete utiliza una dirección IP de origen incorrecta para obscurecer su verdadera fuente) asegurándose de que todos los paquetes tienen una dirección IP de origen que corresponda con la interfaz de origen correcta según la tabla de ruteo.

Normalmente, el dispositivo de seguridad mira solamente a la dirección destino al determinar donde remitir el paquete. El unicast RPF da instrucciones el dispositivo de seguridad también para mirar a la dirección de origen. Esta es la razón por la cual se llama **reenvío de trayecto inverso**. Para cualquier tráfico que usted quiera permitir a través del dispositivo de seguridad, la tabla de ruteo del dispositivo de seguridad debe incluir una ruta de nuevo a la dirección de origen. Vea el RFC 2267 para más información.

Nota: `:- %PIX-1-106021: Niegue el control del trayecto inverso del protocolo del src_addr al dest_addr en el` mensaje del registro del `int_name de la interfaz` puede ser visto cuando se habilita el control del trayecto inverso. Inhabilite el control del trayecto inverso con el **ningún IP verifican el** comando de la **interfaz del trayecto inverso (nombre de la interfaz)** para resolver este problema:

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

Para el tráfico exterior, por ejemplo, el dispositivo de seguridad puede utilizar la ruta predeterminado para satisfacer la protección del unicast RPF. Si el tráfico ingresa de una interfaz exterior, y no conocen a la dirección de origen a la tabla de ruteo, el dispositivo de seguridad utiliza la ruta predeterminado para identificar correctamente la interfaz exterior como la interfaz de origen.

Si el tráfico ingresa la interfaz exterior de un direccionamiento que se sepa a la tabla de ruteo, pero se asocia a la interfaz interior, entonces el dispositivo de seguridad cae el paquete. Semejantemente, si el tráfico ingresa la interfaz interior de un direccionamiento de fuente desconocida, el dispositivo de seguridad cae el paquete porque la ruta que corresponde con (la ruta predeterminado) indica la interfaz exterior.

El unicast RPF se implementa como se muestra:

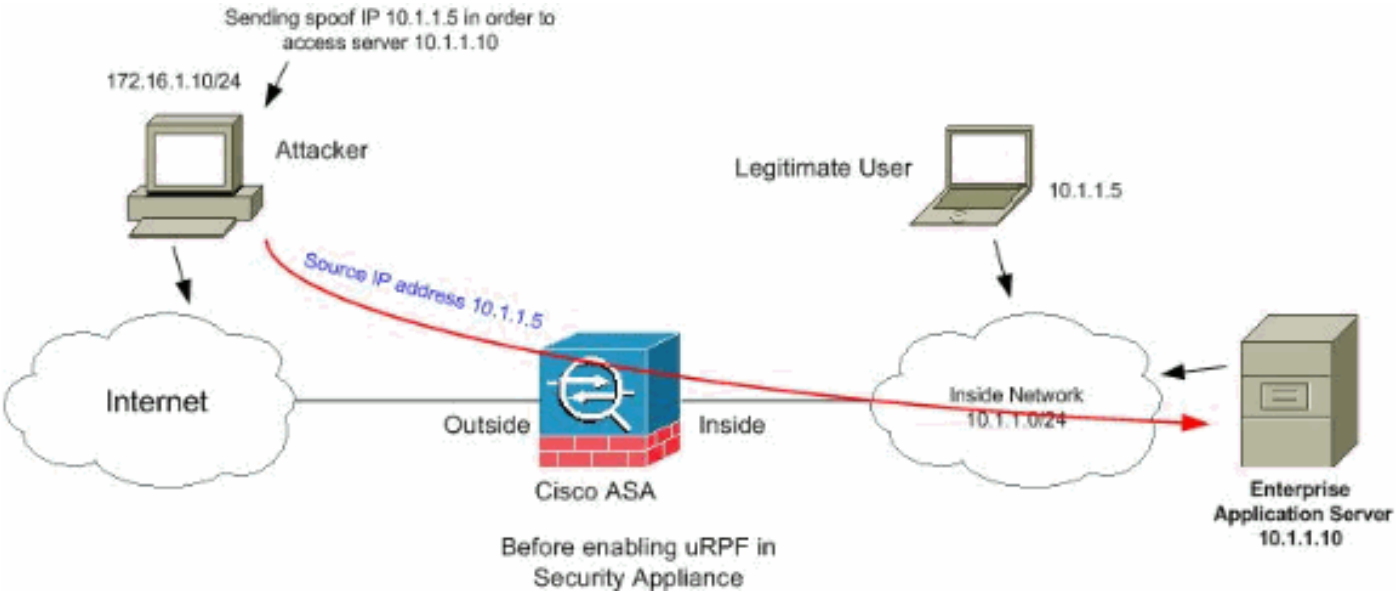
- Los paquetes icmp no tienen ninguna sesión, así que se marca cada paquete.
- El UDP y el TCP tienen sesiones, así que el paquete inicial requiere las operaciones de búsqueda reversas de la ruta. Los paquetes subsiguientes que llegan durante la sesión se marcan usando un estado existente mantenido como parte de la sesión. los paquetes NON-iniciales se marcan para asegurarse que llegaron en la misma interfaz usada por el paquete inicial.

Para habilitar el unicast RPF, ingrese este comando:

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

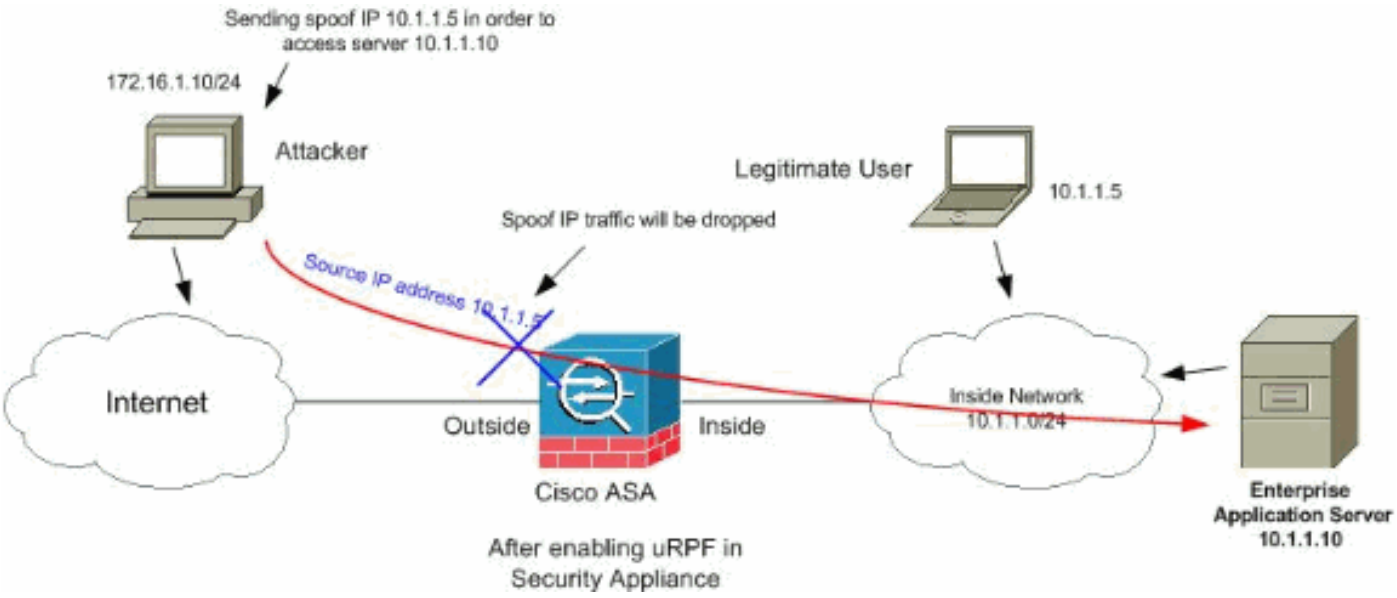
Ejemplo:

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



El unicast RPF puede prevenir los ataques basados en la simulación de la dirección de origen. Usted necesita configurar el uRPF en la interfaz exterior del ASA como se muestra aquí:

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



Identificación del spoofing usando los mensajes de Syslog

El dispositivo de seguridad guarda el recibir de los mensajes de error de syslog como se muestra. Esto indica que los SCR_INVALID usando los paquetes del spoofed o ése pudieron accionar debido al Asymmetric Routing.

1. **%PIX|ASA-2-106001: Inbound TCP connection denied from IP_address/port to IP_address/port flags tcp_flags on interface interface_name** **Explicación**Esto es un mensaje relacionado con la conexión. Este mensaje ocurre cuando una tentativa de conectar con una dirección interna es negada por la política de seguridad que se define para el tipo del tráfico especificado. Los valores posibles de los *tcp_flags* corresponden a los indicadores en el encabezado TCP que eran presente cuando la conexión fue negada. Por ejemplo, un paquete TCP llegó para cuál existe ningún estado de la conexión en el dispositivo de seguridad, y fue caído. *Los tcp_flags* en este paquete son FIN y ACK.*Los tcp_flags* son como sigue:ACK — El número de acuse de recibo fue recibido.FIN — Los datos fueron enviados.PSH — El receptor pasó los datos a la aplicación.RST — La conexión fue reajustada.SYN — Los números de secuencia fueron sincronizados para comenzar una conexión.URG — El puntero urgente era válido declarado.Hay muchas razones de la traducción estática para fallar en el PIX/ASA. Pero, las razones comunes son si la interfaz de la zona desmilitarizada (DMZ) se configura con el mismo nivel de seguridad (0) que la interfaz exterior.Para resolver este problema, asigne un diverso nivel de seguridad a todas las interfacesRefiera a configurar los parámetros de la interfaz para más información.Este mensaje de error también aparece si un dispositivo externo envía un paquete Ident al cliente interno, que es caído por el firewall PIX. Refiera a los problemas de rendimiento de PIX causados por el Protocolo IDENT para 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}** **Explicación**Esto es un mensaje relacionado con la conexión. Se visualiza este mensaje si la conexión especificada falla debido a un **comando deny saliente**. La variable del protocolo puede ser ICMP, TCP, o UDP.**Acción Recomendada:** Utilice el **comando outbound de la demostración** de marcar 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)`**Explicación**El dispositivo de seguridad negó cualquier acceso del paquete del ICMP entrante. Por abandono, todos los paquetes icmp se niegan el acceso a menos que estén permitidos específicamente.

4. `%PIX|ASA-2-106016: Deny IP spoof from (IP_address) to IP_address on interface interface_name.`**Explicación**Se genera este mensaje cuando un paquete llega la interfaz del dispositivo de seguridad que tiene un IP Address de destino de 0.0.0.0 y una dirección MAC del destino de la interfaz del dispositivo de seguridad. Además, se genera este mensaje cuando el dispositivo de seguridad desechó un paquete con una dirección de origen no válida, que puede incluir uno dirección no válida siguiente o de la cierta otra:Red del loopback (127.0.0.0)Broadcast (limitado, red-dirigido, subred-dirigido, y todo-subred-dirigido)La computadora principal de destino (land.c)Para aumentar más lejos la detección del paquete del spoof, utilice el **comando icmp** de configurar el dispositivo de seguridad para desechar los paquetes con las direcciones de origen que pertenecen a la red interna. Esto es porque han desaprobado el **comando access-list** y se garantiza no más para trabajar correctamente.**Acción Recomendada:** Determine si un usuario externo está intentando comprometer la red protegida. Marque para saber si hay clientes mal configurado.
5. `%PIX|ASA-2-106017: Deny IP due to Land Attack from IP_address to IP_address`**Explicación**El dispositivo de seguridad recibió un paquete con el IP Source Address igual al destino IP, y el puerto destino igual al puerto de origen. Este mensaje indica un paquete del spoofed que se diseñe para atacar los sistemas. Se refiere este ataque como un ataque de la pista.**Acción Recomendada:** Si persiste este mensaje, un ataque pudo estar en curso. El paquete no proporciona bastante información para determinar donde el ataque origina.
6. `%PIX|ASA-1-106021: Deny protocol reverse path check from source_address to dest_address on interface interface_name`**Explicación**Un ataque está en curso. Alguien está intentando al spoof una dirección IP en una conexión hacia adentro. Unicast RPF, también conocido como operaciones de búsqueda reversas de la ruta, detectadas un paquete que no tiene una dirección de origen representada por una ruta y asume que es parte de al ataque en su dispositivo de seguridad.Este mensaje aparece cuando usted ha habilitado el unicast RPF con el **IP verifica el** comando del **trayecto inverso**. Esta característica trabaja en la entrada de los paquetes a una interfaz. Si se configura en el exterior, después el dispositivo de seguridad marca los paquetes que llegan del exterior.El dispositivo de seguridad mira para arriba una ruta basada en la dirección de origen. Si una entrada no se encuentra y una ruta no se define, después este mensaje del registro del sistema aparece y se cae la conexión.Si hay una ruta, los controles del dispositivo de seguridad que interconectan corresponde. Si el paquete llegó en otra interfaz, es o un spoof o hay un entorno del Asymmetric Routing que tiene más de una trayectoria a un destino. El dispositivo de seguridad no soporta el Asymmetric Routing.Si el dispositivo de seguridad se configura en una interfaz interna, marca los enunciados de comando o el RIP de la Static ruta. Si no encuentran a la dirección de origen, después un usuario interno es spoofing su direccionamiento.**Acción Recomendada:** Aunque un ataque está en curso, si se habilita esta característica, no se requiere ninguna acción de usuario. El dispositivo de seguridad rechaza el ataque.**Nota:** El comando del **descenso de la demostración ASP** muestra los paquetes o las conexiones caídos por la trayectoria acelerada de la Seguridad (ASP), que pudo ayudarle a resolver problemas un problema. También indica cuando la última vez que borraron a los contadores de caídas ASP. Utilice el comando RPF-**violado descenso de la demostración ASP** en el cual se incrementa el contador cuando el **IP verifica el trayecto inverso** se configura en una interfaz y el dispositivo de seguridad recibe un paquete para el

cual las operaciones de búsqueda de la ruta del IP de la fuente no rindieron la misma interfaz que la en el cual el paquete fue recibido.`ciscoasa#`**`show asp drop frame rpf-violated`**
`Reverse-path verify failed 2` **Nota: Recomendación:** Localice la fuente de tráfico basada en el IP de la fuente impreso en este mensaje del sistema siguiente, e investigue porqué está enviando el tráfico del spoofed.**Nota: Mensajes del registro del sistema:** 106021

7. `%PIX|ASA-1-106022: Deny protocol connection spoof from source_address to dest_address on interface interface_name`**Explicación**Un paquete que corresponde con una conexión llega en una diversa interfaz de la interfaz donde la conexión comenzó.Por ejemplo, si un usuario comienza una conexión en la interfaz interior, solamente el dispositivo de seguridad detecta la misma conexión el llegar en una interfaz del perímetro, el dispositivo de seguridad tiene más de una trayectoria a un destino. Esto se conoce como Asymmetric Routing y no se soporta en el dispositivo de seguridad.Un atacante también pudo intentar añadir los paquetes al final del fichero a partir de una conexión a otra como manera de romperse en el dispositivo de seguridad. En ambos casos, el dispositivo de seguridad visualiza este mensaje y cae la conexión.**Acción de la recomendación:** Este mensaje aparece cuando el **IP verifica el** comando del **trayecto inverso** no se configura. Marque que la encaminamiento no es asimétrica.
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`**Explicación**Un paquete del IP fue negado por el ACL. Este presentaciones del mensaje incluso si usted no tiene la opción del **registro** habilitada para un ACL.**Acción de la recomendación:** Si los mensajes persisten de la misma dirección de origen, los mensajes pudieron indicar una tentativa del huella o de la análisis de puertos. Entre en contacto a los administradores del host remoto.
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.`**Explicación**Este mensaje del registro del sistema indica que eso el establecimiento de una nueva conexión con dispositivo de firewall dará lugar a exceder por lo menos de uno del Máximo configurado de los límites de la conexión. El mensaje del registro del sistema solicita ambos los límites de la conexión configurados usando un comando static, o a ésos configurados usando el Marco de políticas modular de Cisco. La nueva conexión no será permitida con dispositivo de firewall hasta que una de las conexiones existentes se derribe, de tal modo trayendo la cuenta de la conexión actual debajo del Máximo configurado.*cnt* — Cuenta de la conexión actual*límite* — Límite configurado de la conexión*dir* — Dirección del tráfico, entrante o saliente*sorbo* — Dirección IP de origen*deporte* — Puerto de origen*inmersión* — IP Address de destino*dport* — Puerto destino*if_name* — Nombre de la interfaz en la cual se recibe la unidad del tráfico, primario o secundario.**Acción de la recomendación:** Porque los límites de la conexión se configuran por una buena razón, este mensaje del registro del sistema podría indicar un ataque posible DOS, en este caso la fuente del tráfico podría probablemente ser una dirección IP del spoofed. Si la dirección IP de origen no es totalmente al azar, la identificación de la fuente y el bloqueo de ella usando una lista de acceso pudieron ayudar. En otros casos, conseguir las trazas de sniffer y analizar la fuente del tráfico ayudarían en el aislamiento del tráfico no deseado del tráfico legítimo.

Característica básica de la detección de la amenaza en ASA 8.x

El dispositivo del Cisco Security ASA/PIX soporta la característica llamada detección de la amenaza de la versión de software 8.0 y posterior. Usando la detección básica de la amenaza, el dispositivo de seguridad monitorea el índice de paquetes perdidos y de eventos de seguridad debido a estas razones:

- Negación por las Listas de acceso
- Mún formato de paquetes (tal como inválido-IP-encabezado o inválido-TCP-HDR-longitud)
- Límites de la conexión excedidos (ambos límites sistema-anchos del recurso, y conjunto de límites en la configuración)
- Ataque DOS detectado (por ejemplo un error del SPID inválido, del control del escudo de protección con estado)
- Controles básicos del Firewall fallados (esta opción es una tarifa combinada que incluye todas las caídas de paquetes Firewall-relacionadas en esta lista bulleted. No incluye los descensos NON-Firewall-relacionados tales como sobrecarga de la interfaz, paquetes fallados en la Inspección de la aplicación, y ataque de la exploración detectado.)
- Paquetes icmp sospechosos detectados
- Inspección de la aplicación fallada paquetes
- Sobrecarga de la interfaz
- Analizando el ataque detectado (esta opción monitorea los ataques de la exploración; por ejemplo, el primer paquete TCP no es un paquete SYN, o la conexión TCP falló el apretón de manos de tres vías. La detección completa de la amenaza de la exploración (refiera a configurar la detección de la amenaza de la exploración para más información) toma esta información sobre la velocidad del ataque de la exploración y actúa en ella clasificando los host como atacantes y automáticamente evitándolos, por ejemplo.)
- Detección incompleta de la sesión tal como Ataque SYN TCP detectado o ningún ataque de la Sesión UDP de los datos detectado.

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

La detección básica de la amenaza afecta al funcionamiento solamente cuando hay descensos o amenazas potenciales. Incluso en este escenario, el impacto del rendimiento es insignificante.

Utilizan al **comando rate de la amenaza-detección de la demostración** para identificar los SCR_INVALID cuando le registran 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
```

Refiera a configurar la sección básica de la detección de la amenaza de la guía de configuración ASA 8.0 para más información sobre la partición de la configuración.

Mensaje de 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 del registro del sistema ha excedido la tarifa especificada del

umbral de la explosión o la tarifa media del umbral. El objeto puede ser actividad del descenso de un host, del puerto TCP/UDP, protocolo IP, o de los diversos descensos debido a los SCR_INVALID. Indica que el sistema está bajo SCR_INVALID.

Nota: Estos mensajes de error con la resolución son aplicables solamente a ASA 8.0 y posterior.

1. Objeto — El general o la fuente particular de una cuenta de la tarifa del descenso, que pudo incluir éstos:FirewallMún pktsLímite de velocidadAttck DOSDescenso ACLLímite conecAttk ICMPEl analizarAttck SYNExamineInterfaz
2. rate_ID — La velocidad configurada se está excediendo que. La mayoría de los objetos se pueden configurar con hasta tres diversas tarifas para diversos intervalos.
3. rate_val — Un valor de velocidad determinado.
4. total_cnt — El recuento total puesto que el objeto fue creado o borrado.

Estos tres ejemplos muestran cómo ocurren estas variables:

- Para un descenso de la interfaz debido a una limitación CPU o del 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 un descenso de la exploración debido a los SCR_INVALID:`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 los malos paquetes debido a los SCR_INVALID:`%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 de Syslog es uno de éstos:FirewallMún pktsLímite de velocidadAtaque DOSDescenso ACLLímite conecAttk ICMPEl analizarAttck SYNExamineInterfazMarque si la tarifa del descenso es aceptable para el entorno corriente.
2. Ajuste el índice del umbral del descenso determinado a un valor apropiado funcionando con el *comando xxx de la* **tarifa de la amenaza-detección**, donde está uno el *xxx de* éstos:ACL-descensomalo-paquete-descensoCONN-límite-descensoDOS-descensoFW-descensoICMP-descensoexaminar-descensointerfaz-descensoexploración-amenazaAtaque SYN
3. Si el objeto en el mensaje de Syslog es un puerto TCP o UDP, protocolo IP, o un descenso del host, control si la tarifa del descenso es aceptable para el entorno corriente.
4. Ajuste el índice del umbral del descenso determinado a un valor apropiado funcionando con el comando del malo-paquete-**descenso de la tarifa de la amenaza-detección**. Refiera a la sección básica de la detección de la amenaza que configura de la guía de configuración ASA 8.0 para más información.

Nota: Si usted no quiere la tarifa del descenso exceda la advertencia de aparecer, usted puede inhabilitarla no funcionando con el **ningún** comando de la básico-**amenaza de la amenaza-detección**.

Información Relacionada

- Página de soporte adaptante de los dispositivos de seguridad de las Cisco 5500 Series
- Página del soporte de PIX de las Cisco 500 Series
- Defensas contra los ataques de inundación SYN TCP
- Cisco aplicó el boletín de la mitigación: Identificando y explotación de la atenuación de las vulnerabilidades del rechazo de servicio en el módulo content switching
- Cisco aplicó el boletín de la mitigación: Identificando y explotación de la atenuación de las vulnerabilidades múltiples en el Cisco PIX y los dispositivos ASA y el Módulo de servicios del Firewall
- IP spoofing
- Soporte Técnico y Documentación - Cisco Systems