Verificación de la Función Bypass Behavior para Acceso Seguro Compatibilidad con Microsoft 365

Contenido

Problema

Al configurar Cisco Secure Access con la función de compatibilidad de Microsoft 365 habilitada, existe incertidumbre sobre si los nombres de dominio completamente cualificados (FQDN) específicos relacionados con Microsoft se omiten automáticamente del procesamiento de gateway web seguro (SWG) y el descifrado de TLS. Específicamente, se necesita una aclaración con respecto al comportamiento de omisión para estos dominios:

- do.dsp.mp.microsoft.com
- dl.delivery.mp.microsoft.com
- manage.microsoft.com

La principal preocupación gira en torno a si estos dominios requieren una adición manual a la lista de no descifrado o si se excluyen automáticamente cuando se habilita la compatibilidad con Microsoft 365. Además, existe confusión sobre la interacción entre los desvíos de nivel SWG y la configuración de descifrado de nivel IPS, especialmente para manage.microsoft.com, que aparece en la documentación que sugiere que la configuración manual de la lista Do Not Decrypt todavía puede ser necesaria.

Entorno

- Acceso seguro de Cisco
- Función de compatibilidad de Microsoft 365 habilitada
- Inspección de gateway web seguro (SWG) y descifrado de TLS configurado
- Políticas de descifrado IPS en uso
- Servicios de gestión y actualización de Microsoft que requieren conectividad

Resolución

El comportamiento de la característica de compatibilidad de Microsoft 365 se verificó mediante pruebas de laboratorio con los siguientes hallazgos:

Ámbito de la función de compatibilidad de Microsoft 365

La función de compatibilidad de Microsoft 365 exime de la inspección SWG y la aplicación de políticas a los dominios relacionados con Microsoft 365 marcados como "Optimizar" y "Permitir" en las categorías de terminales de Microsoft. Esto permite que el tráfico a esos dominios pase sin alteraciones en la capa SWG.

Resultados de pruebas de laboratorio

Las pruebas se llevaron a cabo en un entorno de laboratorio controlado con la compatibilidad de Microsoft 365 habilitada. Este comportamiento se observó para los FQDN especificados:

Paso 1: Habilitar característica de compatibilidad de Microsoft 365

La función de compatibilidad de Microsoft 365 se activó en la configuración de Secure Access.

Paso 2: Tráfico de prueba para FQDN de destino

El tráfico web se generó para cada uno de los tres FQDN mediante un navegador de Internet estándar:

- do.dsp.mp.microsoft.com
- dl.delivery.mp.microsoft.com
- manage.microsoft.com

Paso 3: Comprobar el comportamiento de omisión en el panel

El análisis del panel de acceso seguro confirmó que no se estaban llevando a cabo la inspección y el descifrado del tráfico web para el tráfico a estos destinos específicos cuando se habilitó la función de compatibilidad de Microsoft 365.

Paso 4: Confirmar comportamiento de dirección DNS

El tráfico DNS a estos destinos continuó dirigiéndose a través de Secure Access, que se alinea con el comportamiento documentado a menos que se configure una exención de DNS específica.

Conclusiones clave sobre el comportamiento

Basado en los resultados de las pruebas y el análisis de la documentación:

- Omisión SWG: Los tres FQDN especificados se omiten de la inspección de tráfico web cuando se habilita la compatibilidad con Microsoft 365.
- Descifrado TLS: El descifrado se omite en la capa SWG para estos dominios.
- Dirección DNS: Las consultas DNS se siguen procesando a través de Secure Access a menos que se eximan explícitamente.
- Cobertura de dominio: Mientras que "*.microsoft.com" como un dominio completo no es totalmente eludido por la especificación, las URL específicas probadas se omiten en la práctica.

Consideraciones sobre la capa IPS

La función de compatibilidad de Microsoft 365 funciona en la capa SWG. Para la omisión del descifrado a nivel de IPS, todavía puede ser necesaria la configuración manual:

- Si también se desea omitir el descifrado IPS para estos dominios, puede ser necesario agregar manualmente la lista No descifrar.
- La lista No descifrar afecta principalmente al descifrado del lado IPS en lugar del procesamiento SWG.
- Esto explica por qué la documentación puede hacer referencia a la adición de manage.microsoft.com a la lista No descifrar incluso cuando la compatibilidad con Microsoft 365 está habilitada.

Causa

La confusión surge de la arquitectura por capas de Cisco Secure Access, donde la compatibilidad de Microsoft 365 afecta al procesamiento de nivel SWG, mientras que el descifrado IPS funciona como una capa independiente con sus propios requisitos de configuración. La función de compatibilidad de Microsoft 365 gestiona automáticamente la omisión de SWG para los dominios de Microsoft calificados, pero las políticas de descifrado IPS pueden requerir una configuración independiente a través de la lista de no descifrado.

Contenido relacionado

- Documentación de compatibilidad de Cisco Secure Access con Microsoft 365
- Crear una lista efectiva de no descifrado para Cisco Secure Access
- 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).