

Umbrella Proxy bloquea la conectividad de aplicaciones Ninja

Contenido

Problema

Los usuarios no pueden ejecutar un sistema remoto con un archivo de instalación descargado cuando se conectan a través de Cisco Umbrella. La aplicación no funciona con la protección Umbrella, lo que afecta específicamente al acceso al sistema remoto. El mismo sistema remoto funciona perfectamente sin problemas cuando el proxy de Cisco Umbrella está desactivado.

Los intentos de resolución de problemas incluyeron pruebas con una política independiente en la que la seguridad del sistema y el destino estaban establecidos en ANY, pero el problema persistió. Además, se intentó enrutar el tráfico a través del acceso de confianza cero (ZTA), pero el problema no se modificó. Se permitía el tráfico a través de Secure Access en TCP/443, pero las conexiones seguían bloqueadas en el terminal.

Entorno

- Cisco Umbrella con funcionalidad de proxy habilitada
- Configuración de acceso de confianza cero (ZTA)
- Políticas de acceso seguro configuradas para el tráfico TCP/443

Resolución

La resolución implica la exclusión de dominios específicos relacionados con NinjaOne del proxy Umbrella para permitir la conectividad directa para la aplicación de acceso remoto.

Paso 1: Identificar dominios afectados

El análisis de la captura de paquetes y los archivos HAR revela que estos dominios relacionados con NinjaOne se ven afectados por el proxy Umbrella:

- ninjarmm.net
- ninjarmm.com
- app.ninjarmm.com
- ninjaone.com
- agent-app.ninjaone.com

Paso 2: Configurar excepciones de dominio

Excluya los dominios identificados de las políticas de seguridad de Internet de gateway web seguro (SWG) y del direccionamiento del tráfico de Internet ZTA. Este cambio de configuración permite que estos dominios omitan el proxy de Umbrella y establezcan conexiones directas.



Nota: Se ha observado que la configuración de la lista No descifrar (NoMlsta) no es eficaz para resolver este problema. El enfoque recomendado es el direccionamiento y la exención del tráfico.

Paso 3: Aplicar cambios de configuración

Implemente las exenciones de dominio en la configuración de Umbrella para excluir el tráfico relacionado con NinjaOne del procesamiento de proxy. Esto permite a la aplicación de acceso remoto establecer conexiones directas con los servicios requeridos.

Paso 4: Validar resolución

Pruebe la funcionalidad de la aplicación de acceso remoto después de aplicar las exenciones para garantizar que se restaura la conectividad adecuada mientras se mantiene la protección de Umbrella para otro tráfico.

Causa

El problema ocurre porque las aplicaciones de acceso remoto NinjaOne rechazan las conexiones con proxy cuando el tráfico se enruta a través del proxy de Cisco Umbrella. La aplicación requiere conectividad directa a dominios NinjaOne específicos para funcionar correctamente. Cuando estas conexiones se procesan a través de Umbrella, el servicio de acceso remoto no puede establecer los canales de comunicación necesarios, lo que provoca un error en la aplicación incluso cuando las políticas de seguridad están configuradas para permitir el tráfico.

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).