H3C WSG1840X Puerta de enlace Multiservicio Inalámbrica Integrada

New H3C Technologies Co., Limited

H3C WSG1840X Puerta de enlace Multiservicio Inalámbrica Integrada

Visión general

El H3C WSG1840X Wireless Integrated Multi-Service Gateway está bien diseñado y posicionado para redes SMB. Tiene gateway, seguridad y funciones de AC integradas, reduciendo el número de dispositivos y TCO en la red. Adopta la innovadora plataforma Comware V7 (denominada V7 de aquí en adelante). V7 viene con el estándar de gestión de control de usuario granular, gestión integral de recursos de RF, control de seguridad inalámbrica 7x24, roaming rápido de capa 2 y capa 3, QoS fuerte y pila dual IPv4/IPv6. Agrega en varias novelas tecnologías inalámbricas como control de plano multi-core, Bonjour y Hotspot 2.0. También soporta múltiples configuraciones de red como la gestión en la nube. Cuando se combina con los AP de H3C para pymes (consultar la información de pedido para más detalles), sirve como una solución ideal de control de acceso para el acceso WLAN de la red de una pequeña y mediana empresa.

WSG1840X

Características

Licencia Todo Incluido para AP

El Gateway Multi-Servicio Integrado Inalámbrico WSG1840X incluye la licencia de AP de forma predeterminada, lo cual protege la inversión del cliente al máximo y también brinda a las PYMES una gran oportunidad de agregar nuevos AP con la expansión de la red inalámbrica sin costo adicional. El número de licencias llega hasta 128, y 64 licencias están incluidas por defecto. Que significa WSG1840X puede gestionar 64 AP ordinarios o 128 AP de pared por defecto. Compra una licencia adicional para ampliar el número de AP ordinarios. <Versión soportada desde WSG1800X-CMW710-E5623>

modelo	Licencia AP por defecto
WSG1840X	64

AC Modelo	Máx. Cant. PA		Licencia	
	WA6120/WA6126/WA6120X	WA6120H	Defecto	Añádelo
WX1840X	128	0	64	64
	0	128	64	0
	64	64	64	32

Todo en uno Gateway

El WSG1840X Wireless Integrated Multi-Service Gateway integra funciones de puerta de enlace, seguridad y AC en una sola caja, lo cual es perfecto para entornos SOHO, SMB y SME. WSG1840X soporta todas las características del controlador empresarial, además, WSG1840X soporta la función de gateway, como PPPOE, NAT, dirección IP dinámica y función de configuración de dirección IP estática.

802.11ax Gestión de AP

Además del manejo de AP 802.11a/b/g/ac, el WSG1840X puede trabajar junto con los APs SMB basados en 802.11ax de H3C (ver información de pedido para más detalles) para proporcionar una velocidad de acceso inalámbrico varias veces más rápida que una red tradicional 802.11a/b/g/ac.

Modos de reenvío flexibles

En una red inalámbrica en modo de reenvío centralizado, todo el tráfico inalámbrico se envía a un AC para su procesamiento, lo cual puede convertirse en un cuello de botella. Especialmente en redes inalámbricas donde se despliegan AP en las sucursales, AC en la sede central y se conectan AP y AC a través de una WAN. En este escenario, el reenvío distribuido es más adecuado. El WSG1840X soporta tanto modos de reenvío distribuido como modo de reenvío centralizado y puede configurar el reenvío basado en SSID según sea necesario.

Funcionalidades de Roaming Inteligente

- Soporte roaming intra-AC, roaming cross-AC y roaming Layer 3 cross-VLAN.
- Función de sincronización de información de roaming del portal. AC y AP soportan el roaming no percibido de los usuarios del Portal entre AC en una red a gran escala, sin el servidor de activación mac del Portal. El controlador inalámbrico puede asumir de forma independiente la función de servidor mac-trigger. Reduce la presión en el servidor del portal y evita que se convierta en un cuello de botella de rendimiento. Cuando el servidor Portal está hecho, el terminal en línea aún puede moverse sin autenticación entre no menos de 10 controladores inalámbricos.
- Función de sincronización de información de roaming 802.1X. AC y AP admiten usuarios 802.1X

para una rápida itinerancia entre AC en una red a gran escala. Soporte autenticación dot1x para roaming rápido entre ACs. Los terminales no necesitan autenticarse de nuevo después de cambiar a un nuevo controlador de acceso. Alivia la presión del servidor y asegura un acceso rápido de los terminales, y apoya la rápida itinerancia entre más de 10 ACs.

- Soporte para los protocolos de roaming rápido 802.11k/v/r

Cambia de canal inteligentemente

- En una WLAN, los AP inalámbricos adyacentes deben trabajar en diferentes canales para evitar la interferencia de canal. Sin embargo, los canales son recursos muy escasos para una WLAN. Hay un pequeño número de canales no superpuestos para los APs. Por ejemplo, utiliza sólo tres canales no superpuestos para la red de 2.4GHz. Por lo tanto, la clave de las aplicaciones inalámbricas es cómo asignar canales para los AP de manera inteligente.
- Mientras tanto, hay muchas posibles fuentes de interferencia que pueden afectar la operación normal de los AP en una WLAN, como AP falsos, radares y hornos de microondas. La técnica de cambio de canal inteligente puede asegurar la asignación de un canal óptimo a cada AP, minimizando así la interferencia de canales adyacentes. Además, la función de detección de interferencias en tiempo real puede ayudar a mantener los AP lejos de fuentes de interferencias como radares y hornos de microondas.

Comparte la carga de AP de manera inteligente

- Según IEEE 802.11, los clientes inalámbricos controlan la itinerancia inalámbrica en las WLAN. Usualmente, el cliente inalámbrico elige un AP basado en la Indicación de Fuerza de Señal Recibida (RSSI). Por lo tanto, muchos clientes eligen el mismo AP con un alto RSSI. Como estos clientes comparten el mismo medio inalámbrico, reduce mucho el rendimiento de cada cliente.
- La función de carga inteligente de AP puede analizar las ubicaciones de los clientes inalámbricos en tiempo real, determinar dinámicamente qué AP en la ubicación actual puede compartir carga entre sí, e implementar el intercambio de carga entre estos APs. Además de compartir carga basado en el número de sesiones en línea, el sistema también soporta compartir carga basado en el tráfico de usuarios inalámbricos en línea.
- Soporte la función de ocultación automática de SSID basada en la utilización de recursos de radio. Cuando los recursos de radio alcanzan o superan el umbral configurado, el SSID se oculta automáticamente para proporcionarte servicios inalámbricos estables y confiables.

Inspección de paquetes profunda de la capa 4-7

El WSG1840X puede identificar una variedad de aplicaciones y se puede implementar el control de políticas, incluyendo ajuste de prioridad, programación, bloqueo y limitación de velocidad para garantizar un uso eficiente de los recursos de ancho de banda y mejorar la calidad de la red.

Implementa sistemas de detección y prevención de intrusos inalámbricos en la capa 7 (WIDS / WIPS).

- El WSG1840X admite la lista negra, la lista blanca, la defensa contra dispositivos no autorizados, la detección de paquetes corruptos, la eliminación de usuarios ilegales, la detección de ataques en la capa MAC con firma actualizable (ataques DoS, ataques de inundación o ataques de intermediario) y las medidas de contramedida.
- Con la base de conocimientos incorporada en WSG1840X, realiza decisiones de seguridad inalámbrica oportunas y precisas. Realiza monitorización de ubicación física visible y desconecta el puerto físico para fuentes de ataque determinadas, como puntos de acceso o terminales rogue.
- Con el dispositivo H3C firewall/IPS, la infraestructura de red también puede implementar defensa de seguridad de capa 7 en el campus inalámbrico, cubriendo conexiones seguras por cable (802.11) e inalámbricas (802.3) de extremo a extremo.

Protege tu red de forma completa

La rica biblioteca de funciones puede completar la detección de virus populares. Apoya a anti-virus para botnets, troyanos y gusanos. Puede identificar más de 1500 aplicaciones de alto perfil. Con tecnología de prevención de ataques avanzada, soporta tanto IPv4 como IPv6. Puede proporcionar protección efectiva contra los siguientes ataques:
1) Ataques anormales de paquetes (como banderas ilegales de paquetes TCP, Land, smurf, WinNuke, Ping de la muerte, tráfico ICMP grande / fragmento pequeño, etc.).
2) Ataques de suplantación de dirección (como ataques de dirección IP, ataques de puerto, etc.).
3) Ataques de tráfico anormal (como Ack Flood, DNS Flood, Fin Flood, HTTP Flood, HTTPS Flood, ICMP Flood, ICMPV6 Flood, SYNACK Flood, SYN Flood, UDP Flood, etc.).

- Zona de seguridad: Permite configurar áreas de seguridad según las interfaces y VLANs.
- Filtrado de paquetes: Aplica ACL estándar o avanzado entre zonas de seguridad para filtrar paquetes basados en la información contenida en ellos, como los números de puerto UDP y TCP. También puedes configurar rangos de tiempo en los que se realizará el filtrado de paquetes.

- Soporte de control de acceso: admite el control de acceso basado en los usuarios y aplicaciones e integra la prevención de intrusiones profunda con el control de acceso.
- Determina dinámicamente si reenviar o descartar un paquete mediante la verificación de su información de protocolo de capa de aplicación y estado. ASPF admite inspeccionar los protocolos de capa de aplicación basados en TCP/UDP, como FTP, HTTP, SMTP, RTSP y otros.
- AAA - Compatible con autenticación basada en RADIUS/HWTACACS+, CHAP y PAP.
- Lista negra—Soporta lista negra estática y lista negra dinámica.
- NAT y NAT con conciencia de VRF.
- 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.
- Routing-- Soporta enrutamiento estático, RIP, OSPF, BGP, políticas de enrutamiento y enrutamiento basado en políticas basado en aplicaciones y URL.
- Monitoreo de tráfico, estadísticas y gestión.

Próxima generación de características multi-servicio.

- Función de equilibrio de carga de enlaces integrados: utiliza tecnologías de inspección del estado del enlace y detección de ocupación del enlace, y se aplica a una salida de red para equilibrar el tráfico entre los enlaces.
- Característica de VPN SSL integrada: proporciona acceso seguro de usuarios móviles a la red empresarial.

Flexible y extensible, integrada y avanzada seguridad de DPI

- Integra las medidas de protección básicas y avanzadas en una plataforma de seguridad.
- Identificación y gestión del tráfico de capa de aplicación: utiliza tecnologías de máquina de estado e inspección de intercambio de tráfico para detectar el tráfico de aplicaciones P2P, mensajería instantánea, juegos en red, acciones, video en red y aplicaciones multimedia en red. Utiliza la tecnología de inspección profunda para identificar el tráfico P2P de manera precisa y proporciona varias políticas para controlar y administrar el tráfico P2P de manera flexible.
- Categorización filtrado de URLs masivas - Utiliza el modo local + nube para proporcionar una lista negra y 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 datos de firmas precisa y actualizada.

Especificaciones de hardware

Artículo	WSG1840X
Dimensiones (ancho × profundidad × altura)	440×165×43.6mm
Peso	1.8kg
Rendimiento inalámbrico	4Gbps
Puerto	LAN: 1*SFP Plus + 4*GE + 1*5GE WAN: 2 GE + 1*USB
Fuentes de alimentación	100V AC to 240V AC:50/60Hz
Operar y almacenar temperatura	0ºC a 45ºC / -40ºC a 70ºC
Operar y almacenar humedad relativa	5% a 95%
Cumplimiento de seguridad	UL 60950-1 CAN/CSA C22.2 No 60950-1 IEC 60950-1 EN 60950-1/A11 AS/NZS 60950 EN 60825-1 EN 60825-2 EN60601-1-2 FDA 21 CFR Subchapter J
EMC	ETSI EN 300 386 V1.3.3:2005 EN 55024: 1998+ A1: 2001 + A2: 2003 EN 55022 :2006 VCCI V-3:2007 ICES-003:2004

	EN 61000-3-2:2000+A1:2001+A2:2005 EN 61000-3-3:1995+A1:2001+A2:2005 AS/NZS CISPR 22:2004 FCC PART 15:2005 GB 9254:1998 GB/T 17618:1998
MTBF	≥50000 horas

Especificaciones del software

Artículo	Característica	WSG1840X
Funciones básicas.	Número de AP gestionados por defecto	64 AP ordinarios o 128 AP de placa de pared.
	Máximo número de APs gestionados	128
	Máximo usuarios de autenticación	2048
802.11MAC	Protocolos 802.11	√
	El número de SSID de toda la máquina.	128
	Oculta el SSID.	√
	Protege con 11G.	√
	11n solamente	√
	Usa los límites de números.	Soportado Basado en SSID, por RF basao.
	Mantén vivo	√
	Inactivo	√
	Asigna códigos de múltiples países	√
	Aislamiento de usuarios inalámbricos	Soportado Usuarios inalámbricos basados en VLAN aislamiento de 2 capas Separa a los usuarios inalámbricos basados en el SSID en 2 capas
	20MHz/40MHz auto-switch en modo 40MHz	√

	Reenviar localmente	Reenvío local basado en SSID+VLAN
CAPWAP	Registro automático de AP	√
	Descubrimiento de AC (opción43 DHCP, DNS)	√
	Túnel IPv6	√
	Sincroniza el reloj.	√
	Reenvía el texto fuente intacto: Jumbo frame forwarding.	√
	Asigna los parámetros básicos de la red de AP a través del AC.	Soportado IP estática, VLAN, dirección AC conectada
	Conexión L2/L3 entre AP y AC	√
	Traverse NAT entre AP y AC	√
Roaming	Interconecta L2 y L3 intra-AC, inter-AP.	√
	Inter-AC, Inter-AP L2 y L3 roaming	√
Características de GW	NAT	√
	PPPoE	√
	DDNS	√
	VPN SSL	√
	IPsec VPN	√
	RIP	√
	GRE	√
Acceso control	Abrir sistema, Clave compartida	√
	WEP-64/128, WEP dinámica	√
	WPA,WPA2,WPA3	√
	TKIP.	√
	CCMP	√ (recomendado 11n)
	SSH v1.5/v2.0	√
	Autenticación del portal	Soportado Autenticación remota, servidor externo.

	Redirección de la página del portal	Soportado SSID basado, página de portal de AP empuje
	Portal by-pass Proxy	√
	802.1x autenticación	EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-MD5, EAP-SIM, LEAP, EAP-FAST, EAP offload (solo TLS, PEAP)
	Autenticación local	802.1X, Portal, autenticación MAC
	Autenticación LDAP.	Utiliza el term base proporcionado y traduce: 802.1X y Portal. EAP-GTC y EAP-TLS admitidos por el inicio de sesión 802.1X.
	Ubicación AP control de acceso de usuarios	√
	Acceso de Invitados	√
	Canal VIP	√
	Detecta ataques ARP.	Soportado Inalámbrico SAVI
	SSID anti-spoofing	Vincula SSID y nombre de usuario.
	Selecciona el servidor AAA basado en el SSID y el dominio.	√
	Respaldar el servidor AAA.	√
	Servidor AAA local para usuarios inalámbricos	√
	TACACS+.	√
QoS	Mapeo de prioridad	√
	Filtra y clasifica los paquetes de nivel 2 a nivel 4.	√
	Límite de tasa	Apoya con una granularidad de 8Kbps
	802.11e/WMM	√
	Control de acceso basado en el perfil del usuario.	√
	Límite de ancho de banda inteligente (algoritmo de igual compartición de	√

	ancho de banda)	
	Limite inteligente de ancho de banda (específico de usuario)	√
	Inteligente garantía de ancho de banda.	Soportado Flujo libre para paquetes provenientes de cada SSID. Cuando el tráfico no está congestionado, y garantiza un ancho de banda mínimo para cada SSID cuando el tráfico está congestionado.
	Optimiza la QoS para el teléfono SVP.	√
	CAC (Control de Admisión de Llamadas)	Basado en el número de usuario/ancho de banda.
	Fin a fin de la calidad de servicio (QoS)	√
	Límite de velocidad de carga AP.	√
Gestión de la RF	Código de país bloquear	√
	Configura el canal estático y la potencia	√
	Configura el canal y la potencia automaticamente.	√
	Ajusta la tasa de transmisión automática.	√
	Detecta y corrige los agujeros de cobertura.	√
	Balanceo de carga.	Basado en el tráfico, el usuario y la frecuencia (compatible con doble frecuencia)
	Equilibrio de carga inteligente	√
	Grupo de balanceo de carga de AP	Soportado: auto-descubrimiento y configuración flexible.
Seguridad	Lista negra estática	√
	Lista negra dinámica	√
	Lista blanca.	√
	Detecta APs intrusos	Soportado SSID basado, BSSID, OUI del dispositivo

	Medida para contrarrestar AP falsos	√
	Detecta ataques de inundación.	√
	Detecta ataques de suplantación	√
	Detectar ataques de IV débiles.	√
	WIPS/WIDS	Soportado Seguridad móvil de 7 capas
Protocolo de Capa 2	ARP (ARP gratuito)	√
	802.1p	√
	802.1q	√ (Máximo de VLANs: 4094)
	802.1x	√
Protocolo IP	Protocolo IPv4	√
	IPv6 nativo.	√
	IPv6 SAVI	√
	Portal de IPv6	√
Multicast	MLD Snooping	√
	IGMP Snooping	√
	Grupo de multidifusión	256
	Multicasta a unicast (IPv4, IPv6)	Soportado Establece límite unicast basado en el entorno operativo.
Redundancia	1+1 conmutación entre ACs.	√
	Comparte inteligente de APs entre ACs.	√
	AP Remota	√
Gestiona y despliega.	Gestiona la red	WEB, SNMP v1/v2/v3, RMON.
	Despliega la red.	WEB, CLI, Telnet, FTP
Característic as verdes	Apaga programado de la interfaz inalámbrica del AP.	√
	Cierre programado del servicio inalámbrico	√
	Ajusta la potencia por paquete (APP)	√
WLAN	RF Ping	√

Aplicación	Análisis de la sonda remota	√
	Ajustar equidad de reenvío de paquetes	√
	Supresión de reenvío de paquetes 802.11n	√
	Acceso basado en la modelación de tráfico	√
	Comparte el canal Co-AP	√
	Reutiliza el canal Co-AP.	√
	Ajusta el algoritmo de tasa de transmisión de la interfaz RF.	√
	Descarta el paquete inalámbrico con señal débil.	√
	Deshabilita el acceso de usuario con señal débil.	√
	Desactiva la caché de paquetes multicast.	√
	Estado parpadeo (limitado a algunos AP)	√
Nuevas características añadidas	Reenvía la política.	√
	VLAN pool	√
	Pasarela Bonjour	√
	802.11w	√
	802.11k,v,r	√
	Hotspot2.0 (802.11u)	√
	NAT	√
	VPN	√
Cortafuegos	Protección contra ataques maliciosos como land, smurf, fraggle, ping de la muerte, teardrop, IP spoofing, fragmentación de IP, ARP spoofing, búsqueda inversa de ARP, bandera	√

	TCP inválida, paquete ICMP grande, escaneo de dirección/puerto, inundación SYN, inundación ICMP, inundación UDP y DNS query flood.	
	Filtra los paquetes de la capa de aplicación de ASPF.	√
	Básica y avanzada ACLs	√
	ACL basada en rango de tiempo	√
	Basado en usuarios y aplicaciones control de acceso	√
	Función de lista negra estática y dinámica	√
	Ligadura MAC-IP	√
	Basado en MAC ACL	√
Antivirus	Detéctalo por firmas de virus.	√
	Manual y automática actualización para la base de datos de firmas	√
	Procesamiento basado en stream	√
	Detéctalo Virus basado en HTTP, FTP, SMTP y POP3.	√
	Tipos de virus incluyen Backdoor, Email-Worm, IM-Worm, P2P-Worm, Trojan, AdWare y Virus.	√
	Registros y reportes de virus	√
	Detéctalo por firmas de virus.	√
Prevención profunda de intrusión.	Prevención contra ataques comunes como hacker, gusano/virus, Troyano, código malicioso, spyware/adware, DoS/DDoS, desbordamiento de búfer, inyección SQL y bypass de IDS/IPS.	√
	Categorías de firmas de ataque (basadas en tipos de ataque y sistemas objetivo) y niveles de	√

	gravedad (que incluyen alta, media, baja y notificación)	
	Actualiza manual o automáticamente la base de datos de firmas de ataque (TFTP y HTTP).	√
	Identificación y control de tráfico P2P/IM.	√
Filtrar capa de correo electrónico/ página web/aplicación	Filtrado de Correo Electrónico	√
	Filtrar direcciones de correo electrónico SMTP	√
	Filtrar el asunto/contenido/archivo adjunto del correo electrónico.	√
	Filtración de páginas web	√
	Filtra el contenido de la URL HTTP.	√
	Bloqueo de Java.	√
	Bloquea ActiveX	√
	Prevención de ataques de inyección SQL.	√
VPN	L2TP VPN	√
	IPsec VPN	√
	GRE VPN	√
	VPN SSL	√
NAT	Muchos a uno NAT, que asigna múltiples direcciones internas a una sola dirección pública	√
	Muchos a muchos NAT, que asigna múltiples direcciones internas a múltiples direcciones públicas.	√
	Uno a uno NAT, que mapea una dirección interna a una dirección pública.	√
	NAT de la dirección de origen y de la dirección de destino	√

	Acceso de los hosts externos a los servidores internos.	√
	Mapea la dirección interna a la 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	√

Información de pedido:

ID de producto	Descripción del producto
EWP-WSG1840X	H3C WSG1840X 8-Port (6*1000BASE-T, 1*5GE-T, and 1*SFP Plus) Wireless Integrated Services Gateway
LIS-WX-1-SME-OVS	H3C SME-OVS Access Controller 1-AP License
LIS-WX-4-SME-OVS	H3C SME-OVS Access Controller 4-AP License
LIS-WX-8-SME-OVS	H3C SME-OVS Access Controller 8-AP License
LIS-WX-16-SME-OVS	H3C SME-OVS Access Controller 16-AP License
Comentarios	Descripción
Apoya a los AP de SMB.	WA6120/WA6126/WA6120X/WA6120H

The Leader in Digital Solutions

New H3C Technologies Co., Limited

Sede de Beijing

Torre 1, Centro LSH, 8 Calle Guangshun Sur, Chaoyang Distrito, Beijing, China

Código postal: 100.102

Sede Hangzhou

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

China

Código postal: 310.052