

La serie SonicWALL® SuperMassive™ E10000 es la nueva plataforma de cortafuegos de SonicWALL de próxima generación desarrollada para ofrecer a las redes grandes escalabilidad, fiabilidad y el más alto nivel de seguridad a velocidades multi-gigabit. La serie SuperMassive E10000 es ideal para proteger las redes corporativas, los centros de datos y las granjas de servidores en entornos corporativos, gubernamentales, universitarios y en implementaciones de proveedores de servicios. Al combinar su arquitectura multinúcleo masiva con la tecnología patentada* SonicWALL Reassembly-Free Deep Packet Inspection™ (RFDPI), la serie SuperMassive E10000 ofrece las prestaciones más avanzadas del mercado en materia de control de aplicaciones, prevención de intrusiones, protección de malware e inspección SSL a velocidades multi-gigabit. Los ingenieros de la nueva serie E10000 se han centrado sobre todo en el rendimiento, el espacio y la refrigeración, logrando el mejor valor de Gbps/Vatio de la industria para las funciones de control de aplicaciones y prevención de intrusiones.

El motor de inspección profunda de paquetes sin reensamblado de SonicWALL escanea hasta el último byte de cada paquete, garantizando no solo una inspección completa del flujo de datos entero sino también un alto rendimiento y una latencia mínima. Esta tecnología es superior a los diseños proxy anticuados que reensamblan el contenido utilizando sockets ligados a programas anti-malware que presentan notables ineficiencias y una hiperpaginación excesiva de la memoria del socket, lo cual provoca una elevada latencia, un bajo rendimiento y limitaciones en el tamaño de los archivos. El motor RFDPI inspecciona por completo el contenido para eliminar las amenazas antes de que accedan a la red. De esta forma proporciona protección contra millones de variantes de malware sin limitación alguna del tamaño de archivo, del rendimiento o de la latencia. El motor RFDPI ofrece también inspección completa del tráfico cifrado mediante SSL y de las aplicaciones que no pasan por el proxy, garantizando una protección integral, independiente de la vía de transporte o del protocolo.

El análisis del tráfico de aplicaciones permite identificar en tiempo real el tráfico de aplicaciones productivo y no productivo y controlarlo mediante potentes políticas a nivel de aplicaciones. El control de las aplicaciones puede realizarse según usuarios individuales o según grupos y puede combinarse con funciones de planificación y listas de excepciones. Las definiciones de aplicaciones, de prevención de intrusión y de malware son constantemente actualizadas por el equipo de investigación de SonicWALL. Además, el avanzado sistema operativo de SonicWALL, SonicOS, proporciona herramientas integradas que permiten personalizar el método de identificación de las aplicaciones.

La arquitectura de la serie E10000 permite un aumento del rendimiento prácticamente lineal y una ampliación hasta 96 núcleos de procesamiento, ofreciendo un rendimiento de más de 40 Gbps en el cortafuegos, de más de 30 Gbps en la inspección de aplicaciones, de más de 30 Gbps en la prevención de intrusiones y de más de 10 Gbps en la protección antimalware. La serie SonicWALL SuperMassive E10000, compuesta por los modelos E10100, E10200, E10400 y E10800, puede ampliarse in situ y protege la inversión en infraestructura de seguridad adaptándose a las crecientes exigencias de ancho de banda y seguridad de la red.

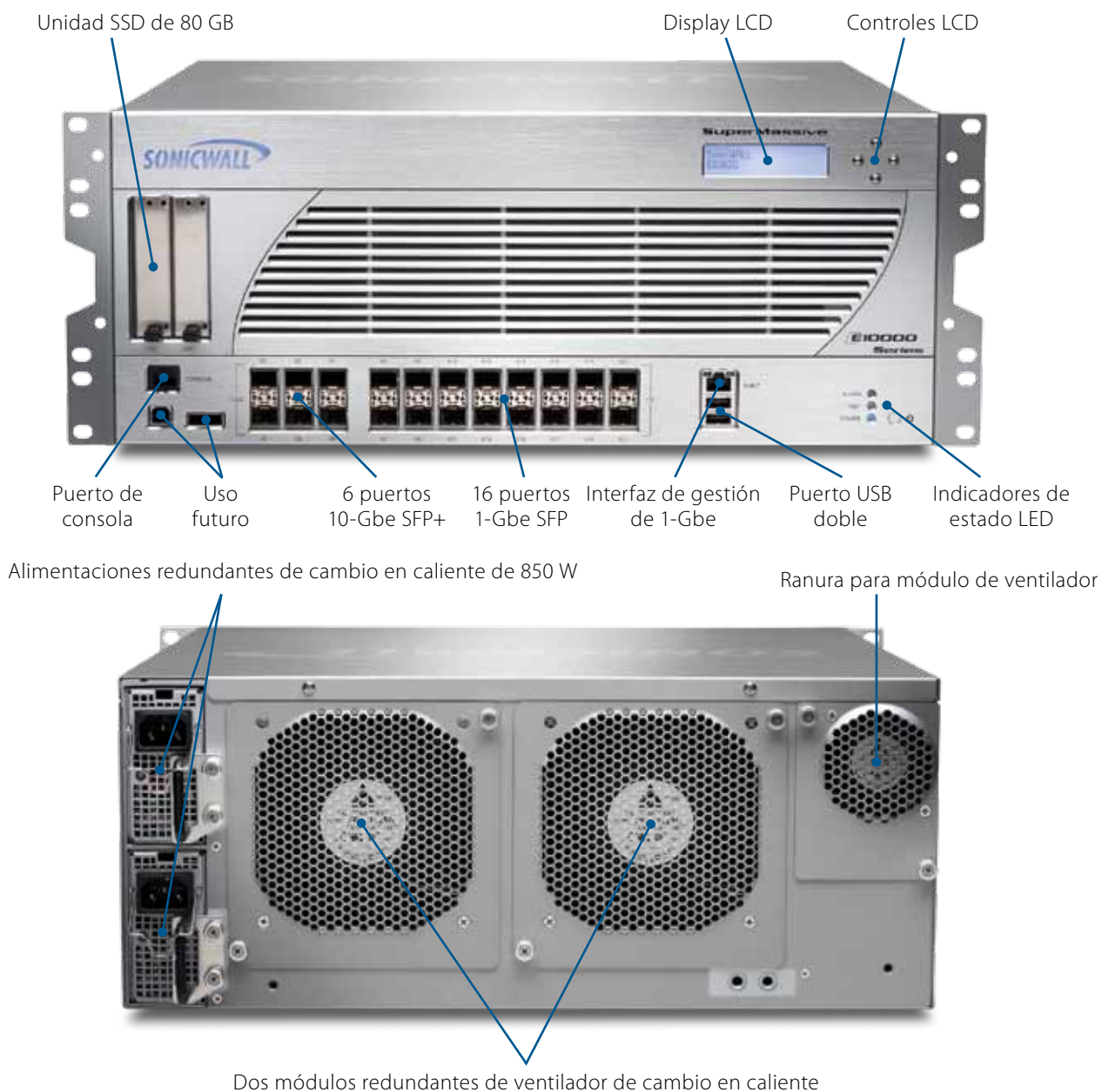
* Patentes en EE UU 7,310,815; 7,600,257; 7,738,380; 7,835,361

- **Arquitectura multinúcleo masivamente escalable, diseñada para infraestructuras de 10/40 Gbps**
- **Prestaciones granulares de Inteligencia, control y visualización de aplicaciones**
- **Protección completa contra amenazas con prevención de intrusiones de alto rendimiento y protección contra malware de baja latencia**
- **Inspección completa del tráfico cifrado mediante SSL sin sobrecarga, latencia o hiperpaginación de memoria relacionada con proxies SSL basados en sockets**

VISIÓN DE CONJUNTO DE LA SERIE

La carcasa de SonicWALL SuperMassive incluye 6 puertos 10-Gbe SFP+ y 16 puertos 1 GbE SFP, dos alimentaciones CA de 850 W y un módulo doble redundante de ventiladores de cambio en caliente. Puede escalarse de forma masiva hasta 96 núcleos de procesamiento.

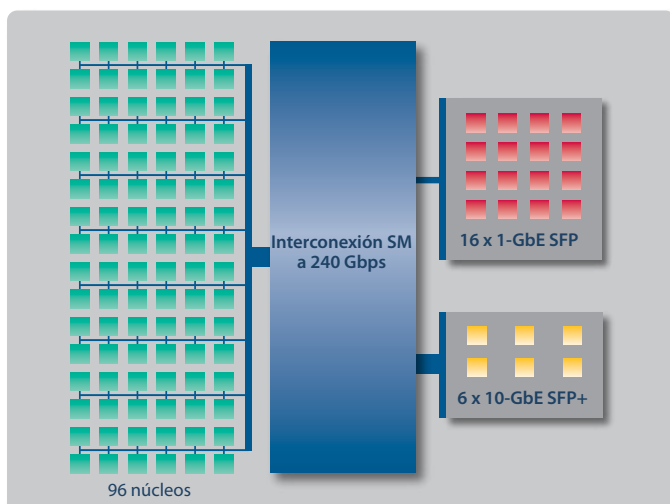
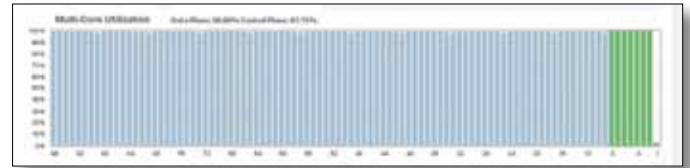
Datos técnicos	E10100	E10200	E10400	E10800
Núcleos de procesamiento	12 (+12 en modo de alta disponibilidad integrado)	24	48	96
Rendimiento del cortafuegos	5,0 Gbps	10 Gbps	20 Gbps	40 Gbps
Rendimiento de inteligencia de aplicaciones	4,0 Gbps	7,5 Gbps	15 Gbps	30 Gbps
Rendimiento IPS	4,0 Gbps	7,5 Gbps	15 Gbps	30 Gbps
Rendimiento antimalware	2,0 Gbps	3,0 Gbps	6,0 Gbps	12 Gbps
Conexiones máximas	1,5 millones	3,0 millones	6,0 millones	12,0 millones
Opciones de ampliación	Ampliable a E10200	Ampliable a E10400	Ampliable a E10800	—



ARQUITECTURA AMPLIABLE PARA MÁXIMO RENDIMIENTO Y ESCALABILIDAD

Rendimiento escalable con arquitectura multinúcleo

Al diseñar la serie SonicWALL SuperMassive E10000, los ingenieros se han centrado en el rendimiento, la escalabilidad y la disponibilidad para proporcionar a las empresas grandes una plataforma capaz de cumplir los más exigentes requerimientos de seguridad. Esta combinación de escalabilidad y rendimiento se basa en la potente arquitectura multinúcleo, masivamente escalable, y en el motor de inspección profunda de paquetes sin reensamblado desarrollado por SonicWALL, capaz de adaptarse de forma lineal a cualquier número de núcleos de procesamiento. Las empresas con requerimientos de seguridad de red crecientes pueden ampliar su sistema para incrementar el rendimiento disponible de su plataforma SuperMassive.



Concebida para el más alto rendimiento

La serie SuperMassive E10000 ha sido diseñada para ofrecer la tecnología de inspección profunda de paquetes de baja latencia que las empresas grandes necesitan. El sistema de interconexión ofrece un ancho de banda sin bloqueo de 240 Gbps con una latencia inferior a 1 μ s para garantizar una comunicación sin obstáculos entre los 96 núcleos de procesamiento, los 6 puertos 10-GbE SFP+ y los 16 puertos 1-GbE SFP.

Diseño inteligente para un rendimiento DPI superior

Aunque la inspección dinámica de paquetes sigue siendo necesaria, no es suficiente para proteger las redes contra las amenazas actuales, basadas en las aplicaciones y en el contenido. Las prestaciones de inspección profunda de paquetes como el control de aplicaciones, la prevención de intrusiones y el antimalware ofrecen un nivel de seguridad y control de red muy superior, pero no deben frenar el rendimiento de la red.

El motor RFDPI patentado* de SonicWALL ofrece una arquitectura single-pass altamente eficiente que consolida todas las prestaciones de seguridad en un motor unificado de escaneo y control de políticas y proporciona el mejor rendimiento de la industria en la inspección profunda de paquetes.

* Patentes en EE UU 7,310,815; 7,600,257; 7,738,380; 7,835,361



PRESTACIONES

Inteligencia y control de aplicaciones

Prestación	Descripción
Control de aplicaciones	Identificación y control de aplicaciones o de componentes individuales de aplicaciones mediante la tecnología RFDPI y no mediante el control de puertos y protocolos conocidos.
Gestión del ancho de banda de las aplicaciones	Asignación de ancho de banda a aplicaciones críticas y limitación del tráfico de aplicaciones poco productivas, para garantizar una red eficiente y productiva.
Identificación personalizada de aplicaciones	Creación y configuración de criterios personalizados para la identificación de aplicaciones según parámetros de tráfico o patrones de comunicación de red inequívocos para cada aplicación.
Análisis del tráfico de aplicaciones	Ofrece a las organizaciones una visión granular del tráfico de aplicaciones, del uso del ancho de banda y de las amenazas de seguridad así como potentes prestaciones de análisis forense y resolución de problemas.
Base de datos de definiciones de aplicaciones	Una base de datos de más de 3.500 definiciones de aplicaciones, en continua expansión, permite a los administradores controlar el uso de las más recientes aplicaciones, ya sea por categorías o a nivel individual.
Informes IPFIX/Netflow	Permite exportar los datos de uso de aplicaciones a través de protocolos IPFIX o Netflow para que puedan supervisarse en SonicWALL Scrutinizer o en cualquier herramienta de monitoreo e informes de un tercer proveedor. Los datos similares pueden exportarse a través de syslog a SonicWALL GMS y SonicWALL Analyzer.
Inspección profunda de paquetes para SSL	Esta función descifra el tráfico SSL, lo escanea en busca de malware e intrusiones mediante el motor de inspección profunda de paquetes sin reensamblado y aplica políticas de control de aplicaciones, URL y contenido al tráfico propicio a utilizar técnicas evasivas.
Seguimiento de la actividad de los usuarios	La identificación de los usuarios se encuentra integrada de forma transparente con Microsoft® Active Directory y otros sistemas de autenticación. Esto permite seguir la identificación individual de los usuarios y generar informes al respecto.
GeolP – Identificación del tráfico en base al país	Identificación y control del tráfico de red a países determinados o procedente de los mismos.

Prevención de amenazas en la pasarela

Antimalware en pasarela	El motor RFDPI propietario de SonicWALL escanea todos los puertos y protocolos en busca de virus, sin limitar el tamaño de archivo o la magnitud del flujo de datos. Los técnicos investigadores de SonicLabs proporcionan constantemente una protección actualizada contra las amenazas, garantizando tiempos de respuesta más rápidos y una prevención efectiva.
Inspección profunda de paquetes sin reensamblado	La inspección profunda de paquetes sin reensamblado sigue el malware independientemente del orden o del momento en el que llegan los paquetes. De esta forma garantiza una latencia extremadamente reducida y elimina las limitaciones del tamaño de archivo y del tamaño de flujo. Asimismo ofrece un mayor rendimiento y más seguridad que los diseños proxy anticuados. Estos reensamblan el contenido utilizando sockets ligados a programas antivirus tradicionales que presentan notables ineficiencias y una hiperpaginación excesiva de la memoria del socket, lo cual provoca una elevada latencia, un bajo rendimiento y limitaciones en el tamaño de los archivos
Anti-Virus (AV) en la nube	El motor RFDPI no utiliza solamente la base de datos integrada, sino que consulta adicionalmente SonicWALL Cloud Service para obtener información adicional sobre más de cuatro millones de definiciones de malware, en constante crecimiento.
Inspección bidireccional	RFDPI puede aplicarse a las conexiones entrantes y salientes para ofrecer protección al tráfico completo de la red independientemente de la dirección.
Actualizaciones de definiciones 24x7	El equipo SonicLabs Research crea y actualiza los bancos de datos de definiciones. Estos se envían automáticamente a los cortafuegos en uso, donde surten efecto inmediatamente, sin que haya necesidad de reinicializar los sistemas o interrumpir su servicio.

Prevención de intrusiones

Prestación	Descripción
Escaneo basado en definiciones	La prevención de intrusiones integrada basada en definiciones escanea los datos útiles de los paquetes en busca de vulnerabilidades y exploits que significan un riesgo para los sistemas internos de misión crítica.
Actualizaciones automáticas de las definiciones	El equipo de investigación de SonicWALL actualiza y distribuye continuamente una amplia lista de más de 5.400 definiciones IPS correspondientes a 52 categorías de ataques. Estas definiciones se hacen efectivas en el acto, sin que sea necesario reinicializar los sistemas o interrumpir su servicio.
Prevención de amenazas salientes	La inspección tanto del tráfico entrante como saliente evita que la red se utilice de forma indebida para ataques DDoS (Distributed Denial of Service) sin que los administradores se den cuenta e impide la transmisión de comandos de control en ataques Botnet.
Protección IPS entre zonas	La prevención de intrusiones puede implementarse entre zonas de seguridad internas para proteger los servidores sensibles y prevenir ataques internos.

VPN

VPN IPSec para conectividad entre emplazamientos	La VPN IPSec de alto rendimiento permite a la serie SuperMassive E10000 actuar como un concentrador VPN para miles de emplazamientos grandes, sucursales u oficinas domésticas.
Acceso remoto mediante VPN SSL o cliente IPSec	Permite utilizar la tecnología VPN SSL o un cliente IPSec de fácil gestión para el acceso sencillo a e-mails, archivos, ordenadores, sitios Intranet y aplicaciones desde una variedad de plataformas.
Pasarela VPN redundante	Al utilizarse múltiples WANs, puede configurarse una VPN primaria y otra secundaria para permitir la reconexión y recuperación automáticas de todas las sesiones VPN.
VPN basada en enrutamiento	El enrutamiento dinámico a través de enlaces VPN garantiza un servicio sin interrupciones en caso de fallo temporal del túnel VPN, ya que el tráfico entre los puntos terminales puede re-enrutarse fácilmente a través de rutas alternativas.

VoIP

QoS avanzada	Garantiza las comunicaciones críticas con etiquetado 802.1p y DSCP y remapeo del tráfico VoIP en la red.
Inspección profunda de paquetes del tráfico VoIP	Detección y bloqueo de amenazas específicas de VoIP mediante definiciones predefinidas.
Soporte de Gatekeeper H.323 y proxy SIP	Bloqueo de las llamadas spam: Todas las llamadas entrantes han de ser autorizadas y autenticadas mediante Gatekeeper H.323 o proxy SIP.

Cortafuegos e interconexión

Inspección dinámica de paquetes	Todo el tráfico de la red se inspecciona, analiza y se somete a las políticas de acceso del cortafuegos.
Protección contra ataques DOS	La protección SYN Flood proporciona defensas contra ataques DOS que utilizan tecnologías de lista negra de capa 3 (SYN proxy) y de capa 2 (SYN).
Implementación flexible	Puede implementarse en el modo tradicional NAT, en el modo puente de capa 2, en el modo Wire y en el modo de TAP de red.
Enrutamiento basado en políticas	Creación de enrutamientos basados en protocolos para direccionar el tráfico a una determinada conexión WAN, con posibilidad de reconexión a una WAN secundaria en caso de fallo de la alimentación.

PRESTACIONES

Cortafuegos e interconexión (continuación)

Prestación	Descripción
Alta disponibilidad	Soporta reconexión dinámica activa/pasiva, reconexión DPI activa/activa y reconexión de agrupación activa/activa para garantizar no solo una mayor fiabilidad debido a la protección contra errores de hardware o de software, sino también un mayor rendimiento, al desviar la carga de procesamiento de la inspección profunda de paquetes sin reensamblado a los núcleos disponibles en las unidades de reserva.
Equilibrio de carga WAN	Balanceo de la carga para un máximo de cuatro interfaces WAN mediante Round Robin o Spillover o utilizando métodos basados en porcentajes.

Gestión y monitoreo

Interfaz de usuario Web	Una interfaz intuitiva basada en Web permite una configuración rápida y cómoda con posibilidad de gestión a través del Sistema de gestión global de SonicWALL (GMS®) o de una CLI.
SNMP	SNMP permite supervisar el sistema y reaccionar rápidamente frente a ataques y alarmas.
Netflow/IPFIX	Permite exportar un amplio conjunto de datos mediante protocolos IPFIX o Netflow para proporcionar una visión granular del tráfico de aplicaciones, del uso del ancho de banda y de las amenazas de seguridad así como potentes prestaciones de análisis forense y resolución de problemas. Compatible con SonicWALL Scrutinizer y otras aplicaciones de monitoreo e informes de terceros proveedores. Los datos similares pueden exportarse a través de syslog a SonicWALL GMS y SonicWALL Analyzer.
Gestión de políticas centralizada	El Sistema de gestión global (GMS®) de SonicWALL permite generar informes y supervisar y configurar múltiples dispositivos SonicWALL a través de una única interfaz intuitiva, ofreciendo la posibilidad de personalizar el propio entorno de seguridad conforme a las políticas individuales.

Visión de conjunto de las prestaciones de SonicOS

Cortafuegos

- Inspección profunda de paquetes sin reensamblado
- Inspección profunda de paquetes para SSL
- Inspección dinámica de paquetes
- Protección contra ataques DOS
- Reensamblado TCP
- Modo stealth

Control de aplicaciones

- Control de aplicaciones
- Bloqueo de componentes de aplicaciones
- Gestión del ancho de banda de las aplicaciones
- Creación de definiciones personalizadas para las aplicaciones
- Visualización del flujo de aplicaciones
- Prevención de fuga de datos
- IPFIX con informes sobre extensiones
- Seguimiento de la actividad de los usuarios
- GeolP – Identificación del tráfico en base al país
- Amplia base de datos de definiciones de aplicaciones

Prevención de intrusiones

- Escaneo basado en definiciones
- Actualizaciones automáticas de las definiciones
- Prevención de amenazas salientes
- Lista de exclusiones IPS
- Mensajes de protocolización interactivos
- CFS unificado y control de aplicaciones con limitación del ancho de banda

Antimalware

- Escaneo de malware basado en flujos
- Antivirus en pasarela
- Antispyware en pasarela
- Descifrado SSL
- Antispam
- Inspección bidireccional
- Tamaño de archivo ilimitado

VPN

- VPN IPSec para conectividad entre emplazamientos
- Acceso remoto mediante VPN SSL o cliente IPSec
- Pasarela VPN redundante
- VPN basada en enrutamiento
- Mobile Connect para iOS

Filtrado de contenido Web

- Filtrado URL
- Tecnología antiproxy
- Bloqueo en base a palabras clave
- Gestión del ancho de banda según categorías de clasificación CFS
- Modelo de políticas unificadas con control de aplicaciones

VoIP

- QoS avanzada
- Gestión del ancho de banda
- Inspección profunda de paquetes del tráfico VoIP
- Interoperabilidad completa
- Soporte de Gatekeeper H.323 y proxy SIP

Interconexión

- Enrutamiento dinámico

- Enrutamiento basado en políticas
- NAT avanzado
- Servidor DHCP
- Gestión del ancho de banda
- IPv6
- Agregación de enlaces
- Redundancia de puertos
- Alta disponibilidad
- Equilibrio de carga

Gestión y supervisión

- Interfaz de usuario Web
- Interfaz de línea de comandos
- SNMP
- Informes Analyzer
- Informes Scrutinizer
- Gestión de políticas e informes mediante GMS
- Protocolización
- Netflow/IPFIX
- Visualización de aplicaciones
- Pantalla de gestión LCD
- Gestión centralizada de políticas
- Inicio de sesión único
- Soporte de servicios de terminal/Citrix
- Integración de funciones de análisis de Solera Networks

Servicios de seguridad

- Intrusion Prevention Service
- Gateway Anti-Malware Service
- Content Filtering Service
- Enforced Client Anti-Virus and Anti-Spyware Service
- Application Intelligence, Control and Visualization Service

Especificaciones del sistema	E10100	E10200	E10400	E10800
Sistema operativo	SonicOS			
Núcleos	12 (+ 12 alta disponibilidad)	24	48	96
Interfaces 10-GbE	6 x 10-GbE SFP+			
Interfaces 1-GbE	16 x 1-GbE SFP			
Interfaces de gestión	1 GbE, 1 consola			
Memoria (RAM)	8 GB	16 GB	32 GB	64 GB
Almacenamiento	80 GB SSD, Flash			
Rendimiento de inspección del cortafuegos	5,0 Gbps	10 Gbps	20 Gbps	40 Gbps
Rendimiento de inspección de aplicaciones	4,0 Gbps	7,5 Gbps	15 Gbps	30 Gbps
Rendimiento IPS	4,0 Gbps	7,5 Gbps	15 Gbps	30 Gbps
Rendimiento de inspección antimalware	2,0 Gbps	3,0 Gbps	6,0 Gbps	12 Gbps
Rendimiento VPN	2,5 Gbps	5,0 Gbps	10 Gbps	20 Gbps
Conexiones por segundo	80.000/seg.	160.000/seg.	320.000/seg.	640.000/seg.
Conexiones máximas (SPI)	1,5 millones	3,0 millones	6,0 millones	12,0 millones
Conexiones máximas (DPI)	1,2 millones	2,5 millones	5,0 millones	10,0 millones
VPN				
Túneles entre emplazamientos	10.000	10.000 (20.000)*	10.000 (40.000)*	10.000 (80.000)*
Clientes VPN IPSec	2.000	2.000 (4.000)*	2.000 (8.000)*	2.000 (16.000)*
Licencias VPN SSL	20 (1.000)*	50 (2.000)*	50 (4.000)*	50 (8.000)*
Cifrado	DES, 3DES, AES (128, 192, 256 bit)			
Autenticación	MD5, SHA-1			
Intercambio de claves	Grupos Diffie Hellman 1, 2, 5, 14			
VPN basada en enrutamiento	RIP, OSPF			
Interconexión				
Asignación de direcciones IP	Estática (DHCP PPPoE, L2TP y cliente PPTP), servidor DHCP interno, DHCP Relay			
Modos NAT	1:1, muchos:1, 1:muchos, NAT flexible (IPs solapadas), PAT, modo transparente			
Interfaces VLAN	512			
Protocolos de enrutamiento	BGP*, OSPF, RIPv1/v2, enrutamiento estático, enrutamiento basado en políticas, multicast			
QoS	Prioridad de ancho de banda, ancho de banda máx., ancho de banda garantizado, marcado DSCP, 802.1p			
Autenticación	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, base de datos interna, servicios de terminal, Citrix			
IPv6	IPv6 RFDPI, cortafuegos, VPN, NAT; Dual stack IPv4/IPv6; traducciones IPv6 hacia/desde IPv4; ICMPv6; DHCPv6; DNSv6			
VoIP	H323-v1-5 completo, SIP			
Normas	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Certificaciones pendientes	FIPS 140-2, Common Criteria EAL4+, NEBS, ICSA Firewall			
Soporte CAC (Common Access Card)	Pendiente			
Hardware				
Alimentación	Dos alimentaciones redundantes de cambio en caliente, 850 W			
Ventiladores	Dos ventiladores redundantes de cambio en caliente			
Display	Display LCD frontal			
Potencia de entrada	100-240 V CA, 60-50 Hz			
Consumo máximo de energía (W)	350	400	550	750
Factor de forma	Preparado para montaje en bastidor 4U			
Dimensiones	43 x 43,5 x 17,8 cm (17x18x7 pulgadas)			
Peso	26,3 kg (58 lb)	26,3 kg (58 lb)	27,7 kg (61 lb)	30,3 kg (67 lb)
Peso DEEE	26,8 kg (59 lb)	26,8 kg (59 lb)	28,1 kg (62 lb)	30,8 kg (68 lb)
Peso de envío	35,8 kg (79 lb)	35,8 kg (79 lb)	37,2 kg (82 lb)	39,9 kg (88 lb)
Conformidad con normas	FCC Class A, CE, C-Tick, VCCI, Compliance MIC, UL, cUL, TÜV/GS, CB, NOM, RoHS, DEEE			
Entorno	5-40 °C (40-105 F)			
Humedad	10-90% sin condensación			

*Disponible con licencia ampliada

Las especificaciones, prestaciones y la disponibilidad están sujetas a modificaciones.

Cortafuegos de próxima generación de la serie SuperMassive E10000

INFORMACIÓN DE PEDIDO

Producto	Nº de producto
SuperMassive E10100, 6 puertos SFP+ 10GbE, 16 puertos SFP 1GbE, dos ventiladores, dos alimentaciones CA	01-SSC-8883
SuperMassive E10200, 6 puertos SFP+ 10GbE, 16 puertos SFP 1GbE, dos ventiladores, dos alimentaciones CA	01-SSC-8882
SuperMassive E10400, 6 puertos SFP+ 10GbE, 16 puertos SFP 1GbE, dos ventiladores, dos alimentaciones CA	01-SSC-8881
SuperMassive E10800, 6 puertos SFP+ 10GbE, 16 puertos SFP 1GbE, dos ventiladores, dos alimentaciones CA	01-SSC-8856
Ampliaciones del sistema	Nº de producto
Ampliación SuperMassive E10100 a E10200	01-SSC-9496
Ampliación SuperMassive E10200 a E10400	01-SSC-9497
Ampliación SuperMassive E10400 a E10800	01-SSC-9498
Servicios E10100	Nº de producto
Prevención de amenazas – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus para E10100 (1 año)	01-SSC-9500
Inteligencia y control de aplicaciones – Application Intelligence, Application Control, App Flow Visualization para E10100 (1 año)	01-SSC-9506
Content Filtering Premium Business Edition para E10100 (1 año)	01-SSC-9503
Soporte Platinum para SuperMassive E10100 (1 año)	01-SSC-9512
Comprehensive Gateway Security Suite – Application Intelligence, prevención de amenazas, filtrado de contenidos con soporte para E10100 (1 año)	01-SSC-9515
Servicios E10200	Nº de producto
Prevención de amenazas – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus para E10200 (1 año)	01-SSC-9518
Inteligencia y control de aplicaciones – Application Intelligence, Application Control, App Flow Visualization para E10200 (1 año)	01-SSC-9524
Content Filtering Premium Business Edition para E10200 (1 año)	01-SSC-9521
Soporte Platinum para SuperMassive E10200 (1 año)	01-SSC-9530
Comprehensive Gateway Security Suite – Application Intelligence, prevención de amenazas, filtrado de contenidos con soporte para E10200 (1 año)	01-SSC-9533
Servicios E10400	Nº de producto
Prevención de amenazas – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus para E10400 (1 año)	01-SSC-9536
Inteligencia y control de aplicaciones – Application Intelligence, Application Control, App Flow Visualization para E10400 (1 año)	01-SSC-9542
Content Filtering Premium Business Edition para E10400 (1 año)	01-SSC-9539
Soporte Platinum para SuperMassive E10400 (1 año)	01-SSC-9548
Comprehensive Gateway Security Suite – Application Intelligence, prevención de amenazas, filtrado de contenidos con soporte para E10400 (1 año)	01-SSC-9551
Servicios E10800	Nº de producto
Inteligencia y control de aplicaciones – Application Intelligence, Application Control, App Flow Visualization para E10800 (1 año)	01-SSC-9560
Prevención de amenazas – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus para E10800 (1 año)	01-SSC-9554
Content Filtering Premium Business Edition para E10800 (1 año)	01-SSC-9557
Soporte Platinum para SuperMassive E10800 (1 año)	01-SSC-9566
Comprehensive Gateway Security Suite – Application Intelligence, prevención de amenazas, filtrado de contenidos con soporte para E10800 (1 año)	01-SSC-9569
Accesorios	Nº de producto
Ventilador de sistema FRU para la serie SuperMassive E10000	01-SSC-8885
Módulo de ventilador SSD para la serie SuperMassive E10000	01-SSC-8886
Alimentación de sistema FRU para la serie SuperMassive E10000	01-SSC-8887



Línea de soluciones de seguridad dinámica de SonicWALL



SEGURIDAD DE RED



ACCESO REMOTO SEGURO



SEGURIDAD DE WEB Y EMAIL



BACKUP Y RECUPERACIÓN



POLÍTICAS Y GESTIÓN

SonicWALL Iberia

T + 34 935 041 694

Spain@sonicwall.com

Contactos de soporte SonicWALL

www.sonicwall.com/emea/4724.html



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™