Contenido

Pregunta:

¿Por qué vemos 502/504 errores GATEWAY_TIMEOUT al hojear a los determinados sitios?

Síntomas: Los usuarios están recibiendo 502 o 504 errores de tiempo de espera del gateway de Cisco WSA al hojear a ciertos sitios web

Los usuarios están recibiendo 502 o 504 errores de tiempo de espera del gateway al hojear a los sitios web. Los registros del acceso mostrarían 'NONE/504 o 'NONE/502

Línea del registro del acceso de la muestra:

1233658928.496 153185 10.10.70.50 **NONE/504** 1729 GET http://www.example.com/ - www.example.com DIRECTO - .....

Hay muchas razones por las que WSA puede volver un error de tiempo de espera de 502 o 504 gatewayes. Aunque estas respuestas de error sean similares, es importante entender las diferencias sutiles entre ellas.

Aquí están algunos ejemplos de los tipos de escenarios que puedan ocurrir:

- **502**: El WSA ha intentado establecer una conexión TCP con el servidor Web, pero no ha recibido un SYN/ACK.
- **504**: El WSA está recibiendo un Restablecimiento TCP (RST) que termina la conexión con el servidor Web.
- **504**: El WSA no está consiguiendo una respuesta de un servicio solicitado antes de la comunicación con el servidor Web, tal como DNS está fallando.
- **504**: El WSA ha establecido una conexión TCP con el servidor Web y ha enviado una petición get, pero el WSA nunca recibe el HTTP de respuesta.

Abajo están los ejemplos de cada escenario y de más detalles con respecto a los problemas potenciales:

502: El WSA ha intentado establecer una conexión TCP con el servidor Web, pero no ha recibido un SYN/ACK.
Si el servidor Web no responde a los paquetes SYN WSA, después de que una determinada cantidad de tentativas, el cliente sean enviadas un error de tiempo de espera de 502 gatewayes. Las causas típicas para esto son: **1.** El servidor Web o la red del servidor Web está teniendo problemas. **2.** Un problema de red en la red WSA está evitando que los paquetes SYN llegaran a Internet. **3.** Un Firewall o un dispositivo similar está cayendo los paquetes SYN WSA o el SYN/ACK del servidor Web

4. El IP spoofing se habilita en el WSA, pero no se configura correctamente (ningún cambio de dirección del trayecto de retorno)

Pasos de Troubleshooting:

El primer paso es verificar si puede el WSA ping de ICMP el servidor Web. Esto se puede hacer usando el comando CLI siguiente:

Ping www.example.com WSA>

Si el ping falla, no significa que el servidor está abajo. Puede significar que los paquetes icmp están consiguiendo bloqueados en alguna parte en la trayectoria. Si el ping tiene éxito, después podemos saber con seguridad que el WSA tiene un nivel básico layer3 de Conectividad al servidor Web.

Una prueba telnet verificará si el WSA tiene la capacidad de establecer una conexión TCP en el puerto 80 al servidor Web. Vea las instrucciones más lejos en este artículo para realizar una prueba telnet.

Bloque de los problemas de red o del Firewall

Si el ping es acertado, pero el telnet falla, hay una buena posibilidad que un dispositivo de filtrado, tal como un Firewall, está evitando que este tráfico consiguiera a través de la red. Se recomienda que analizan los registros y/o a las capturas de paquetes del Firewall del Firewall para otros detalles.

El IP spoofing habilita, pero configurado no correctamente

Si explícitamente el envío a través de proxy a través del WSA o de la prueba telnet es acertado, éste muestra que el WSA puede comunicar directamente al servidor Web, pero cuando los proxys de un cliente con el WSA con el IP spoofing, hay un problema.

Sin IP del cliente el spoofing:

- El WSA envía un SYN al servidor Web que usa su propia dirección IP como la fuente. Cuando se vuelve el paquete, va directamente al WSA.

Con IP del cliente el spoofing:

- El WSA envía el SYN, sino que por el contrario, utiliza el IP del cliente como la fuente. Sin una configuración de la red especial, el paquete de devolución será enviado al cliente en vez del WSA.
- Para utilizar IP del cliente el spoofing, la red se debe configurar de una manera muy específica para facilitar que los paquetes están reorientados correctamente. Si los paquetes del trayecto de retorno del servidor Web se están enviando al cliente en vez del WSA, el WSA nunca verá los servidores SYN/ACK y enviará un error de tiempo de espera de 502 gatewayes de nuevo al cliente.

504: El WSA está recibiendo un Restablecimiento TCP (RST) que termina la conexión con el servidor Web.

Si el WSA recibe un paquete del Restablecimiento TCP en su conexión ascendente al servidor Web, el WSA enviará un error de tiempo de espera de 504 gatewayes al cliente.

Las causas típicas para esto son:

1. El control de tráfico de la capa 4 de Cisco (L4TM) está bloqueando el proxy WSA de conectar al servidor Web.

2. El Firewall, el IDS, el IPS, o el otro dispositivo de la inspección de paquetes está bloqueando el WSA.

Pasos de Troubleshooting:
Primero determine si el TCP RST está viniendo del L4TM o de otro dispositivo.
Si el L4TM está bloqueando este tráfico, el tráfico aparecerá en los informes GUI bajo el "***monitor - > el control de tráfico L4***". Si no, el RST está viniendo de un diverso dispositivo.
Bloqueo L4TM:
Se recomienda que si el L4TM está bloqueando, no bloquee en los puertos que el proxy WSA también está ejecutando encendido. Hay razones múltiples de esto:
1. El proxy WSA proporciona un mensaje de error amigable en el caso del problema, en vez apenas del TCP que reajusta la conexión. Esto ayudará a la confusión del límite de los usuarios finales cuando se bloquean.
2. El proxy WSA tiene la capacidad de analizar y de bloquear el contenido del específico, mientras que el L4TM bloquea todo el tráfico que corresponde con una dirección IP puesta.
Para configurar el L4TM para no bloquear en los puertos del proxy, vaya al "***GUI - los servicios del > Security (Seguridad) - > el control de tráfico L4***".
Si el sitio es un mún sitio web conocido, pero hay razones por las que el tráfico debe ser permitido, el sitio puede ser mencionado blanco en:
"*GUI - > administrador de seguridad de la red - > control de tráfico L4 - > permita la lista*"

Bloqueo del Firewall/IDS /IP:
Si otro dispositivo en el establecimiento de una red está bloqueando el WSA de la conexión con el servidor Web, se recomienda para analizar el siguiente:
1. Registros del bloque del Firewall
2. Capturas del ingreso/del paquete de egreso durante el problema

Los registros del bloque pueden confirmar rápidamente si el dispositivo está bloqueando el WSA. A veces un Firewall, un IPS, o un IDS bloquearán el tráfico y no lo registrarán apropiadamente. Si éste es el caso, la única forma de probar de donde el TCP RST está viniendo, es obtener el ingreso y la salida captura del dispositivo. Si un RST se está enviando la interfaz de ingreso y ningunos paquetes viajaron a través del lado de la salida, el dispositivo de seguridad es definitivamente la causa.

504: El WSA ha establecido una conexión TCP con el servidor Web y ha enviado una petición get, pero el WSA nunca recibe el HTTP de respuesta.

Si el WSA envía un HTTP GET, pero nunca recibe una respuesta, enviará un error de tiempo de espera de 504 gateways al cliente.

Las causas típicas para esto son:

- El Firewall, el IDS, el IPS, o el otro dispositivo de la inspección de paquetes está permitiendo la conexión TCP, pero está bloqueando el contenido HTTP de alcanzar al servidor Web. En este caso, la prueba telnet puede ayudar a aislar que la clase de datos HTTP se está bloqueando.

Los registros del bloque del Firewall pueden confirmar rápidamente si/porqué el dispositivo está bloqueando el WSA. A veces un Firewall, un IPS, o un IDS bloquearán el tráfico y no lo registrarán apropiadamente. Si éste es el caso, la única forma de probar de donde el TCP RST está viniendo, es obtener el ingreso y la salida captura del dispositivo. Si un RST se está enviando la interfaz de ingreso y ningunos paquetes viajaron a través del lado de la salida, el dispositivo de seguridad es definitivamente la causa.

Conectividad de prueba con un servidor Web que usa el telnet
Del WSA CLI, funcione con el **comando telnet**: **Telnet** WSA> Seleccione por favor de que interconéctele quieren al telnet. 1. Auto 2. Administración (192.168.15.200/24: wsa.hostname.com) 3. P1 (192.168.113.199/24: data.com) [1]> **3** Ingrese el nombre de host remoto o el IP Address. []> **www.example.com** Ingrese el puerto remoto. [25]> **80** Intentando 10.3.2.99… Conectado con www.example.com. El carácter de escape es “^]”. Nota: El mensaje “conectado” en el rojo, indica que TCP establecido con éxito entre el WSA y el servidor Web. Un pedido de HTTP se puede enviar manualmente a través de esta sesión telnet también. Lo que sigue es una petición de la muestra que se puede teclear después del mensaje “conectado”: --- **GET http://www.example.com HTTP/1.1** **HOST: www.example.com** **{Ingrese}** --- Nota: Aseegurese agregar el retorno de carro adicional en el extremo, si no el servidor no responderá a la petición.