



Secure Connect Gateway 5.x: Edición virtual Guía de implementación

Requisitos de red

En esta sección, se enumeran los requisitos mínimos de red, los requisitos de puertos y los detalles de traducción de direcciones IP para el sistema local.

i NOTA: Para obtener información sobre los puertos necesarios, consulte la *matriz de soporte de Secure Connect Gateway 5.x: versión virtual* disponible en la página de [documentación del Secure Connect Gateway: edición virtual](#).

- La traducción de direcciones de red (NAT) solo es compatible entre el secure connect gateway y Dell Technologies. NAT **no es compatible** entre el secure connect gateway y los dispositivos administrados.
- La traducción de direcciones de puerto (PAT) no es compatible con las direcciones IP de ninguno de los dispositivos administrados por el secure connect gateway.
- Las direcciones IP dinámicas (DHCP) no se deben utilizar para ningún componente de los servidores del secure connect gateway, los servidores del administrador de políticas ni los dispositivos administrados.
- Se requiere conexión a Internet: red estándar de 1 GbE o más rápida mediante HTTP con autenticación básica.
- El sistema local debe poder conectarse a los siguientes servidores **Enterprise** a través de los puertos 443 y 8443:
 - Para IPV6
 - srs-1-v6.dell.com
 - Para IPV4
 - esrs3-core.emc.com
 - esrs3-core.dr.emc.com
- El sistema local debe poder conectarse a los siguientes servidores de **Global access** a través de los puertos 443 y 8443:
 - Para IPV6
 - SRSgduprd01-v6.dell.com
 - SRSgduprd02-v6.dell.com
 - SRSgduprd03-v6.dell.com
 - SRSgduprd04-v6.dell.com
 - SRSgduprd05-v6.dell.com
 - SRSgduprd06-v6.dell.com
 - SRSghopr01-v6.dell.com
 - SRSghopr02-v6.dell.com
 - SRSghopr03-v6.dell.com
 - SRSghopr04-v6.dell.com
 - SRSghopr05-v6.dell.com
 - SRSghopr06-v6.dell.com
 - Para IPV4
 - esr3gduprd01.emc.com
 - esr3gduprd02.emc.com
 - esr3gduprd03.emc.com
 - esr3gduprd04.emc.com
 - esr3gduprd05.emc.com
 - esr3gduprd06.emc.com
 - esr3ghopr01.emc.com
 - esr3ghopr02.emc.com
 - esr3ghopr03.emc.com
 - esr3ghopr04.emc.com
 - esr3ghopr05.emc.com
 - esr3ghopr06.emc.com
 - esr3gscprd01.emc.com
 - esr3gscprd02.emc.com
 - esr3gscprd03.emc.com
 - esr3gscprd04.emc.com
 - esr3gscprd05.emc.com

- esr3gscprd06.emc.com
- esr3gckprd01.emc.com
- esr3gckprd02.emc.com
- esr3gckprd03.emc.com
- esr3gckprd04.emc.com
- esr3gckprd05.emc.com
- esr3gckprd06.emc.com
- esr3gckprd07.emc.com
- esr3gckprd08.emc.com
- esr3gckprd09.emc.com
- esr3gckprd10.emc.com
- esr3gckprd11.emc.com
- esr3gckprd12.emc.com
- esr3gspprd01.emc.com
- esr3gspprd02.emc.com
- esr3gspprd03.emc.com
- esr3gspprd04.emc.com
- esr3gspprd05.emc.com
- esr3gspprd06.emc.com
- Configure al menos un servidor DNS.
- Use solo una dirección IP estática para el sistema local. Las direcciones IP dinámicas no son compatibles. No puede cambiar la dirección IP después de la implementación.
- Para garantizar la integridad y la seguridad de la comunicación, los dispositivos de red no deben llevar a cabo ningún método de descifrado SSL en el tráfico para el back-end. Si se intenta hacerlo, se perderá la conectividad con el back-end.

i NOTA: Si el descifrado SSL está habilitado en los servidores proxy y en otros dispositivos, asegúrese de que los servidores **Global access** y **Enterprise** se agreguen a la lista de exclusión de descifrado SSL en los servidores proxy y los dispositivos.

En la siguiente tabla, se enumeran los puertos que deben estar abiertos en el sistema local:

Tabla 1. Puertos de red para el sistema local

PUERTO	PROTOCOLO	DIRECCIÓN	USO
443*	HTTPS	Saliente del sistema local a Dell	Es compatible con la comunicación desde el secure connect gateway a Dell. Se requiere para el registro del secure connect gateway, las alertas de productos y el soporte remoto.
990	FTPS	Saliente del sistema local a Dell	Se utiliza para la conmutación por error de alertas si el canal de transferencia de archivos 443 no está disponible.
8443*	MQTT sobre TLS	Saliente del sistema local a Dell	Se utiliza para el soporte remoto, la pub/sub y la sincronización del inventario.
25	SMTP (con STARTTLS opcional)	Saliente del sistema local al servidor SMTP del cliente	Se utiliza cuando configura un servidor SMTP para enviar mensajes de correo electrónico.
8443 u 8888	HTTPS y HTTP	Saliente del sistema local al administrador de políticas	Utilice 8443 si el administrador de políticas tiene cifrado SSL. Utilice 8888 si el administrador de políticas no tiene puerto de cifrado SSL.
5700*	HTTPS	Entrante desde el navegador del cliente a la interfaz de usuario web de SCG	Se utiliza para acceder a la interfaz de usuario localmente.

*Requerido: este puerto debe estar abierto en el sistema local.

i NOTA: Para mantener una conexión TLS segura, no debe modificar ni cambiar los certificados de los puertos 443 u 8443 que se comunican desde el secure connect gateway con Dell.

i AVISO: Este contenido se ha traducido mediante inteligencia artificial (IA). Puede contener errores y se proporciona “tal cual” sin garantía de ningún tipo. Para ver el contenido original (sin traducir), consulte la versión en inglés. Si tiene preguntas o dudas sobre este contenido, póngase en contacto con Dell en Dell.Translation.Feedback@dell.com.