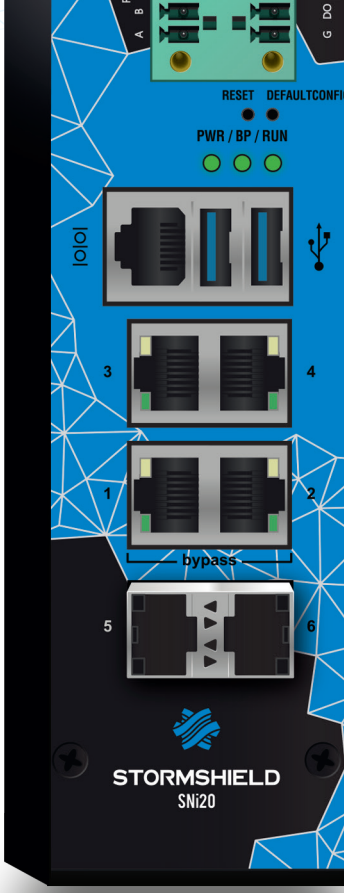
STORMSHIELD

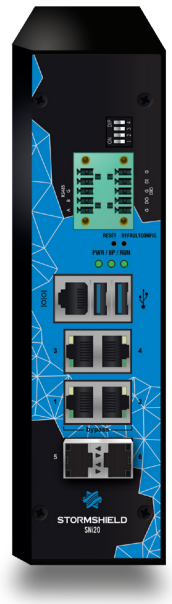
SEGURIDAD EN LA RED

STORMSHIELD **SNi20**

Cortafuegos industrial



2,4 Gbps	10 ms	DPI	NAT
RENDIMIENTO DEL CORTAFUEGOS	LATENCIA MÁXIMA	PROTOCOLOS INDUSTRIALES	INTEGRACIÓN EN REDES INDUSTRIALES



Un producto adaptado a su entorno

Con una combinación de funciones de integración de red única y transparente (enrutamiento y NAT) y seguridad avanzada, el SNi20 se integra sin cambiar la infraestructura operativa existente.

Integración en entornos industriales

- Seguridad de funcionamiento (clúster, bypass y alimentación)
- Subestaciones eléctricas (IEC 61850-3)
- Adecuado para entornos operativos difíciles (carril DIN, IP30)
- Coste de adquisición optimizado para aplicaciones a gran escala

Seguridad en tiempo real

- Mantenimiento remoto seguro de sus máquinas y autómatas (VPN SSL/IPsec)
- Control remoto de los procesos distribuidos
- Segmentación por zonas sin cambiar el sistema
- Protección de las operaciones (DPI, IPS, filtrado)

DATOS TÉCNICOS

RENDIMIENTO*	
Rendimiento del cortafuegos (UDP 1518 bytes)	**2,4 Gbps**
Rendimiento del cortafuegos (IMIX**)	**1,4 Gbps**
Rendimiento IPS (UDP 1518 bytes)	**1,6 Gbps**
Rendimiento IPS (1 Mb archivos HTTP)	**900 Mbps**
Latencia (máx.)	**10**
VPN*	
Rendimiento IPSec - AES-GCM	**600 Mbps**
N.º máx. de túneles VPN IPSec	**100**
Número máximo de SSL VPN (en modo portal)	**50**
Número de clientes simultáneos VPN SSL	**20**
CONECTIVIDAD DE RED	
N.º de sesiones simultáneas	**500 000**
N.º de nuevas sesiones por segundo	**20 000**
N.º de pasarelas principales (máx.)/backup (máx.)	**64/64**
CONECTIVIDAD	
Interfaces cobre 10/100/1000	**2-4**
Puertos SFP (cobre/fibra) 1 Gbps	**0-2**
Administración	**1 puerto serie y 2 USB 3.0**
PROTOCOLOS - DEEP PACKET INSPECTION (DPI)	
Protocolos Modbus, UMAS, S7 200-300-400, EtherNet/IP,CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose y SV), S7+ y IT	
ALTA DISPONIBILIDAD	
Activo/Pasivo	✔
Bypass	**Opcional**
HARDWARE	
Almacenamiento	**Tarjeta SD**
Chip TPM	✔
MTBF a 25 °C (en años)	**35,1**
Instalación	**Carril Din (anchura 35 mm, norma EN 50022)**
Altura x Anchura x Profundidad (mm)	**210 x 60 x 155**
Peso	**1,75 kg (3,86 libras)**
Altura x Anchura x Profundidad con embalaje (mm)	**190 x 270 x 235**
Peso con embalaje	**2,46 kg (5,42 libras)**
Fuente de alimentación redundante (CC)	**2x 12-48VDC 3-0,75A**
Consumo eléctrico (en reposo) CC a +25 °C	**15**
Consumo eléctrico (carga completa, máx.) CC a 25 °C	**19**
Ventiladores	**-**
Disipación térmica (máx., en BTU/h)	**64,83**
Temperatura de funcionamiento	**de -40 °C a +70 °C (de -40 °C a +158 °F)**
Humedad relativa en funcionamiento (sin condensación)	**de 0 % a 95 %**
Nivel de protección que ofrece el dispositivo (código IP)	**IP30**
Temperatura de almacenamiento	**de -40 °C a +85 °C (de -40 °C a +185 °F)**
Humedad relativa de funcionamiento (sin condensación)	**de 0 % a 95 %**

CERTIFICACIONES

CE/FCC/CB, EN 61000-6-2, EN 61000-6-4, IEC 61000-4-18, IEC 60068-2, IEC 61850-3, IEEE 1613, EN 50121-4, IEC 60529

FUNCIONES

CONTROL DE USO

Modo cortafuegos/IPS/IDS, Cortafuegos basado en identidad, Detección y gestión de aplicaciones, Cortafuegos para servicios de Microsoft - Cortafuegos/IPS/IDS industrial, Control de aplicaciones industriales, Detección y control de uso de dispositivos móviles, Inventario de aplicaciones (opcional), Detección de vulnerabilidades (opcional), Geolocalización (países, continentes), Reputación de host dinámico, Autenticación transparente (Active Directory SSO Agent, SSL, SPNEGO), Autenticación VDI multiusuario basada en agente (Citrix-TSE), Autenticación en modo invitado y patrocinio, webservices.

PROTECCIÓN CONTRA AMENAZAS

Prevención y detección de intrusiones, Autodetección de protocolos y comprobación del cumplimiento, Inspección de aplicaciones, Protección frente a ataques de denegación de servicio (DoS), Protección contra inyección SQL, Protección contra Cross-Site Scripting (XSS), Protección frente a scripts y códigos maliciosos Web2.0 (limpieza y autorización), Detección de troyanos, Detección de conexiones interactivas (Botnet, Mando y Control), Protección contra las técnicas de evasión, Gestión avanzada de la fragmentación, Respuesta automática a ataques (notificación, cuarentena, bloqueo, QoS, volcado), Detección y descifrado SSL, Protección VoIP (SIP), Seguridad colaborativa: Reputación IP.

CONFIDENCIALIDAD

VPN IPSec sitio a sitio o nómada, Acceso remoto VPN SSL en modo túnel multi-OS (Windows, Android, iOS, etc.), Agente VPN SSL configurable de forma centralizada (Windows), Compatibilidad VPN IPSec Android/iPhone.

RED - INTEGRACIÓN

IPv6 - Modos NAT, PAT, transparente (puente)/enrutado/híbrido, Enrutamiento dinámico (RIP, OSPF, BGP), Multicast, Gestión de enlaces múltiples (balanceo, conmutación por error), Gestión de PKI interna o externa multiniveles, Autenticación multidominio (incluido LDAP interno), Enrutamiento basado en políticas (PBR), Gestión QoS, DHCP cliente/relé/servidor, Cliente NTP, LACP, Spanning Tree Protocols (RSTP y MSTP), SD-WAN, Autentificación multifactor (MFA).

GESTIÓN

Interfaz de gestión Web con navegación privada (cumplimiento de la RGPD), Política de seguridad orientada a objetos, Política de seguridad contextual, Ayuda para la configuración en tiempo real, Contadores de reglas, Actualizaciones de seguridad conectadas o desconectadas, Política de seguridad global/local, Informes de registro integrados y herramientas de análisis, Informes interactivos y personalizables, Compatibilidad con servidor syslog múltiple UDP/ TCP/TLS, Agente SNMP v1, v2, v3, IPFIX, Copia de seguridad automatizada de configuraciones, API abierta, Registro de scripts.

Documento no contractual. Las funcionalidades mencionadas son las de la versión 4.x.

** El rendimiento se evalúa en laboratorio y en condiciones ideales para la versión 4.x. Los resultados pueden variar en función de las condiciones del ensayo y de la versión del software.*