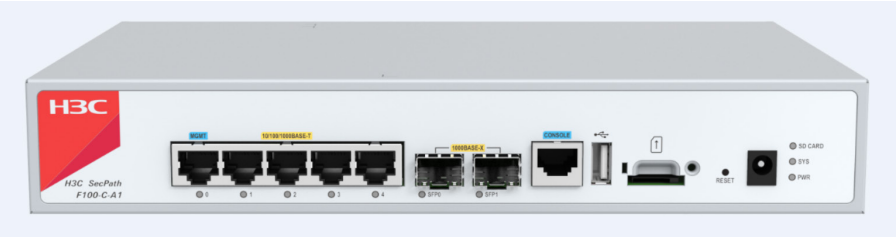
H3C SecPath F100-C-A1 y F100-C-A2 Next - La nueva generación de firewalls

Resumen del producto

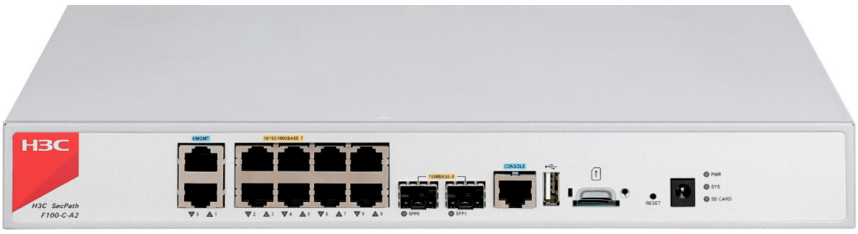
Los firewalls H3C SecPath F100-C-A1 y F100-C-A2 son firewalls de alto rendimiento de próxima generación diseñados para pequeñas y medianas empresas, puntos de salida de redes de campus y sucursales de WAN. Cumple con las demandas de la era Web 2.0 y se alinea con la tendencia tecnológica de seguridad profunda e integración de red.

Los modelos H3C SecPath F100-C-A1 y F100-C-A2 incorporan un sistema de protección de seguridad multidimensional capaz de efectuar un control de acceso de seguridad integrado de IPS, AV, DLP y otros tipos de tráfico desde diversas dimensiones, como son el usuario, la aplicación, el tiempo y la tupla de cinco.

Soporta múltiples servicios VPN, incluyendo L2TP VPN, GRE VPN, IPsec VPN y SSL VPN. Pueden cooperar con puntos finales inteligentes para facilitar el servicio de oficina móvil. Ofrecen capacidades de enrutamiento robustas y admiten los protocolos de enrutamiento RIP, OSPF y BGP y el enrutamiento basado en políticas basado en aplicaciones y URL. Además, estas firewalls ofrecen una protección integral de seguridad para redes IPv4 e IPv6.



Firewall H3C SecPath F100-C-A1



Firewall H3C SecPath F100-C-A2

Características y ventajas

Plataformas de procesamiento de software y hardware de alto rendimiento

Usa procesadores de alto rendimiento multinúcleo y 64 bits avanzados y cachés.

Excelente disponibilidad con respecto a operadores

- Se sirven de plataformas de software y hardware de alta disponibilidad y pertenecientes a H3C cuya eficacia está probada tanto por operadores de telecomunicaciones como por pequeñas y medianas empresas.
- Son compatibles con la tecnología H3C SCF, capaz de virtualizar varios dispositivos en uno solo para propiciar la gestión unificada de recursos, la realización de copias de seguridad de servicios y la mejora del rendimiento del sistema.

Funciones de protección de seguridad de gran potencia

- Protección contra ataques: Detecta y previene varios ataques, incluyendo Land, Smurf, Fraggle, ping de la muerte, tear drop, IP spoofing, IP fragment, ARP spoofing, reverse ARP lookup, invalid TCP flag, large ICMP packet, escaneo de IP/puerto, y ataques comunes de DDoS como SYN flood, UDP flood, DNS flood e ICMP flood.
- Zona de seguridad: permite al usuario la configuración de zonas de seguridad en función de las interfaces y las VLAN.
- Filtrado de paquetes: permite aplicar ACL estándar o avanzada entre zonas de seguridad para filtrar paquetes según la información contenida en ellos, como números de puerto UDP y TCP También permite configurar los intervalos de tiempo durante los cuales se lleva a cabo el filtrado de paquetes.
- Control de acceso: permite ejercer un control de acceso determinado por los usuarios y las aplicaciones e integra funciones de prevención exhaustiva de intrusiones con el control de acceso.
- ASPF: comprueba la información y el estado del protocolo de la capa de aplicación para determinar de forma dinámica si se debe reenviar o anular un paquete. La función ASPF permite la inspección de FTP, HTTP, SMTP, RTSP y otros protocolos de capa de aplicación de TCP y UDP.
- AAA: compatible con la autenticación mediante funciones Local, RADIUS/HWTACACS+, CHAP y PAP.
- Lista negra: Soporta lista de denegación estática y lista de denegación dinámica.
- NAT y VRF-aware NAT.
- VPN: admite las VPN L2TP, IPsec/IKE, GRE y SSL. Así pues, permite la conexión de dispositivos inteligentes a las redes VPN.
- Enrutamiento: permite funcionalidades de enrutamiento, como enrutamiento estático, RIP, OSPF, BGP, directivas de enrutamiento y enrutamiento basado en aplicaciones, URL y directivas.
- Registros de seguridad: compatible con registros de operaciones, registros de coincidencias de directivas por pares de zonas, registros de protección contra ataques, registros DS-LITE y registros NAT444.
- Monitorización, cómputo y gestión de tráfico.

Seguridad DPI flexible, ampliable, integrada y avanzada

- Plataforma de procesamiento de servicios de seguridad integrados: Integra altamente las medidas de protección de seguridad básicas y avanzadas en una plataforma de seguridad.
- Identificación y gestión del tráfico de la capa de aplicación.

- Emplea tecnologías de inspección de máquinas de estado e intercambio de tráfico con el objetivo de detectar el tráfico de aplicaciones P2P, de mensajería instantánea, de juegos en red, de bolsa, de vídeo en la red y de multimedia en la red, como Thunder, Web Thunder, BitTorrent, eMule, eDonkey, QQ, MSN y PPLive.
- Se sirve de una tecnología de inspección exhaustiva para identificar con gran precisión el tráfico P2P y brinda múltiples políticas concebidas para controlar y gestionar el tráfico P2P de una forma flexible.

- Motor de inspección de intrusiones de gran precisión y eficacia: emplea el motor FIRST (inspecciones completas con rigurosas pruebas de estado) de H3C y diversas tecnologías de inspección de intrusiones muy precisas y basadas en los estados de las aplicaciones. El motor FIRST es compatible, además, con la inspección simultánea de software y hardware para proporcionar resultados mucho más eficaces.
- Protección contra virus en tiempo real: utiliza un motor antivirus basado en flujos para prevenir, detectar y eliminar códigos maliciosos presentes en el tráfico de red.
- Filtrado rápido y categorizado de URL: proporciona una lista de denegación y una lista de permisos básica para filtrar URL y te permite consultar el servidor de filtrado de categorías en línea.
- Base de datos de firmas de seguridad completa y actualizada: H3C cuenta con un equipo senior dedicado a las bases de datos de firmas y laboratorios profesionales de protección frente a ataques capaces de proporcionar bases de datos de firmas precisas y actualizadas.

Funciones IPv6 a la vanguardia del sector

- Firewall de estado IPv6.
- Protección frente a ataques IPv6.
- Reenvío de datos, enrutamiento estático y dinámico IPv6 y multidifusión IPv6.
- Tecnologías de transición a IPv6, como tunelización GRE de IPv6 sobre IPv4, tunelización manual, tunelización 6to4, tunelización IPv6 automático compatible con IPv4, tunelización ISATAP, NAT444 y DS-Lite.
- IPv6 ACL y RADIUS.

Funcionalidad para múltiples servicios de nueva generación

- Función de equilibrio de carga de enlaces integrada: emplea tecnologías de inspección de estado de enlaces y de detección de ocupación de enlaces y aplica los resultados en los puntos de salida para equilibrar el tráfico entre enlaces.
- VPN SSL integrada: se sirve de tecnologías como USB-Key, mensajes SMS y el sistema de autenticación existente en la empresa para autentificar a los usuarios, por lo que permite accesos seguros de los usuarios móviles a la red de la empresa.
- Sistema de prevención de pérdida de datos (DLP): permite el filtrado de correos electrónicos por dirección de correo SMTP, sujeto, archivo adjunto y contenido; el filtrado de archivos FTP y el filtrado de capas de aplicaciones (incluidos bloqueo Java/ActiveX y prevención de ataques de inyección SQL).

Función inalámbrica AC

- Soporta un máximo de 64 APs, con un rango recomendado de 16 a 32 APs. Permite configuración automática y

plug-and-play, así como gestión unificada, configuración y actualizaciones para AP inalámbricos.

- Ofrece tecnología de autenticación integral para puntos finales inalámbricos, compatible con la autenticación 802.1X/MAC/Portal.

Gestión inteligente

- Gestión inteligente de políticas de seguridad: detecta políticas duplicadas, optimiza las reglas de concordancia y detecta y sugiere políticas de seguridad generadas en la red interna de forma dinámica.
- SNMPv3: compatible con SNMPv1 y SNMPv2.
- Configuración y gestión basada en CLI a través del puerto de consola.
- Gestión en la web a través de una interfaz de usuario gráfica sencilla e intuitiva.
- Gestión unificada H3C IMC SSM: permite la recolección y el análisis de información de seguridad para ofrecer, de forma intuitiva, datos sobre las condiciones de la red y de seguridad. Gracias a ello, es posible ahorrar esfuerzos de gestión y mejorar en gran medida su eficacia.
- Gestión de registros centralizada y basada en una avanzada tecnología de desglose y análisis de datos: solicita y recibe información para generar y compilar diferentes tipos de registros (como syslogs y registros de flujo binario) en el mismo formato. Al mismo tiempo, presenta una buena capacidad para comprimir y almacenar grandes cantidades de registro. El usuario puede cifrar y exportar los registros almacenados a dispositivos de almacenamiento externos, como DAS, NAS y SAN, para prevenir la pérdida de registros de seguridad de importancia.
- Informes muy abundantes: incluye informes basados en aplicaciones e informes de análisis de flujos.
- Exportación de informes en diversos formatos: entre los que destacan PDF, HTML, word y txt.
- Personalización de informes a través de la interfaz web: el usuario puede personalizar el intervalo de tiempo, el dispositivo de origen de los datos, el período de generación de los informes y el formato de exportación.
- Actualización de software en servicio (ISSU): las actualizaciones de software requieren un tiempo mínimo de inactividad.
- Paginación de registros: divide los archivos BSL, ATK y CFGLOG en cinco tipos de archivos de registro. El firewall permite la paginación de registros en backend, la limpieza y la especificación de parámetros de registro, la consulta de la paginación y la configuración de registros para un módulo independiente.
- Plataforma Cloudnet y gestión de APPs.

Especificaciones

Ítem	F100-C-A1	F100-C-A2
Puertos	5 GE + 2 SFP (MTU: 1500 por defecto)	10 GE + 2 SFP
Medios de almacenami	Tarjeta TF con tamaño máximo de 500 GB	

ento	
Temperatura ambiente	Operativa: 0 °C a 45 °C (32 °F a 113 °F) Almacenamiento: -40°C a +70°C (-40°F a +158°F)
Modo de funcionamiento	Ruta, transparente e híbrido
AAA	Autenticación de Portal Autenticación RADIUS Autenticación HWTACACS Autenticación PKI/CA (formato X.509) Autenticación de dominio Autenticación CHAP Autenticación PAP
Firewall	Tecnología de firewall virtual SOP compatible con la virtualización completa de los recursos de hardware, incluidos la CPU, las memorias y el almacenamiento Zona de seguridad Protección frente a ataques maliciosos, como land, smurf, fraggle, ping de la muerte, teardrop, suplantación de IP, fragmentación IP, suplantación de ARP, búsqueda de ARP inversa, bandera TCP inválida, paquete ICMP, escaneo de direcciones y puertos, inundación SYN, inundación ICMP, inundación UDP e inundación DNS. ACL básicas y avanzadas ACL basada en intervalo de tiempo Control de acceso basado en usuarios y aplicaciones Filtrado de paquetes para la capa de aplicación ASPF Listas negras estáticas y dinámicas Enlace MAC-IP ACL basada en MAC Transmisión transparente de VLAN 802.1Q Sub-Interfaz VLAN
Antivirus	Detección de virus basada en firmas Actualizaciones manuales y automáticas de la base de datos de firmas Procesamiento basado en flujos Detección de virus basada en HTTP, FTP, SMTP y POP3 Entre los virus detectables se encuentran las puertas traseras, los gusanos de correo electrónico, los gusanos IM, los gusanos P2P, los troyanos, los AdWare y los virus Reportes e informes de virus

Prevención exhaustiva de intrusiones	Prevención contra ataques comunes, como hackers, gusanos y virus, troyanos, códigos maliciosos, spyware y adware, DoS y DDoS, desbordamientos de búfer, inyecciones SQL y bypass de IDS e IPS Categorías de firmas de ataque (en función de los tipos de ataques y de los sistemas objetivos) y niveles de seguridad (incluidos alto, medio, bajo y notificación) Actualización manual y automática de la base de datos de firmas de ataques (TFTP y HTTP). Identificación y control del tráfico P2P/IM
Filtrado de correos electrónicos /páginas web y capas de aplicación	Filtrado de correos electrónicos Filtrado de direcciones de correo electrónico SMTP Filtrado de sujetos, contenido y archivos adjuntos de correos electrónicos Filtrado de páginas web Filtrado de contenido y URL HTTP Bloqueo de Java Bloqueo de ActiveX Prevención de ataques de inyección de SQL
NAT	Many-to-one NAT: asigna varias direcciones internas a una sola dirección pública Many-to-many NAT: asigna varias direcciones internas a múltiples direcciones públicas One-to-one NAT: asigna una dirección interna a una dirección pública NAT de direcciones de origen y direcciones de destino Acceso de hosts externos a servidores internos Asignación de direcciones internas a direcciones de interfaz públicas Compatibilidad de NAT para DNS Configuración de períodos efectivos de NAT NAT ALG para NAT ALG: incluidos DNS, FTP, H.323, ILS, MSN, NBT, PPTP y SIP
VPN	L2TP VPN VPN IPSec VPN GRE VPN SSL
Servicios IP	Reenvío IP ICMP, Tracert, ping, Telnet, Servidor DHCP, Relay DHCP y Cliente DHCP Enrutamiento: Estático, RIP, OSPF, BGP Multicast: IGMP, PIM-SM y PIM-DM Firewall de estado IPv6 Protección frente a ataques IPv6 Reenvío de IPv6 Protocolos IPv6 como ICMPv6, PMTU, Ping6, DNS6, TraceRT6, Telnet6, cliente DHCPv6 y relé DHCPv6.

	Enrutamiento IPv6: RIPng, OSPFv3, BGP4+, enrutamiento estático, enrutamiento basado en políticas Multidifusión IPv6: PIM-SM, y PIM-DM Técnicas de transición a IPv6: NAT-PT, tunelización IPv6, NAT64 (DNS64) y DS-LITE Seguridad IPv6: NAT-PT, tunelización IPv6, filtro de paquetes IPv6, RADIUS, políticas de pares de zonas IPv6, límites de conexión IPv6
Alta disponibilidad	Conmutación por error de estado RBM activa-activa y activa-pasiva Sincronización de la configuración de dos firewalls Sincronización de estado IKE en la VPN IPsec VRRP
Gestión de configuración	Gestión de configuración CLI a través del puerto de consola. Gestión remota a través de la web, SSH Gestión de dispositivos a través de H3C IMC SSM SNMPv3, compatible con SNMPv2 y SNMPv1 Política de seguridad inteligente
Protección medioambiental	Cumplimiento de la directiva RoHS de la UE

Rendimiento

	F100-C-A1	F100-C-A2
Velocidad del cortafuegos (1518B)	1,2 Gbps	1,2 Gbps
Capa de aplicación de rendimiento	600 Mbps	600 Mbps
IPS rendimiento	600 Mbps	600 Mbps
Protección contra amenazas de paso.	500 Mbps	500 Mbps
túnel IPsec (sitio-a-sitio)	500	500
Rendimiento de IPsec (1400B)	150 Mbps	250 Mbps
Usuarios de VPN SSL	500	500
Rendimiento de SSL VPN	80 Mbps	100 Mbps
Límite de sesiones simultáneas	900 mil	900 mil
Máximo de nuevas conexiones por segundo	8000	8000

Guía de pedidos

Carcasa

PID	Descripción
SecPath F100-C-A1-I.	Firewall H3C SecPath F100-C-A1
SecPath F100-C-A2-I	Firewall H3C SecPath F100-C-A2

Licencia

PID	Descripción
LIS-F100BAS-ACG-1Y	H3C SecPath F100-BAS Licencia de Servicio de Actualización de Firmas de Aplicación, 1 Año
LIS-F100BAS-ACG-3Y	Adquiere la Licencia de Servicio de Actualización de Firma de Aplicación para H3C SecPath F100-BAS por 3 años.
LIS-F100BAS-AV-1Y	H3C SecPath F100-BAS AV Licencia de Servicio de Seguridad Antivirus, 1 Año.
LIS-F100BAS-AV-3Y	H3C SecPath F100-BAS AV Licencia de Servicio de Seguridad Anti-Virus, 3 años
LIS-F100BAS-IPS-1Y	H3C SecPath F100-BAS, licencia de servicio de actualización de firmas de IPS, 1 año
LIS-F100BAS-IPS-3Y	Licencia de Servicio de Actualización de Firmas de IPS H3C SecPath F100-BAS, 3 años.
LIS-F100BAS-IPS/ACG-1Y	H3C SecPath F100-BAS IPS/ACG Licencia de Actualización de Firma de Servicio, 1 Año.
LIS-F100BAS-IPS/ACG-3Y	H3C SecPath F100-BAS IPS/ACG Servicio de Actualización de Firmas de Licencia, 3 años.
LIS-F100BAS-SSL-30	H3C SecPath F100BAS Licencia de VPN SSL para 30 usuarios
LIS-F100BAS-SSL-100	H3C SecPath F100BAS SSL VPN para 100 Usuarios Licencia
LIS-F100-BAS-TI-1Y	Obtén la licencia de actualización de amenazas de seguridad de H3C SecPath F100-BAS por 1 año.
LIS-F100-BAS-TI-3Y	Licencia de Servicio de Actualización de Amenazas de Seguridad para H3C SecPath F100-BAS, 3 años
LIS-F100BAS-URL-1Y	H3C SecPath F100-BAS, licencia de servicio de actualización de firmas de URL, 1 año
LIS-F100BAS-URL-3Y	H3C SecPath F100-BAS Licencia de Servicio de Actualización de Firma de URL,3 Años
LIS-WX-1-BE	Licencia de controlador de acceso mejorado, 1 AP, para verticales, para V7
LIS-WX-4-BE	Licencia de controlador de acceso mejorada, 4 AP, para verticales, para V7
LIS-WX-8-BE	Licencia de controlador de acceso mejorado, 8 AP, para verticales, para V7
LIS-WX-16-BE	Licencia de Controlador de Acceso Mejorado, 16 AP, para Verticales, para V7

Introducción a la Licencia

Licencia	Característica	Antes de la instalación de la licencia	Después de la expiración de la licencia	Punto
LIS-F100B AS-ACG	Reconocimiento de aplicación (APR)	No se admite la actualización de la biblioteca de firmas de APR.	Actualizar la biblioteca de firma APR no es compatible.	1 año 3 años
LIS-F100B AS-AV	Antivirus	No hay disponible antivirus y no se admite la actualización de la biblioteca de firmas de virus.	El antivirus aún está disponible, pero no puedes actualizar la biblioteca de firmas de virus ni usar la consulta en la nube, la inspección mejorada y la función de colaboración de sandbox.	1 año 3 años
LIS-F100-BAS-TI	Inteligencia de amenazas (incluida la reputación de IP, la reputación de URL y la reputación de dominio)	No hay inteligencia de amenazas disponible y no se admite la actualización de la biblioteca de firmas de inteligencia de amenazas	La inteligencia de amenazas sigue estando disponible, pero no se admite la actualización de la biblioteca de firmas de inteligencia de amenazas.	1 año 3 años
LIS-F100B AS-IPS	IPS	IPS no está disponible y no se admite la actualización de la biblioteca de firmas de IPS.	IPS sigue disponible, pero no se admite la actualización de la biblioteca de firmas IPS	1 año 3 años
LIS-F100B AS-SSL	VPN SSL	El sistema soporta solamente el número máximo predeterminado de usuarios de SSL VPN.	N/A	Permanente
LIS-F100B AS-URL	Filtrado de URL	La consulta de URL cloud no está disponible y no se admite la actualización de la biblioteca de firma de URL.	URL nube consulta no disponible y la actualización de la biblioteca de firma URL no es compatible	1 año 3 años

New H3C Technologies Co., Limited

Sede de Hangzhou
310 Calle Liuhe, Parque Científico Zhijiang, Hangzhou,
República Popular China.
Código postal: 310053
Tfno: 0571-86760000
Fax: 0571-86760001
Versión: 20150108-V1.0

Copyright ©2020 New H3C Technologies Co., Limited Reserva todos los derechos
Descargo de responsabilidad: Si bien H3C se esfuerza por proporcionar información lo más veraz posible en este documento, es imposible garantizar que ninguno de los detalles contenga algún tipo de error técnico o de impresión. Por consiguiente, H3C no asume ningún tipo de responsabilidad derivada de la precisión del contenido de este material.
H3C se reserva el derecho de modificar el contenido del presente documento sin necesidad de previo aviso.

http://www.h3c.com