Configuración de puertos proxy para tráfico de puertos no estándar en WSA 1000V

Contenido

Problema

Un proxy WSA 1000V alojado en VMware estaba procesando correctamente el tráfico del cliente en los puertos 80 y 443, pero no el tráfico en puertos no estándar, como el 890. Cuando el acceso a un destino que utiliza un puerto no estándar se bloqueó inicialmente mediante una directiva, el WSA registró correctamente la solicitud bloqueada. Sin embargo, después de agregar la dirección IP y la URL a una política de permisos, el tráfico seguía fallando y no se generaban los registros correspondientes en el proxy. Este comportamiento sugería que el tráfico no estaba llegando al WSA o no estaba siendo procesado por este después de que se creara la política de permiso, lo que afectaba al acceso del cliente a las aplicaciones que utilizan puertos no estándar.

Entorno

- Proxy de Cisco WSA 1000V alojado en VMware
- Versión del software 15.0.0
- El tráfico en los puertos 80 y 443 se procesa normalmente.
- El tráfico de puerto no estándar (por ejemplo, el puerto 8890) no está siendo procesado por el proxy.
- Permitir políticas configuradas para destinos afectados.

Resolución

El problema se resolvió configurando WSA para admitir puertos no estándar en la configuración del perfil de identificación. Era necesario actualizar la configuración de los puertos proxy para

incluir los números de puerto no estándar requeridos.

Configuration Steps

Paso 1: Acceda a la interfaz de Web Security Manager.

Paso 2: Vaya a la configuración Identification Profiles.

Vaya a Administrador de seguridad web > Perfiles de identificación.

Paso 3: Seleccione el perfil de identificación deseado que requiere compatibilidad con puertos no estándar.

Paso 4: Expanda las opciones de configuración avanzada.

En la página Perfil de identificación, expanda la pestaña Avanzado.

Paso 5: Configure el parámetro Puertos de Proxy.

Seleccione el link junto a Puertos Proxy para acceder a la configuración del puerto.

Paso 6: Agregue los números de puerto no estándar requeridos.

Agregue los números de puerto específicos que los clientes utilizan para las conexiones de puerto no estándar (por ejemplo, 8890).

Paso 7: Guarde y confirme los cambios de configuración.

Después de implementar estos cambios de configuración, el WSA puede procesar e inspeccionar el tráfico en los puertos no estándar especificados, lo que permite que el proxy gestione correctamente las conexiones del cliente y aplique políticas al tráfico que utiliza estos puertos.

Causa

El WSA 1000V se configuró con parámetros de puerto de proxy predeterminados que solo incluían puertos estándar HTTP (puerto 80) y HTTPS (puerto 443). La configuración de los puertos proxy del perfil de identificación no incluía los puertos no estándar requeridos por las aplicaciones cliente. Sin la configuración explícita de estos puertos en los parámetros avanzados del perfil de identificación, WSA no pudo interceptar, procesar ni aplicar políticas al tráfico mediante puertos no estándar, incluso cuando se configuraron políticas de permiso para los destinos.

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).