Producción ASA y capturas de paquetes del troubleshooting y el analizar de la velocidad de la conexión

Resumen

Introducción

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

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 Cisco (ASA).

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.

Antecedentes

Algunos clientes pudieron experimentar un problema cuando primero despliegan un ASA o cuando prueban la nueva Conectividad. El problema es el rendimiento de procesamiento de TCP para las conexiones que atraviesan el ASA son mucho más bajas que cuando el ASA no está en el trayecto de conexión (o las conexiones sea mucho más lento que antes de que el ASA fuera implementado en la red).

Por ejemplo, un cliente pudo substituir el router de menor capacidad de D-Link (o el otro dispositivo de ruteo) por un ASA 5505 o un ASA 5510; sin embargo, una vez que substituyen al router, la velocidad de la conexión se reduce grandemente. El cliente pudo plantear un caso con el TAC de Cisco porque creen que el ASA causó la reducción en la velocidad de la conexión.

Información sobre la Función

Metodología de Troubleshooting

Los flujos TCP retrasan cuando hay pérdida del paquete o retraso de paquetes en la red. Para entender la causa exacta del problema, los datos deben mostrar los paquetes TCP reales en el alambre para esa conexión y cómo la red pudo afectarles. Alertan generalmente a un administrador de la red al problema cuando realizan una acción específica, tal como una transferencia de archivos FTP o una prueba de velocidad en línea. El problema puede ser reproducido lo más a menudo posible. Por lo tanto, el administrador puede recopilar los datos requeridos para encontrar la causa raíz.

Para recopilar los datos requeridos, el **comando show tech** debe ser funcionado con del ASA antes y después de la prueba. Este comando muestra la configuración y las estadísticas de paquete (principalmente de la servicio-**directiva de la demostración**) y también las demostraciones si los errores de interfaz incrementan.

Requieren a las capturas de paquetes bidireccionales, simultáneas (tomadas de las dos interfaces ASA afectadas que las travesías de la conexión) diagnosticar completamente la causa del problema.

Refiera a estos documentos por ejemplos de cómo aplicar a las capturas de paquetes al ASA:

- Resuelva problemas las conexiones con el PIX y el ASA
- Episodio #1 del podcast de la Seguridad de TAC - Usando la utilidad de la captura de paquetes ASA para resolver problemas

Análisis de datos

Una vez que usted recopila los datos requeridos, usted puede utilizar a las capturas de paquetes para determinar que de estos problemas pudieron haber ocurrido:

- Los paquetes del host exterior se caen o se retrasan antes de que alcancen la interfaz exterior ASA.
- Los paquetes son retrasados o caídos por el ASA.
- Los paquetes se retrasan o se caen en alguna parte en la red interna.

  Nota: Este análisis asume que los datos están enviados de un host en la interfaz exterior a un host en la interfaz interior.

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

La secuencia TCP que se une es un específico técnico de la consideración a este problema porque, cuando usted dedica ciertas características en el ASA, se une el Firewall completamente la secuencia TCP que pasa con él.

Por ejemplo, si el ASA descubre un paquete faltante en la red (puesto que no se recibe en el ASA), envía un ACK en nombre del otro Punto final de TCP para los datos que falta. Este escenario es el más común. Si el ASA descubre los paquetes que llegan fuera de servicio, el ASA reordena los paquetes y los pasa al receptor en la orden apropiada. Si no hay descensos o paquete de la red que reordenan, no hay efectos secundarios a habilitar esta característica. Si todos los paquetes enviados por cualquier Punto final de TCP pasajero con éxito con la red y el

ASA, usted no sabrían se habilita esta característica puesto que no toma medidas en los flujos de paquetes. Solamente cuando hay el problema con la conexión TCP en la red habilitando esta característica más lejos para retrasar el tráfico de la red. El acto de unirse la secuencia TCP es mismo uso intensivo de recurso para el ASA. Para cada paquete caído en la red el ASA debe no sólo enviar una petición del paquete TCP la retransmisión de ese paquete, pero debe también mitigar los paquetes que el remitente continuó enviando después de que el paquete fuera a faltar.

Problemas Comunes

Valores mal configurado de la velocidad y dúplex en la interfaz que conecta el ASA con el dispositivo adyacente

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

Marque la **salida de la interfaz de la demostración del** ASA para los claros errores que son 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
```

Envíe el tráfico al módulo ips

Cuando el ASA se configura para enviar el tráfico al módulo ips, la característica que se une de la secuencia TCP se dedica en el ASA. Refiera a la sección de la *análisis de datos de* este documento para más información sobre la característica que se une de la secuencia TCP.

La modificación ASA de las causas de la opción MSS TCP menosprecia la disminución del funcionamiento

Por abandono el ASA fija la opción MSS TCP en los paquetes SYN a 1380. Por lo tanto, los Puntos finales de TCP no deben transmitir bytes más grandes de un segmento TCP de 1380. Este valor es más bajo que a menudo el valor predeterminado de 1460 bytes y representa un descenso del rendimiento del TCP del alrededor seis por ciento (el 6%). El funcionamiento pudo mejorar es usted aumento la configuración del máximo MSS en el ASA o inhabilitar el ajuste MSS. Antes de que usted modifique el comando default en el ASA, entienda los riesgos implicados con respecto a la fragmentación potencial si el paquete se encapsula más a fondo en la trayectoria en alguna parte.

Para más información, refiera a la sección de los tcpmss de la conexión del sysopt de la *referencia de comandos de las 5500 Series de Cisco ASA*.

FAQ

Información Relacionada

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