

Especificaciones de comportamiento y configuración de postura ZTA basada en cliente de Secure Access

Contenido

Problema

Se han planteado preguntas sobre el comportamiento específico y las capacidades de configuración de la funcionalidad de estado de acceso de confianza cero (ZTA) basada en cliente de Cisco Secure Access cuando se utiliza para el acceso a Internet. Las preocupaciones específicas incluían:

- Si los requisitos de estado del sistema operativo admiten un período de gracia configurable de hasta 365 días durante el cual los dispositivos pueden seguir utilizando el módulo ZTA para acceder a destinos de Internet aunque no cumplan la versión de SO necesaria.
- Si los requisitos de estado distintos de los del sistema operativo, como firewall o contraseña del sistema, entre otros, provocan un bloqueo inmediato del acceso de destino cuando no se cumplen.
- Si los mensajes de advertencia personalizados o las acciones distintas del bloqueo (como la supervisión) se pueden configurar para los fallos de requisitos de estado a través de la interfaz GUI de Secure Access.

Entorno

- Funcionalidad de Cisco Secure Access con acceso de confianza cero (ZTNA)
- Implementación de estado ZTA basada en el cliente
- Caso práctico de acceso a Internet
- Requisitos de estado, incluidas las condiciones de sistema operativo, firewall y contraseña del sistema

Resolución

Las aclaraciones descritas en las siguientes secciones se proporcionaron con respecto al comportamiento de estado ZTA basado en el cliente Secure Access y las capacidades de configuración.

Período de gracia de estado del sistema operativo

El comportamiento de los requisitos de estado del sistema operativo descrito es correcto. Cuando se configura una condición de estado del sistema operativo, admite un período de gracia configurable de hasta 365 días. Durante este período de gracia, los dispositivos que no cumplan con la versión de SO requerida pueden seguir utilizando el módulo ZTA para acceder a destinos de Internet mientras actualizan a la versión de destino.

Requisitos de estado del sistema no operativo

Para las condiciones de estado distintas del sistema operativo (como firewall, contraseña del sistema y otros controles de seguridad), el acceso a los destinos se bloquea inmediatamente cuando no se cumplen estos requisitos. Estos tipos de estado no admiten la funcionalidad de período de gracia disponible para los requisitos del sistema operativo.

Acciones de error de estado y mensajes personalizados

Las acciones para los fallos de requisitos de estado se controlan a través de la configuración de la política de acceso.

La política de acceso admite varios tipos de acción, entre los que se incluyen:

- Permiso
- Bloqueo
- Avisar

- Aislar

Los mensajes de advertencia personalizados y las páginas de notificación para los fallos de estado se pueden configurar mediante la configuración del perfil de seguridad de la directiva de acceso. La administración de la página de notificación y advertencia se gestiona a través de la interfaz de configuración y documentación de Administrar páginas de notificación.

Esto significa que las acciones que no sean bloqueos (como la supervisión a través de la acción de advertencia) están disponibles y se pueden configurar, contrariamente a la evaluación inicial de que solo eran posibles las acciones de bloqueo.

Causa

Las preguntas surgieron de la necesidad de comprender las diferencias de comportamiento específicas entre los requisitos de estado del sistema operativo y otros tipos de estado, así como de aclarar las opciones de configuración disponibles para la gestión de fallos de estado que no se pueden ver inmediatamente en la interfaz GUI de Secure Access.

Contenido relacionado

- Documentación de Administrar páginas de notificación para 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).