Firewalls de la serie H3C SecPath F1000-AI

Firewalls de próxima generación

New H3C Technologies Co., Limited

Firewalls de la serie H3C SecPath F1000-AI

Resumen del producto

La serie de firewalls H3C SecPath F1000-AI incorpora capacidades innovadoras de Inteligencia Artificial (IA) para pequeñas y medianas empresas, salidas de campus y sucursales de WAN.

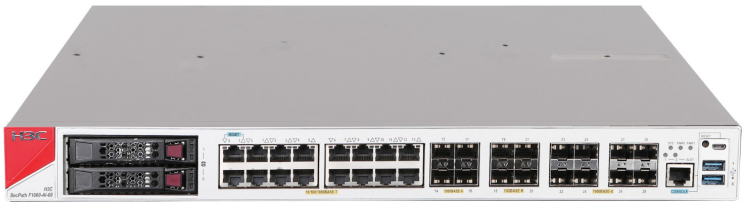
H3C SecPath Serie F1000-AI cumple con los requisitos de Web 2.0 y admite las siguientes funciones de seguridad y red:

- Protección de seguridad y control de acceso basados en usuarios, aplicaciones, tiempo, cinco tuplas y otros elementos. Las características típicas de protección de seguridad incluyen IPS, AV y DLP.
- Incluye servicios VPN, como L2TP VPN, GRE VPN, IPsec VPN y SSL VPN.
- Capacidades de enrutamiento, incluyendo enrutamiento estático, RIP, OSPF, BGP, IS-IS, políticas de enrutamiento y enrutamiento basado en aplicaciones y URL.
- IPv4 y IPv6 dual stacks, y protección de estado y prevención de ataques para IPv6.

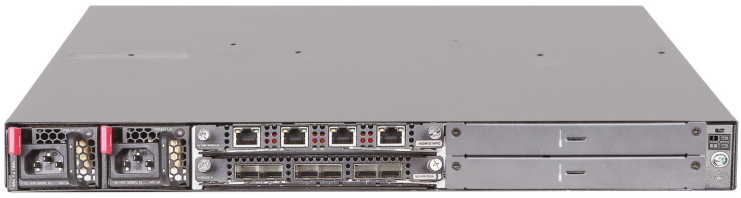
F1000-AI-10 Vista Frontal

F1000-AI-10 Vista trasera

F1000-AI-15 Vista Frontal

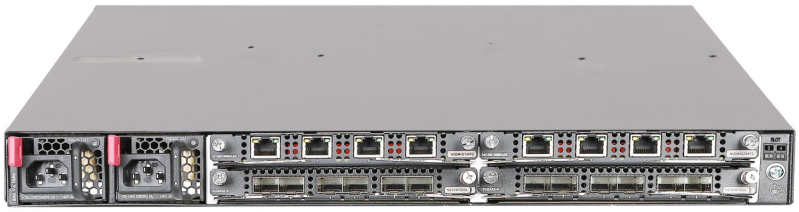


F1000-AI-60/70 Vista Frontal

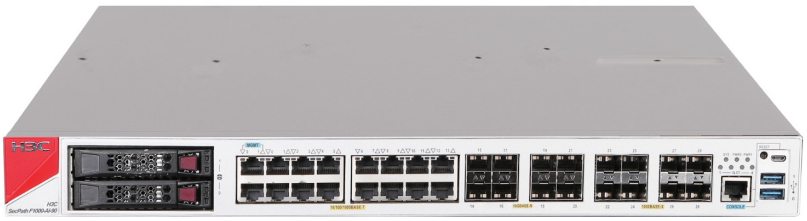


F1000-AI-60/70 Vista Trasera

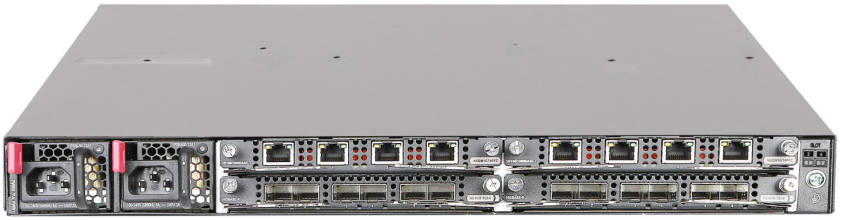
F1000-AI-80 Vista Frontal



F1000-AI-80 Vista trasera



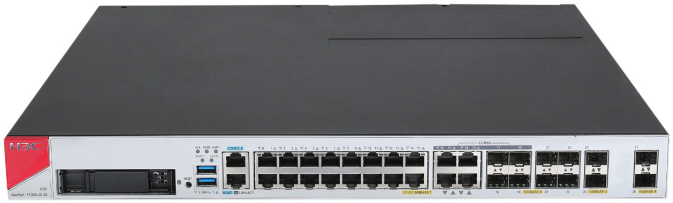
F1000-AI-90 Vista Frontal



F1000-AI-90 Vista trasera

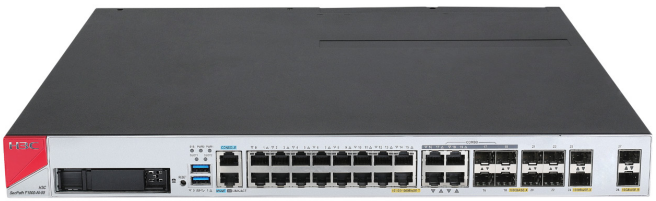
F1000-AI-25 Vista Frontal

F1000-AI-25 Vista trasera



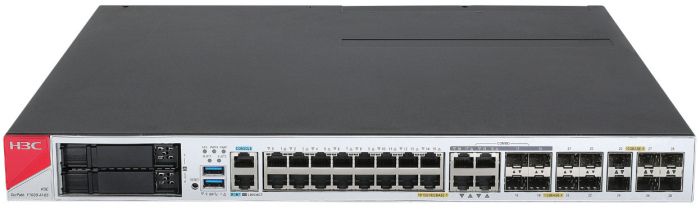
F1000-AI-35 Vista Frontal

F1000-AI-35 Vista trasera



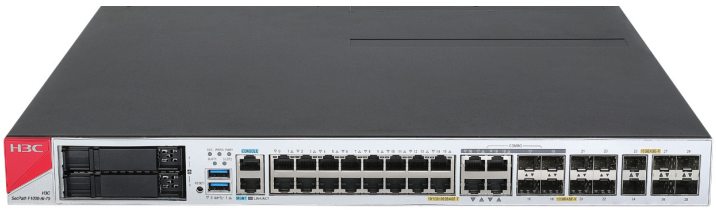
F1000-AI-55 Vista Frontal

F1000-AI-55 Vista trasera



F1000-AI-65 Vista Frontal

F1000-AI-65 Vista trasera



F1000-AI-75 Vista Frontal

F1000-AI-75 Vista trasera

Características y beneficios

Plataformas de software y hardware de alto rendimiento

Utiliza procesadores avanzados de 64 bits y múltiples núcleos y cachés.

Alta disponibilidad a nivel de operador

- Utiliza plataformas de hardware y software propietarias de H3C que han sido probadas por operadores de telecomunicaciones y pequeñas y medianas empresas.
- Apoya H3C SCF, que puede virtualizar múltiples dispositivos en uno para una gestión unificada de recursos, respaldo de servicios y mejora del rendimiento del sistema.
- Apoya la tecnología H3C RBM (Hot Backup Management) que proporciona una solución de alta disponibilidad a nivel de dispositivo y nivel de sistema. Además de aumentar el ancho de banda de enlace, mejorar la fiabilidad de la red y compartir la carga de tráfico.

Poderosa protección de seguridad

- Protección contra ataques—Detecta y previene varios ataques, incluyendo Land, Smurf, Fraggle, ping de la muerte, Tear Drop, suplantación de IP, fragmentación de IP, suplantación de ARP, búsqueda inversa de ARP, bandera inválida de TCP, paquete ICMP grande, escaneo de IP/puerto, y ataques DDoS comunes como inundación SYN, inundación UDP, inundación DNS e inundación ICMP.
- SOP N:1 virtualización—Utiliza la tecnología de virtualización basada en contenedores. Un firewall de la serie F1000 se puede virtualizar en múltiples firewalls lógicos, que tienen las mismas características que el firewall físico. Cada firewall virtual puede tener su propia política de seguridad y puede ser gestionado de forma independiente.
- Zona de seguridad—configura zonas de seguridad según las interfaces y las VLAN.
- Filtrado de paquetes—aplica ACL estándar o avanzada entre zonas de seguridad para filtrar paquetes en base a información contenida en ellos, como números de puertos UDP y TCP. También puedes configurar rangos de tiempo durante los cuales se realizará el filtrado de paquetes.
- Control de acceso—Soporta control de acceso basado en usuarios y aplicaciones e integra prevención de intrusos profunda con control de acceso.
- ASPF—Determina dinámicamente si se debe reenviar o descartar un paquete verificando la información y el estado del protocolo de capa de aplicación. ASPF admite la inspección de protocolos de capa de aplicación basados en TCP/UDP, como FTP, HTTP, SMTP, RTSP y otros.
- AAA—Admite autenticación basada en RADIUS/HWTACACS+, CHAP y PAP.
- Lista negra—compatible con lista negra estática y lista negra dinámica.
- NAT y NAT compatibles con VRF

- VPN—Soporta L2TP, IPsec/IKE, GRE y VPN SSL. Permite que los dispositivos inteligentes se conecten a las VPN.
- Enrutamiento—Soporta enrutamiento estático, RIP, OSPF, BGP, políticas de enrutamiento y enrutamiento basado en aplicaciones, URL y políticas.
- Registros de seguridad—Soporta registros de operación, registros de coincidencia de políticas de pares de zonas, registros de protección contra ataques, registros de DS-LITE y registros de NAT444.
- Tráfico monitoreo, estadísticas y gestión.

Flexible y extensible, integrada y avanzada seguridad de DPI

- Plataforma de procesamiento de servicios de seguridad integrada—Integra de manera altamente las medidas de protección básicas y avanzadas en una plataforma de seguridad.
- Identificación y gestión del tráfico de capa de aplicación.
  - Utiliza la máquina de estado y las tecnologías de inspección de intercambio de tráfico para detectar el tráfico de aplicaciones P2P, IM, juegos en red, acciones, video en red y multimedia en red, como Thunder, Web Thunder, BitTorrent, eMule, eDonkey, WeChat, Weibo, QQ, MSN y PPLive.
  - Utiliza la tecnología de inspección profunda para identificar el tráfico P2P de manera precisa y proporciona múltiples políticas para controlar y administrar el tráfico P2P de manera flexible.
  - H3C SecPath NGFW soporta más de 7,000 protocolos y más de 6,000 aplicaciones, que se actualizan cada 2 semanas.
- Motor de inspección de intrusiones altamente preciso y efectivo—utiliza el motor de Inspección Completa con Prueba Rigurosa de Estado (FIRST), de propiedad de H3C, y varias tecnologías de inspección de intrusiones para implementar una inspección altamente precisa de intrusiones basada en estados de la aplicación. El motor FIRST también admite inspecciones simultáneas de software y hardware para mejorar la eficiencia de la inspección.
- Protección antivirus en tiempo real—utiliza el motor antivirus basado en transmisión para prevenir, detectar y eliminar códigos maliciosos del tráfico de red.
- Filtrado categorizado de URLs masivas—utiliza el modo local+nube para proporcionar 139 bibliotecas de URLs categorizadas y 130 millones de URL, así como admitir más de 20 millones de reglas de filtrado de URL. Proporciona una lista negra y una lista blanca de filtrado básico de URL y te permite consultar el servidor de filtrado de categoría de URL en línea.
- Base de firmas de seguridad completa y actualizada—H3C cuenta con un equipo senior de base de datos de firmas y laboratorios profesionales de protección contra ataques que pueden proporcionar

una base de firmas precisa y actualizada.

- Tarjeta de Negocios Inteligente (módulo de IA)— apoya con CPU/memoria independiente, puede instalar software de terceros basado en Linux.

Oferta las mejores funciones IPv6 de la industria

- Firewall estadístico IPv6.
- Protege contra ataques relacionados con IPv6.
- Traduce: Reenvío de datos IPv6, enrutamiento estático y enrutamiento dinámico IPv6, e IPv6 multicast.
- Tecnologías de transición IPv6, incluyendo NAT-PT, túnel IPv6 sobre GRE IPv4, túnel manual, túnel 6to4, túnel IPv6 automático compatible con IPv4, túnel ISATAP, NAT444 y DS-Lite.
- IPv6 ACL y RADIUS.

Siguiente generación de características de múltiples servicios

- Característica integrada de balanceo de carga de enlace—utiliza tecnologías de inspección de estado y detección de ocupación de enlaces, y se aplica a una salida de red para equilibrar el tráfico entre enlaces.
- Característica de Balanceo de Carga del Servidor—Soporta balanceo de carga del servidor (SLB), soporta coincidencia basada en tipos de aplicaciones como HTTP, RADIUS, MYSQL, etc., soporta reglas de coincidencia basadas en características de tráfico IP, ISP, usuario, interfaz de entrada, carga TCP, etc. (se proporcionan capturas de pantalla).
- Función integrada de SSL VPN—Utiliza una clave USB, mensajes SMS y el sistema de autenticación existente en la empresa para autenticar a los usuarios, proporcionando acceso seguro a los usuarios móviles a la red de la empresa.
- Prevención de fuga de datos (DLP)—Soporta la filtración de correos electrónicos por dirección SMTP, asunto, adjunto y contenido, filtrado de URL y contenido HTTP, filtrado de archivos FTP y filtrado de capa de aplicación (incluyendo bloqueo de Java/ActiveX y prevención de ataques de inyección SQL).
- Sistema de prevención de intrusiones (IPS)—Soporta la interceptación activa en tiempo real de ataques DOS, desmontaje por fuerza bruta, escaneo de puertos, sniffing, gusanos y otros ataques o tráfico malicioso de red, protege la información de la red interna de infracciones.
- Antivirus (AV)—Utiliza un motor de detección de virus de alto rendimiento y una base de datos de firmas de virus actualizada diariamente para prevenir ataques de más de 5 millones de virus.
- Prevención de amenazas desconocidas—Utiliza la plataforma de conciencia situacional para detectar y localizar rápidamente las amenazas. Esto garantiza que el firewall pueda tomar medidas de seguridad globales tan pronto como un punto único esté bajo ataque.

- Firewall de Aplicación Web (WAF)—Protección profunda de seguridad en la web. Apoya una protección fina de aplicaciones web. Para los ataques de CC más molestos, la detección y verificación de contenido de diversas solicitudes de clientes de aplicaciones web se llevan a cabo para asegurar su seguridad y legitimidad, bloqueando en tiempo real las solicitudes ilegales, y protegiendo de manera efectiva todo tipo de sitios web.
- Inteligencia de amenazas (TI)—La inteligencia de amenazas es el conocimiento sobre una amenaza que contiene información contextual. La inteligencia de amenazas puede identificar incidentes de ciberseguridad como infiltraciones y robo de datos, así como la motivación, proceso de ataque e instalaciones utilizadas por el atacante. La inteligencia de amenazas puede detectar rápidamente tráfico sospechoso mediante la vinculación con reglas asociadas, de modo que los administradores puedan determinar de antemano si es necesario mejorar las capacidades de seguridad relevantes en la red. Incluye la reputación de IP, la reputación de dominio y la reputación de URL.
- Función SD-WAN (Solución H3C AD-WAN)—El dispositivo podría ser gestionado por el controlador H3C AD-WAN, podría ser desplegado como un nodo SD-WAN de concentrador/punto de red. El dispositivo debería soportar funciones SD-WAN incluyendo pero no limitadas a A-FEC, optimización de WAN, etc.

Gestión inteligente

- Gestión de políticas de seguridad inteligente - Detecta políticas duplicadas, optimiza las reglas de coincidencia de políticas, detecta y propone políticas de seguridad generadas dinámicamente en la red interna.
- SNMPv3—Compatible con SNMPv1 y SNMPv2.
- Configura y gestiona basándote en la línea de comandos.
- Gestión basada en web, con una interfaz gráfica simple y amigable.
- H3C IMC SSM gestión unificada: recolecta y analiza información de seguridad, ofrece una vista intuitiva de las condiciones de red y seguridad, ahorrando esfuerzos de gestión y mejorando la eficiencia.
- Gestión centralizada de registros basada en tecnología avanzada de análisis y filtrado de datos: solicita y recibe información para generar registros, compila diferentes tipos de registros (como syslogs y registros de transmisión binarios) en el mismo formato, y comprime y almacena grandes cantidades de registros. Puedes encriptar y exportar registros guardados a dispositivos de almacenamiento externos como DAS, NAS y SAN para evitar pérdidas de registros de seguridad importantes.
- Apoya la plataforma de nube pública (H3C Cloudnet).
- Incluye informes basados en aplicaciones y informes de análisis basados en secuencias.
- Varios formatos de informe exportados, incluye PDF, HTML, word y txt.
- Personaliza el informe a través de la interfaz web: puedes ajustar el rango de tiempo, el dispositivo de

origen de los datos, el período de generación y el formato de exportación.

Especificaciones

Artículo	F1000-AI-10/15	F1000-AI-60/70	F1000-AI-80/90	F1000-AI-25/35/55	F1000-AI-65/75
Dimensiones (Ancho x Profundidad x Altura)	440mm×260mm×44.2mm	440mm×435mm×44.2mm			
USB 3.0	2	2	2	2	2
montado en rack	Sí	Sí	Sí	Sí	sí
Peso.	3.7kg	10.0kg	10.0kg	5.4kg	5.6kg
Fuente de alimentación	AC	Doble intercambiable en caliente, AC o DC	Doble intercambiable en caliente, AC o DC	Doble intercambiable en caliente, AC o DC	Doble intercambiable en caliente, AC o DC
Consumo de energía	39W	180W	180W	23W	46W
MTBF(Año)	77.36	45.39	43.2	53.38	50.31
MTTR(h)	1	1	1	1	1
Puertos	1 × Puerto de consola (CON) 2 × Puerto de administración 18 × Gigabit Ethernet puertos de cobre 4 puertos Gigabit Ethernet con función de bypass	1 × Puerto de consola (CON) 2 × Puerto de administración 12 × Puertos de fibra Ethernet Gigabit 14 × Gigabit Ethernet puertos de cobre 4 × 10-	1 × Puerto de consola (CON) 2 × Puerto de administración 8 × Puertos de fibra Ethernet Gigabit 14 × Gigabit Ethernet puertos de cobre 8 × 10-	1 × Puerto de consola (CON) 1 × Puerto de administración 6 × Puertos de fibra Ethernet Gigabit 16 × Gigabit Ethernet puertos de cobre 4 × Puertos	1 × Puerto de consola (CON) 1 × Puerto de administración 4 × Puertos de fibra Ethernet Gigabit 16 × Gigabit Ethernet puertos de cobre 4 × Puertos Combo de Gigabit Ethernet 6 × 10-Gigabit Ethernet fiber ports

	8 ×Puertos Combo de Gigabit Ethernet 2 × 10-Gigabit Ethernet fiber ports	Gigabit Ethernet fiber ports	Gigabit Ethernet fiber ports	Combo de Gigabit Ethernet 2 × 10-Gigabit Ethernet fiber ports	
Ranuras de expansión	0	2/4	4	2	2
Módulos de interfaz	N/A	4 puertos módulo de interfaz GE PFC 4-port GE módulo de interfaz de fibra 4-puerto módulo de interfaz de fibra 10-GE 6-puerto módulo de interfaz de fibra 10-GE	4 puertos módulo de interfaz GE PFC 4-port GE módulo de interfaz de fibra 4-puerto módulo de interfaz de fibra 10-GE 6-puerto módulo de interfaz de fibra 10-GE	4 puertos módulo de interfaz GE PFC 4-port GE módulo de interfaz de fibra 4-puerto módulo de interfaz de fibra 10-GE	4 puertos módulo de interfaz GE PFC 4-port GE módulo de interfaz de fibra 4-puerto módulo de interfaz de fibra 10-GE 6-puerto módulo de interfaz de fibra 10-GE
Almacenamiento	480G M.2	2 × 480G SSD	2 × 480G SSD	1 × 480G SSD/ 500G HDD/1TB HDD	2 × 480G SSD/ 500G HDD/1TB HDD
Flash	4GB	4GB	8GB	4GB	4GB
SDRAM	2GB	8G	16G	4GB/4GB/8GB	8G
Temperatura	Funcionamiento: 0°C a 45°C (32°F a 113°F) Almacenamiento: –40°C a +70°C (–40°F a +158°F)				
Modos de	Ruta, transparente y híbrida				

operación	
AAA	Portal de autenticación Autenticación RADIUS Autenticación HWTACACS PKI/CA (X.509 formato) autenticación Autenticación de dominio. Autenticación CHAP Autenticación PAP
Cortafuegos	Aplica la tecnología de firewall virtual SOP, que soporta la virtualización completa de los recursos de hardware, incluyendo CPU, memoria y almacenamiento. Asignar zona de seguridad Protección contra ataques maliciosos, como land, smurf, fraggle, ping de la muerte, teardrop, IP spoofing, IP fragmentation, ARP spoofing, búsqueda inversa de ARP, bandera inválida de TCP, paquete ICMP grande, escaneo de dirección/puerto, SYN flood, ICMP flood, UDP flood y DNS query flood. Básicos y avanzados ACLs Rango de tiempo ACL Traducir al español: Control de acceso basado en usuarios y aplicaciones. Aplicar filtrado de paquetes de capa de aplicación ASPF. Función de lista negra estática y dinámica. Asociación MAC-IP Basado en MAC ACL Limitación de MAC Traducción: Transmitir VLAN transparente 802.1Q Control de ancho de banda
Antivirus	Detección de virus basada en firmas Manual y automático actualización para la base de datos de firmas Procesamiento basado en flujo. Detección de virus basada en HTTP, FTP, SMTP y POP3 Tipos de virus incluyen Backdoor, Email-Worm, IM-Worm, P2P-Worm, Trojan, AdWare y Virus. Registros y informes de virus
Prevención	Prevención contra ataques comunes como hacker, gusano/virus, troyano, código

profunda de intrusiones.	malicioso, spyware/adware, DoS/DDoS, desbordamiento de búfer, inyección SQL y eludir IDS/IPS. Categorías de firmas de ataque (basadas en tipos de ataques y sistemas objetivo) y niveles de gravedad (incluyendo alto, medio, bajo y notificación) Manual y automático actualiza la base de datos de firmas de ataque (TFTP y HTTP). Identificar y controlar el tráfico P2P/IM
Filtrar correo electrónico/ página web/capa de aplicación	Filtrar el correo electrónico Filtra direcciones de correo electrónico SMTP Filtrar asunto/contenido/adjuntos de correo electrónico Filtrar páginas web URL HTTP/filtrado de contenido Bloquea en Java Bloquear ActiveX Prevén ataques de inyección SQL
NAT	Mapea múltiples direcciones internas a una dirección pública con Many-to-one NAT. Muchos-a-muchos NAT, que mapea múltiples direcciones internas a múltiples direcciones públicas Mapea una dirección interna a una dirección pública con NAT uno-a-uno. NAT tanto la dirección de origen como la dirección de destino Acceso de hosts externos a servidores internos. Mapeo de dirección interna a dirección de interfaz pública Soporte NAT para DNS Establece el período efectivo para NAT NAT ALGs para NAT ALG, incluyendo DNS, FTP, H.323, ILS, MSN, NBT, PPTP y SIP
VPN	L2TP VPN IPSec VPN GRE VPN SSL VPN
IPSEC VPN	ESP-DES-CBC/ESP-3DES-CBC/ESP-AES-128-CBC/ESP-AES-192-CBC/ESP-AES-256-CBC/ESP-AES-128-GCM/ESP-NULL/SM1-cbc-128/SM4-cbc
IPSEC VPN Autenticación del	MD5/SHA1/SM3

algoritmo	
IPv6	Estado del firewall IPv6 Protege ataques IPv6 Reenvío de IPv6 Protocolos de IPv6 como ICMPv6, PMTU, Ping6, DNS6, TraceRT6, Telnet6, Cliente DHCPv6 y Relay DHCPv6. Enrutamiento IPv6: RIPng, OSPFv3, BGP4+, enrutamiento estático, enrutamiento basado en políticas Multidifusión IPv6: PIM-SM y PIM-DM Técnicas de transición de IPv6: NAT-PT, túneles IPv6, NAT64 (DNS64) y DS-LITE Seguridad de IPv6: NAT-PT, túnel IPv6, filtro de paquetes IPv6, RADIUS, políticas de pares de zonas IPv6, límite de conexión IPv6
IEEE	IEEE 802.1X
Alta disponibilidad	Virtualización SCF 2:1 Failover estatal activo/activo y activo/pasivo. Sincroniza la configuración de dos firewalls. Sincroniza el estado IKE en la VPN IPsec. VRRP
Gestiona la configuración.	Gestiona la configuración en la interfaz de línea de comandos. Gestiona remotamente a través de la web. Gestiona dispositivos a través de H3C IMC SSM. Usa SNMPv3, compatible con SNMPv2 y SNMPv1. Política de seguridad inteligente
Protección del medio ambiente	Cumplimiento RoHS de la UE
EMC	FCC Parte 15 (CFR 47) CLASE A ICES-003 CLASE A Clasificación VCCI clase A CISPR 22 CLASE A EN 55022 CLASE A AS/NZS CISPR22 CLASE A CISPR 32 CLASE A

	EN 55032 CLASE A AS/NZS CISPR32 CLASE A CISPR 24 EN 55024 EN 61000-3-2 EN 61000-3-3 ETSI EN 300 386 GB 9254 GB 17625.1 YD/T 993
Seguridad	UL 60950-1 CAN/CSA C22.2 No 60950-1 IEC 60950-1 EN 60950-1 AS/NZS 60950-1 FDA 21 CFR Subcapítulo J GB 4943.1

Descripción de la licencia

Licencia	Característica	Antes de la instalación de la licencia	Después de la expiración de la licencia	Periodo de validez
LIS-F1000-LB	Balanceo de carga del servidor.	No está disponible el balanceo de carga del servidor.	Disponible el balanceo de carga del servidor.	Permamente
LIS-F1000-ACG	Reconocimiento de aplicaciones (APR)	No se admite la actualización de la biblioteca de firmas APR.	No se admite la actualización de la biblioteca de firmas APR.	1 año 3 años
LIS-F1000-AV	Antivirus	No está disponible el antivirus y no se admite actualizar la biblioteca de firmas de virus.	El anti-virus todavía está disponible, pero no puedes actualizar la biblioteca de firmas de virus ni utilizar la consulta en la nube, la	1 año 3 años

			inspección mejorada y la función de colaboración en sandbox.	
LIS-F1000-TI	Utiliza inteligencia de amenazas (incluyendo reputación de IP, reputación de URL y reputación de dominio).	No está disponible la inteligencia de amenazas y no se admite la actualización de la biblioteca de firmas de inteligencia de amenazas.	Threat intelligence sigue disponible, pero no actualices la biblioteca de firmas de amenazas.	1 año 3 años
LIS-F1000-IPS	IPS	No está disponible IPS y no se admite la actualización de la biblioteca de firmas de IPS.	IPS sigue disponible, pero no actualices la biblioteca de firmas de IPS.	1 año 3 años
LIS-F1000-SSL	SSL VPN	El sistema soporta solo el número máximo predeterminado de usuarios de SSL VPN.	N/A	Permamente
LIS-F1000-URL	Filtrar URL	URL de consulta en la nube no disponible y no se admite la actualización de la biblioteca de firmas URL.	URL de consulta en la nube no disponible y no se admite la actualización de la biblioteca de firmas URL.	1 año 3 años
LIS-F1000-WAF	Protege el WAF	La protección WAF no está disponible y no se admite la actualización de la biblioteca de firmas WAF.	Protege tu WAF pero no actualices la biblioteca de firmas.	1 año 3 años

* Comparte el mismo licencia con el firewall físico.

Consulta de pedidos

SecPath Serie F1000-AI	
NS-SecPath F1000-AI-	H3C SecPath F1000-AI-10 Firewall Appliance

10	
NS-F1000-AI-15	H3C SecPath F1000-AI-15 Firewall Appliance
NS-F1000-AI-25	H3C SecPath F1000-AI-25 Firewall Appliance
NS-F1000-AI-35	H3C SecPath F1000-AI-35 Firewall Appliance
NS-F1000-AI-55	H3C SecPath F1000-AI-55 Firewall Appliance
NS-F1000-AI-60	H3C SecPath F1000-AI-60 Firewall Appliance
NS-F1000-AI-65	H3C SecPath F1000-AI-65 Firewall Appliance
NS-F1000-AI-70	H3C SecPath F1000-AI-70 Firewall Appliance
NS-F1000-AI-75	H3C SecPath F1000-AI-75 Firewall Appliance
NS-F1000-AI-80	H3C SecPath F1000-AI-80 Firewall Appliance
NS-F1000-AI-90	H3C SecPath F1000-AI-90 Firewall Appliance
Fuente de alimentación	
PSR150-A1-B	150W AC Power Supply
PSR150-D1-B	150W DC Power Supply
PSR250-12A1	250W AC Power Supply Module(Air Outlets in Panel)
PSR450-12D	450W DC Power Supply Module (Air Outlets in Panel)
PSR450-12AHD	450W HVDC Power Supply Module (AC/336V HVDC Input Supported, Air Outlets in Panel)
Módulos	
NSQM1GT4PFC	H3C SecPath F1000 Series PFC Card
NSQM1TG4FBA	H3C SecPath F1000 Series, 4 Ports SFP+ Module
NSQM1GP4FBA	H3C SecPath F1000 Series, 4 Ports SFP Module
NSQM1NIMTG6A	H3C SecPath F1000 Series 6-Port Ten-Gigabit Ethernet Optical Interface Module(SFP+)
Disco Duro	
NS-HDD-500G-SATA-SFF	H3C SecPath Series,500GB 2.5inch SATA HDD HardDisk Module
NS-HDD-1T-SATA-SFF	H3C SecPath Series,1TB 2.5inch SATA HDD HardDisk Module
NS-SSD-480G-SATA-SFF	H3C SecPath Series,480GB 2.5inch SATA SSD HardDisk Module
Licencia	
LIS-F1000-IPS1-1Y	H3C SecPath F1000,IPS Signature Update Service,1 Year
LIS-F1000-IPS3-3Y	H3C SecPath F1000,IPS Signature Update Service,3 Years
LIS-F1000-AV-1Y	H3C SecPath F1000,AV Anti-Virus Security License,1 Year
LIS-F1000-AV-3Y	H3C SecPath F1000,AV Anti-Virus Security License,3 Years
LIS-F1000-ACG1-1Y	H3C SecPath F1000,Application Signature Update Service,1 Year
LIS-F1000-ACG3-3Y	H3C SecPath F1000,Application Signature Update Service,3 Years
LIS-F1000-LB	H3C SecPath F1000,SLB License, permanent authorization
LIS-F1000-SSL-25	H3C SecPath F1000,SSL VPN for 25 Users

LIS-F1000-SSL-125	H3C SecPath F1000,SSL VPN for 125 Users
LIS-F1000-SSL-500	H3C SecPath F1000,SSL VPN for 500 Users
LIS-F1000-SSL-1000	H3C SecPath F1000,SSL VPN for 1000 Users
LIS-F1000-URL-1Y	H3C SecPath F1000 URL Signature Update Service License,1 Year
LIS-F1000-URL-3Y	H3C SecPath F1000 URL Signature Update Service License,3 Years
LIS-IMC7-SVF1KA-25	H3C iMC-SSL VPN Authentication Client-F1000-25 License
LIS-IMC7-SVF1KB-125	H3C iMC-SSL VPN Authentication Client-F1000-125 License
LIS-IMC7-SVF1KC-500	H3C iMC-SSL VPN Authentication Client-F1000-500 License
LIS-IMC7-SVF1KD-1K	H3C iMC-SSL VPN Authentication Client-F1000-1000 License
LIS-F1000-WAF-1Y	H3C SecPath F1000 WAF Signature Update License,1 Year
LIS-F1000-WAF-3Y	H3C SecPath F1000 WAF Signature Update License,3 Year
Transceptores	
SFP-GE-SX-MM850-A	1000BASE-SX SFP Transceiver, Multi-Mode (850nm, 550m, LC)
SFP-GE-LX-SM1310-A	1000BASE-LX SFP Transceiver, Single Mode (1310nm, 10km, LC)
SFP-GE-LH40-SM1310	1000BASE-LH40 SFP Transceiver, Single Mode (1310nm, 40km, LC)
SFP-GE-LH40-SM1550	1000BASE-LH40 SFP Transceiver, Single Mode (1550nm, 40km, LC)
SFP-GE-LH80-SM1550	1000BASE-LH80 SFP Transceiver, Single Mode (1550nm, 80km, LC)
SFP-GE-LH100-SM1550	1000BASE-LH100 SFP Transceiver, Single Mode (1550nm, 100km, LC)
SFP-XG-LX220-MM1310	SFP+ Module(1310nm,220m,LC)
SFP-XG-SX-MM850-A	SFP+ Module(850nm,300m,LC)
SFP-XG-LX-SM1310	SFP+ Module(1310nm,10km,LC)
SFP-XG-LH40-SM1550	SFP+ Module(1550nm,40km,LC)
Servicios	
SV-PS-SES-OS	Oversea Security Expert Service

The Leader in Digital Solutions

New H3C Technologies Co., Limited

Sede Beijing

Torre 1, Centro LSH, Calle Sur de Guangshun 8, Chaoyang Distrito, Pekín, China.

Traduce al español. Zip: 100102

Sede Hangzhou

No.466 Calle Changhe, Distrito de Binjiang, Hangzhou, Zhejiang.

China

Traduce al español. Zip: 310052

Derechos reservados ©2021 New H3C Technologies Co., Limited

Descargo de responsabilidad: Aunque H3C se esfuerza por proporcionar información precisa en este documento, no podemos garantizar que los detalles no contengan errores técnicos o de impresión. Por lo tanto, H3C no puede aceptar responsabilidad por cualquier inexactitud en este documento.

H3C se reserva el derecho de modificar los contenidos aquí sin previo aviso.