Resolución de problemas de rendimiento de ASA y velocidad de conexión y análisis de capturas de paquetes

Contenido

Introducción

Este documento describe cómo resolver problemas de producción y velocidad de conexión de Cisco Adaptive Security Appliance (ASA).

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 Cisco.

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.

Antecedentes

Algunos clientes pueden experimentar un problema cuando implementan por primera vez un ASA o cuando prueban una nueva conectividad. El problema es que el rendimiento de TCP para las

conexiones que fluyen a través del ASA es mucho menor que cuando el ASA no está en la trayectoria de conexión (o las conexiones son mucho más lentas que antes de que el ASA se implementara en la red).

Por ejemplo, un cliente podría reemplazar un router D-Link de gama baja (u otro dispositivo de ruteo) por un ASA 5505 o un ASA 5510; sin embargo, una vez que se reemplaza el router, la velocidad de conexión se reduce considerablemente. El cliente puede plantear un caso con Cisco TAC porque cree que ASA ha provocado la reducción de la velocidad de conexión.

Metodología de solución de problemas

Los flujos TCP se ralentizan cuando hay pérdida de paquetes o retraso de paquetes en la red. Para entender la causa exacta del problema, los datos deben mostrar los paquetes TCP reales en el cable para esa conexión y cómo la red podría afectarlos. Por lo general, se alerta al administrador de la red del problema cuando realiza una acción específica, como una transferencia de archivos FTP o una prueba de velocidad en línea. La mayoría de las veces se puede reproducir el problema. Por lo tanto, el administrador puede recopilar los datos necesarios para encontrar la causa raíz.

Para recopilar los datos requeridos, el comando **show tech** debe ejecutarse desde el ASA antes y después de la prueba. Este comando muestra la configuración y las estadísticas de paquetes (principalmente de **show service-policy**) y también muestra si los errores de la interfaz aumentan.

Las capturas de paquetes simultáneas bidireccionales (tomadas de las dos interfaces ASA afectadas por la conexión) son necesarias para diagnosticar completamente la causa del problema.

Consulte estos documentos para ver ejemplos de cómo aplicar capturas de paquetes al ASA:

- Solución de problemas de conexiones a través de PIX y ASA
- Episodio de podcast de seguridad del TAC nº 1: uso de la utilidad de captura de paquetes ASA para la resolución de problemas

Análisis de datos

Una vez que recopile los datos requeridos, puede utilizar las capturas de paquetes para determinar cuál de estos problemas podría haber ocurrido:

- Los paquetes del host externo se descartan o se retrasan antes de que lleguen a la interfaz externa del ASA.
- Los paquetes son demorados o descartados por el ASA.
- Los paquetes se retrasan o se descartan en algún lugar de la red interna.

  Nota: Este análisis asume que los datos se envían desde un host en la interfaz exterior a un host en la interfaz interna.

Este vídeo muestra un ejemplo de cómo realizar el análisis en una captura de paquetes:

La fusión de flujo TCP es una consideración técnica específica para este problema porque, cuando se utilizan ciertas funciones en el ASA, el firewall une completamente el flujo TCP que

pasa a través de él.

Por ejemplo, si el ASA detecta un paquete que falta en la red (ya que no se recibe en el ASA), envía un ACK en nombre del otro extremo TCP para los datos que faltan. Este escenario es el más común. Si el ASA detecta los paquetes que llegan fuera de servicio, el ASA reordena los paquetes y los pasa al receptor en el orden adecuado. Si no hay caídas de red o reordenamiento de paquetes, no hay efectos secundarios para habilitar esta función. Si todos los paquetes enviados por cualquiera de los extremos TCP pasaron exitosamente a través de la red y el ASA, no sabría que esta función está habilitada porque no toma acción sobre los flujos de paquetes. Sólo cuando haya problemas con la conexión TCP en la red, esta función ralentizará aún más el tráfico de red. El acto de unir el flujo TCP es muy intenso en recursos para el ASA. Por cada paquete descartado en la red, el ASA no sólo debe enviar un paquete TCP que solicite la retransmisión de ese paquete, sino que también debe almacenar en búfer los paquetes que el remitente continuó enviando después de que el paquete faltara.

Problemas Comunes

Valores de velocidad y dúplex mal configurados en la interfaz que conecta ASA al dispositivo adyacente

Este problema ocurre a menudo cuando un dispositivo es reemplazado por un ASA. Si los valores de velocidad y dúplex en la interfaz ASA no son los mismos que los valores en el dispositivo adyacente, las caídas de paquetes ocurren en esa interfaz. Verifique los valores de velocidad y dúplex en la interfaz ASA así como en la interfaz adyacente.

Verifique la salida **show interface** del ASA para ver si hay errores obvios que sean síntomas de este problema:

```
Interface Ethernet0/0 "Outside", is up, line protocol is up
Hardware is i82546GB rev03, BW 100 Mbps
Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
MAC address 0019.2f58.c324, MTU 1500
IP address 192.168.222.122, subnet mask 255.255.255.252
124047996 packets input, 35340918453 bytes, 0 no buffer
Received 3 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 L2 decode drops
156918660 packets output, 40931551514 bytes, 0 underruns
1 output errors, 4286634 collisions, 0 interface resets
0 babbles, 123332 late collisions, 4752834 deferred
0 lost carrier, 0 no carrier
input queue (curr/max blocks): hardware (0/0) software (0/0)
output queue (curr/max blocks): hardware (0/245) software (0/0)
Traffic Statistics for "Outside":
124047995 packets input, 33107957301 bytes
157041993 packets output, 38195084709 bytes
103480 packets dropped
1 minute input rate 2140 pkts/sec, 477200 bytes/sec
1 minute output rate 2630 pkts/sec, 396763 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 2152 pkts/sec, 525496 bytes/sec
5 minute output rate 2701 pkts/sec, 421215 bytes/sec
5 minute drop rate, 0 pkts/sec
```

Enviar tráfico al módulo IPS

Cuando el ASA se configura para enviar tráfico al módulo IPS, la función de coalescencia de flujo TCP se activa en el ASA. Refiérase a la sección *Análisis de Datos* de este documento para obtener más información sobre la función de coalescencia de flujo TCP.

La modificación de ASA de la opción TCP MSS causa una ligera disminución del rendimiento

De forma predeterminada, el ASA establece la opción TCP MSS en los paquetes SYN en 1380. Por lo tanto, los extremos TCP no deben transmitir un segmento TCP mayor que 1380 bytes. Este valor es inferior al valor predeterminado de 1460 bytes y representa una caída del rendimiento de TCP de alrededor del seis por ciento (6%). El rendimiento podría mejorar si aumenta la configuración máxima de MSS en el ASA o inhabilita el ajuste de MSS. Antes de modificar el comando predeterminado en el ASA, comprenda los riesgos relacionados con la posible fragmentación si el paquete se encapsula más en alguna parte del trayecto.

Para obtener más información, consulte la sección tcpmss de conexión sysopt de *Referencia de Comandos de Cisco ASA 5500 Series*.

Información Relacionada

- Referencia de Comandos de Cisco ASA 5500 Series, 8.2
- Soporte Técnico y Documentación - Cisco Systems