Problema de comprobación de estado del proxy upstream de WSA tras interrupción de red

Contenido

Problema

Después de una interrupción prolongada de la red, un dispositivo de seguridad Cisco Web Security Appliance (WSA) configurado para utilizar un proxy upstream especificado por FQDN puede no reanudar el reenvío de tráfico a un proxy upstream y enviar tráfico directamente en su lugar. Este problema se manifiesta cuando el WSA marca el proxy upstream como "muerto" durante la interrupción de la red, pero no reconoce cuándo el proxy upstream vuelve a estar disponible, incluso después de que se restaure la conectividad de red.

Los síntomas específicos observados incluyen:

- WSA configurado con proxy upstream a través de FQDN y "Gestión de fallos = continuar directamente"
- Interrupción de la red a largo plazo que afecta a la conectividad con el proxy upstream y el servidor DNS
- Después de la recuperación de la red, los registros de acceso no muestran etiquetas DEFAULT_PARENT, lo que indica que el tráfico continúa omitiendo el proxy ascendente
- Se produce un problema en un dispositivo WSA mientras que otro en el mismo entorno funciona normalmente

Entorno

- Dispositivo de seguridad Cisco Web Security Appliance (WSA) serie S
- AsyncOS 14.5.2-011 (versión afectada)
- Hardware S695

- Proxy upstream configurado con la especificación FQDN
- Gestión de fallos configurada como "Go Direct"
- Entorno de red con infraestructura de switch L2

Resolución

Este problema se resuelve actualizando AsyncOS a una versión que contiene la corrección para CSCwi13124. Este error se ha corregido en estas versiones de AsyncOS:

- AsyncOS 15.5.0-566
- AsyncOS 15.5.0-710

Solución temporal para las versiones actuales

Para los entornos que no se pueden actualizar inmediatamente, hay disponible una mitigación temporal ajustando el tiempo de espera inactivo máximo para verificar proxies upstream sin respuesta:

Paso 1: Acceda a la CLI y navegue hasta la configuración avanzada de proxy:

```
cli -> advancedproxyconfig -> MISCELLANEOUS
```

Paso 2: Modifique la configuración de tiempo de espera inactivo máximo:

```
"Enter maximum idle timeout for checking unresponsive upstream proxy (in seconds)"
```

Paso 3: Reduzca el valor máximo predeterminado (86400 segundos/24 horas) a un valor menor para reducir el tiempo entre comprobaciones de estado.

Método de recuperación inmediata

Si el problema está afectando actualmente el flujo de tráfico, el siguiente comando puede restaurar inmediatamente la funcionalidad del proxy upstream:

Paso 1: Acceda al menú de diagnóstico:

```
CLI > diagnostic > PROXY > kick
```

Esto reinicia el proceso proxy y restaura las operaciones normales del proxy upstream.

Validación y procedimiento de prueba

Para probar si el problema está presente o se ha resuelto después de una actualización, revise estos pasos:

Paso 1: Establecer supervisión básica

Supervise los registros de acceso y de proxy para confirmar que WSA está enviando tráfico al proxy upstream. Verifique que el tráfico esté llegando al lado del proxy upstream.

Paso 2: Simular interrupción de red

Después de confirmar el flujo de tráfico normal al proxy upstream, desconecte estas conexiones:

- WSA a conexión de proxy upstream
- Conexión de WSA a servidor DNS

Paso 3: Detección de fallos del monitor

Verifique los registros de proxy y los registros del sistema para estos indicadores:

- El registro de proxy puede mostrar el proxy upstream como "... declarado muerto"

- El registro del sistema puede mostrar "Crítico: Fallos máximos alcanzados al consultar el servidor DNS..."

Paso 4: Mantener estado interrumpido

Sin reiniciar el proceso proxy, mantenga el estado desconectado del Paso 2 y continúe generando solicitudes durante aproximadamente 10 horas.

Paso 5: Restaure la conectividad

Después de aproximadamente 10 horas, restaure las conexiones que se desconectaron en el paso 2.

Paso 6: Supervisar el comportamiento de recuperación

Después de completar el Paso 5, monitoree los logs de acceso y los logs de proxy sin reiniciar el proceso de proxy:

- En un sistema fijo: El tráfico se reanuda a través del proxy upstream y los registros de proxy muestran transiciones de estado normales
- En un sistema afectado: Los registros de acceso muestran que el tráfico continúa omitiendo el proxy upstream, y los registros de proxy no mostrarán los mensajes "... was sick, now heald" o "... was healtho, now sick"

Causa

La causa raíz de este problema es una falla lógica en el mecanismo de verificación de estado del proxy upstream. Cuando WSA determina que un proxy upstream configurado está "muerto" (sin respuesta), implementa un algoritmo de backoff exponencial que duplica el intervalo de comprobación de estado después de cada fallo. Este intervalo puede alcanzar un máximo de 24 horas (86400 segundos).

Este problema ocurre cuando el proxy upstream vuelve a estar disponible durante uno de estos intervalos extendidos. Aunque el proxy se ha recuperado y responde con normalidad, WSA no realizará una comprobación de estado hasta que haya transcurrido el intervalo de tiempo completo configurado. Esto puede dar lugar a hasta 24 horas de routing de tráfico directo continuo en lugar de reanudar el uso de proxy upstream.

Este comportamiento afecta a las configuraciones WSA en las que:

- El proxy upstream lo especifica el nombre de host DNS/FQDN (no la dirección IP)
- La gestión de fallos se establece en "Directa"
- Las interrupciones de red extendidas afectan a la conectividad del proxy upstream y del servidor DNS

ID de falla de funcionamiento de Cisco: CSCwi13124

Contenido relacionado

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).