Cisco Secure Access Fragmented ICMP Packet Handling

Contenido

Problema

Las solicitudes de eco ICMP mayores que la MTU no reciben respuestas cuando se envían con el bit DF (no fragmentar) deshabilitado. Este comportamiento se produce en dos escenarios específicos:

- Desde los puntos finales de VPN a través de la interfaz VPN cuando se envían paquetes ICMP que exceden el tamaño de MTU de la interfaz VPN con el bit DF borrado
- Desde terminales en las instalaciones a través de un túnel IPsec entre un router de sitio y Cisco Secure Access (CSA) al enviar paquetes ICMP que exceden el tamaño de MTU de la interfaz de túnel IPsec con el bit DF borrado

En ambos casos, no se reciben respuestas ICMP, lo que lleva a preguntas sobre si CSA descarta paquetes fragmentados con el bit DF deshabilitado.

Entorno

- Cisco Secure Access (CSA)
- Terminales RAVPN (VPN de acceso remoto)
- Túneles IPsec entre routers de sitio y CSA
- Tráfico ICMP que excede los tamaños de MTU de interfaz
- Escenarios de paquetes fragmentados con bit DF borrado

Resolución

Cisco Secure Access descarta paquetes fragmentados en escenarios de superposición y

subyacentes. Este comportamiento se documenta en la documentación de ayuda de Cisco Secure Access, que establece explícitamente: "Los paquetes fragmentados en la capa subyacente o superpuesta se descartan".

Comportamiento esperado

Cisco Secure Access está diseñado para descartar paquetes fragmentados independientemente de si se producen en la red subyacente o superpuesta. Esto se aplica a:

- Paquetes ICMP enviados desde extremos RAVPN que exceden la MTU de la interfaz VPN con bit DF borrado
- Paquetes ICMP enviados desde terminales en las instalaciones a través de túneles IPsec que exceden la MTU de la interfaz de túnel con bit DF borrado

Este comportamiento es uniforme en todos los escenarios que implican paquetes fragmentados dentro de la infraestructura de Cisco Secure Access.

La solicitud de característica CSE-I-5739 ha sido creada para esto.

Causa

Cisco Secure Access está diseñado para descartar paquetes fragmentados como una decisión de diseño de seguridad y rendimiento. Este comportamiento se implementa para evitar posibles vulnerabilidades de seguridad y sobrecarga de procesamiento asociadas con el reensamblado de paquetes en escenarios de red subyacentes y superpuestos.

Contenido relacionado

- Documentación de ayuda de Cisco Secure Access - Gestión de paquetes fragmentada
- 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).