

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES PARA LA ADQUISICIÓN DE PUNTOS DE ACCESO WIFI Y SUS LICENCIAS, CON DESTINO A CENTROS EDUCATIVOS PÚBLICOS PERTENECIENTES AL GOBIERNO DE NAVARRA

1.- OBJETO Y AMBITO

La Dirección General de Universidades y Recursos Educativos desea implantar y actualizar el sistema wifi en determinados Centros Educativos Públicos pertenecientes al Gobierno de Navarra.

Para todo ello se abre el presente proceso de licitación, que incluye lo siguiente:

- Suministro de equipamiento Wifi consistente en puntos de acceso (APs) con controladora embebida en los mismos y kits de montaje.
- Suministro de licencias para el funcionamiento de los elementos anteriores con soporte mínimo de cinco años (sin coste adicional).

Por tanto, quedan expresamente excluidos de este procedimiento los trabajos de configuración e instalación de los equipos suministrados.

2.- PRESCRIPCIONES TÉCNICAS

A continuación, se presenta un resumen de prescripciones técnicas que han de cumplir las ofertas presentadas.

Aquellas ofertas que presenten equipos que no cumplan las especificaciones mínimas indicadas en este apartado serán objeto de exclusión del procedimiento de licitación.

Igualmente será motivo de exclusión la falta de justificación adecuada del cumplimiento de los requerimientos solicitados.

2.1 - Características de las controladoras embebidas en los AP

- Todas las funcionalidades solicitadas a continuación deberán estar activas durante los 5 años de duración del presente contrato, por lo que se consideran incluidas en el precio de cada controlador todas las licencias necesarias para ello. Todas las funcionalidades de controladora residirán dentro de los puntos de acceso sin límite en cuanto a las funcionalidades indicadas. Este tipo de configuración permitirá mantener un punto central de administración y control.
- El controlador virtual podrá realizar la gestión de todos los puntos de acceso y será totalmente escalable añadiendo los equipos necesarios sin necesidad de coste de licencias adicionales. Los APs podrán agruparse y gestionarse en “colmenas” donde se podrán mezclar puntos de acceso de diferentes tipos (11n, 11ac, 2x2 MIMO, 3x3, etc...)
- No se admitirán soluciones con algún tipo de recurso en cloud.

2.2 - Gestión de recursos radio

Características Mínimas

- Debe gestionar automática y dinámicamente la frecuencia y potencia a la que deben trabajar los puntos de acceso para optimizar la cobertura existente y rendimiento de los clientes inalámbricos. Este control deberá tomar en cuenta no sólo las fuentes de interferencia WiFi, sino también las no-WiFi.
- Debe ser capaz de gestionar el acceso de los clientes a la red WIFI de forma que sea capaz de garantizar un acceso equilibrado en el tiempo o acceso preferencial. De esta manera se evita que los clientes lentos degraden en exceso el rendimiento RF. Esta funcionalidad se hará con independencia del cliente inalámbrico.
- El controlador virtual deberá poder repartir de manera dinámica los clientes WiFi entre los AP y bandas radio más convenientes en función de su carga. Esta funcionalidad se hará con independencia del tipo de cliente inalámbrico asociado.
- Soporte de protocolos estándar para facilitar el “roaming” entre puntos de acceso:
 - 802.11r
 - 802.11k
 - 802.11v
- El controlador deberá ser capaz de disminuir los efectos de la interferencia co-canal coordinando el acceso de los clientes a los puntos de acceso que están en el mismo canal con el fin de que el rendimiento de la red no se vea degradado.
- Los APs deberán poder ser configurados de forma estática o dinámica para funcionar exclusivamente en modo sonda (no participan en la transmisión de datos).
- Todos los puntos de acceso ofertados deben tener la posibilidad de implementar redes mesh wireless para que en el futuro la red wireless se pueda extender desde cualquier AP instalado sin necesidad de nuevo cableado o nuevas conexiones de red ethernet.
- Capacidad del controlador para dirigir de manera dinámica y automática los clientes WiFi hacia los AP más convenientes, evitando así el efecto “sticky client”. Esta funcionalidad se hará con independencia del cliente inalámbrico.
- Se podrán programar horarios y días para habilitar y deshabilitar SSIDs específicos de forma automática sin intervención manual de ningún operador.
- Todas las funcionalidades estarán residentes en la propia colmena de APs sin requerir elementos adicionales de control o seguridad. Tampoco se requerirá de elementos adicionales o conexión remota para realizar funcionalidades relativas al entorno de radio-frecuencia (búsqueda de interferencias, análisis del aire, selección de canales, etc).

2.3. Propiedades de red

Características Mínimas

- El controlador (ya sea físico o virtual) deberá soportar mecanismos para reducir de una manera sencilla el tráfico de broadcast y multicast, limitando el número de usuarios por VLAN y asignando nuevos usuarios a las VLANs menos ocupadas (“vlan-pooling”).
- Todos los puntos de acceso deberán también ser capaces establecer túneles VPN y cifrar mediante IPSec todo el tráfico que envíen a un punto central.
- Los APs deberán poder realizar captura de paquetes para poder ser analizados posteriormente desde un puesto central. La funcionalidad de captura de paquetes deberá ser simultánea a la funcionalidad de transmisión de datos. En ningún caso, el AP deberá ser reseteado y cambiado de modo para realizar la captura de paquetes.

- El controlador deberá ser capaz de hacer de proxy del tráfico mDNS para permitir el descubrimiento de impresoras, proyectores, discos en red, etc mediante protocolos “bonjour”, “upnp” o DLNA.
- Se valorará la capacidad de limitar la visibilidad de conexiones basadas en mDNS mediante autorización dinámica.
- Capacidad, embebido en el propio sistema operativo, de monitorizar parámetros NO-RF como, Asociación de radio Wireless, Autenticación, Asignación de direcciones Ip dinámicas y resolución DNS.

2.4 Redundancia

Características Mínimas

- Los controladores wireless (ya sean físicos o virtuales) deberán estar redundados con replicación automática de configuraciones entre controladores.
- Soporte de redundancia activo-activo.
- Soporte de redundancia N+1.
- Cualquier punto de acceso podrá realizar las funciones de controladora virtual y siempre existirá un equipo principal y otro de backup. Esta configuración será automática y no requerirá de intervención manual.

2.5 Seguridad

Características Mínimas

- Soporte de los siguientes métodos de autenticación:
 - 802.1x - (EAP, LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, EAP-OTP, EAP-GTC, EAP-TLV, EAP-AKA, EAP-MD5)
 - MAC
 - Portal Cautivo
- Soporte de autenticación sobre distintos tipos de servidores :
 - Base de datos interna
 - LDAP/ SSL Secure LDAP
 - RADIUS
- Soporte de CoA (RFC 3576)
- Soporte de RFC 5997
- Soporte de EAP-Offload, terminación local del EAP en el mismo controlador Wireless para aumentar el rendimiento de autenticación de la red inalámbrica.
- Soporte de inspección de conversaciones 802.1X entre clientes y servidor RADIUS para poder implementar derivación de roles sobre puntos de acceso de otros fabricantes.
- Soporte simultáneo de WPA y WPA2 sobre el mismo SSID.
- Soporte de roles de usuario que permitan diferenciar el tráfico de los usuarios y los destinos permitidos sin necesidad de separarlos en VLANs o SSIDs según el servicio prestado. Se soportarán las siguientes funcionalidades:

- Asignación de ancho de banda por rol o por usuario.
 - Reglas de Firewall basadas en la identidad del usuario y no en la dirección del origen del usuario.
 - Reglas de acceso por horario o por localización dentro de la red (punto de acceso).
 - Mapeo opcional del usuario a una VLAN independiente del SSID al que este asociado.
- Se podrán establecer túneles VPN con puntos centrales entre los APs que forman parte de la red para tener acceso a recursos centrales.
- Cuando se utilice más de un controlador wireless, la comunicación entre ellos deberá ser cifrada mediante túnel IPSec.
- Firewall embebido para realizar inspección de tráfico stateful con el objetivo de crear distintos roles de usuario e identificar los de flujos de tráfico.
- Filtrado de contenidos web que permita aplicar políticas sobre el tráfico web, en función de dos parámetros:
 - Categoría Web.
 - Reputación Web.
- En el caso de filtrado a web, se podrá redirigir a los usuarios a determinada dirección cuando accedan a websites bloqueados.
- Capacidad de realizar las funciones de IDS (Intrusión Detection System) wireless, como detección de Rogue APs o ataques de denegación de servicio (DoS), sin necesidad de utilizar soluciones externas de otros fabricantes.
- Capacidad de realizar funciones de IPS (Intrusion Protection System) wireless, con mecanismos de contención de intrusos como el “blacklisting”, sin necesidad de utilizar soluciones externas.
- Se podrá definir un portal cautivo básico dentro de los puntos de acceso para validar a los usuarios invitados. La solución permitirá mantener una base de datos restringida de usuarios para dichos invitados. Se permitirá crear un usuario/password de tipo operador para gestionar únicamente dichos usuarios dentro del cluster de Aps.
- Se podrá configurar acceso de invitados mediante Facebook WiFi sin elementos externos.
- Deberá tener seguridad del clúster, un protocolo de comunicación para asegurar los mensajes del plano de control entre los puntos de acceso. Mensajes del plano de control como la configuración, la unión de clúster y otros mensajes distribuidos entre los dispositivos en un clúster estarán asegurados utilizando este protocolo. La seguridad del clúster debe operar en el puerto UDP 4434 y utilizará el protocolo DTLS para proteger mensajes.

2.6 Calidad de Servicio y Comunicaciones Unificadas

Características Mínimas

- El controlador deberá implementar mecanismos de calidad de servicio como:
 - Limitar el ancho de banda:
 - Por usuario.
 - Por grupo de usuarios.

- Por AP.
 - Por aplicación
- Garantizar ancho de banda mínimo.
 - Por SSID.
 - Por grupo de usuarios.
 - Por aplicación.
- El controlador deberá tener capacidad para establecer reglas de seguridad a nivel de aplicación. Se deberá especificar el número máximo de reglas configurables por “rol” o “SSID”.
- Identificación y priorización automática del tráfico de voz, soportando los protocolos de VoIP más habituales: H.323, SIP, SIP-Q, IAX y SCCP.
- Control de las conexiones de VoIP de los usuarios (Control de Admisión de Llamadas, CAC): Posibilidad de limitar el número de conversaciones de voz soportadas por cada punto de acceso y para diferentes tipos de usuario, por ejemplo usuarios bajo cobertura del AP o usuarios que hacen roaming. Posibilidad de desviar una llamada o usuario hacia otro AP cuando el límite de llamadas de un AP ya se ha cubierto.
- El controlador soportará mecanismos que minimicen el tiempo de roaming entre APs como OKC (Opportunistic Key Caching) situando el tiempo de roaming idealmente por debajo de 50 milisegundos.
- Capacidad de que un punto de acceso detenga el Control Automático de la Radiofrecuencia (cambio de canal, escaneo, etc) cuando tenga llamadas de voz establecidas. Con esto se evita que se corte la conversación. El AP debe esperar (de forma dinámica) a realizar el escaneo cuando se termine la conversación.
- 8 colas de prioridad tanto en el controlador como en la parte wireless de los Aps.
- Tanto el controlador wireless como los APs deben marcar (802.1p, TOS, DSCP) el tráfico entre ambos (tráfico del túnel) para que sea priorizado por los switches y routers intermedios.
- El controlador wireless debe ser capaz de marcar y dar prioridad alta al tráfico de voz aunque no venga marcado y aunque esté mezclado en la misma VLAN y SSID que el tráfico de datos.
- El controlador wireless será capaz de dar de priorizar el tráfico de cualquier aplicación diseñada por el cliente, independientemente de los protocolos soportados por los terminales wireless (WMM, etc...).
- El controlador deberá poder convertir el trafico multicast en unicast para dar servicios de Video sobre Wifi de manera eficiente.
- El controlador deberá tener capacidad de inspección de paquetes en tiempo real (DPI) en todos los niveles OSI (1-7), específicamente a nivel 4-7. Este DPI deberá ser de última generación, capaz de reconocer no sólo aplicaciones de voz y video sino toda la familia de nuevas aplicaciones móviles como Whatsapp, Facebook, etc.
- No existirá limite en cuanto a las reglas que se podrán establecer de filtrado de aplicaciones, pudiéndose aplicar por usuario y SSID características de priorización de tráfico, marcado, eliminación, etc.

2.7 - Despliegue y Gestión de la infraestructura

- Los puntos de acceso y controladora virtual tendrán la posibilidad de despliegue simplificado. Se podrá realizar la autoprovisión de los equipos sin intervención manual ni configuración específica en cada sede.
- Los APs podrán asociarse a una plataforma de gestión central para descargarse la configuración automáticamente y entrar en servicio automáticamente.
- Toda la red de APs podrá gestionarse desde una única interfaz vía https y tendrá visibilidad de todos los puntos de acceso de la red.
- Toda la configuración estará centralizada y será distribuida a todos los APs que forman parte de la colmena de puntos de acceso.
- Opcionalmente, la colmena de APs podrán gestionarse desde una plataforma centralizada.
- Opcionalmente, los APs podrán ser reconfigurados para depender de controladoras físicas. Este cambio de configuración no requerirá de cambio ni actualización de firmware y deberá estar disponible mediante un cambio de configuración en el interfaz de gestión del propio AP.

2.8 - Características de los puntos de acceso

- Obligatoriamente se proveerán al menos 1700 puntos de acceso.
- Los puntos de acceso anteriores deberán corresponder a una única referencia.
- Los puntos de accesos deberán estar provistos de su correspondiente kit de montaje.
- Las funcionalidades mínimas que se requieren sobre los puntos de acceso Wifi son las que se indican a continuación. Se valorará adicionalmente que el fabricante de los dispositivos disponga de una solución de provisión automática, de manera que la primera configuración de los APs se pueda realizar mediante plantillas en un sistema centralizado y sea el propio AP al ser conectado a la red quien busque automáticamente a este “servidor de configuraciones”.
- Todos los puntos de acceso deberán soportar el estándar 802.11ac wave 2 con soporte de “beamforming” basado en estándares. Así como mantener la compatibilidad con estándares anteriores 802.11 a/b/g/n.
- Los puntos de acceso deberán incluir tecnología MIMO con al menos soporte para 2 y 4 flujos espaciales, es decir, serán al menos, 4x4:4 en 5 GHz y 2x2:2 en 2,4 GHz.
- Soportará MU-MIMO.
- Capacidad de ser alimentado con PoE.
- Rango de temperatura operacional de entre, como mínimo, -0 y 50 grados centígrados.
- Las radios deberán poder hacer Análisis de Espectro para detectar interferencias no-Wifi y servir clientes de manera simultánea.
- El AP deberá poder detectar y clasificar las fuentes de interferencia externas (Microondas, Bluetooth, DECT, etc...).

- Todos los puntos de acceso ofertados deben incorporar radios de última generación con posibilidad de analizar el espectro para detectar posibles interferencias.
- Certificado Wi-Fi Alliance (WFA) 802.11a/b/g/n/ac.
- Soporte de los siguientes métodos de cifrado:
 - CCMP/AES (recomendado)
 - TKIP
 - Secure Sockets Layer (SSL) and TLS.
 - RC4 128-bit and RSA 1024- and 2048-bit.
- Los puntos de acceso deberán incluir radios que no se vean afectadas por interferencias de las redes 3G/4G.
- Se valorará el valor de la “Sensibilidad” (dBm) de las radios, es decir, la capacidad de reconstruir un flujo de datos a partir de una señal débil.
- Al menos 1 interfaz 10/100/1000 BASE-T.
- Posibilidad de aplicaciones móviles para facilitar el despliegue, administración o monitorización de los puntos de acceso.
- Los puntos de acceso deberán contar con un beacon integrado (BLE) que permita entre otras cosas, el acceso al cli por bluetooth.
- Los puntos de acceso podrán convertirse en pesados (gestionados por una controladora externa) con un cambio de firmware desde el modo de funcionamiento “ligero” (autónomos), es decir, cambio de pesado a ligero en el mismo punto de acceso sin necesidad de cambiar el hardware y posibilidad de volver de nuevo a pesado si así se requiriera.
- El punto de acceso dispondrá de un puerto usb.
- Soporte de IPM (Intelligent Power Monitoring).

2.9 - Gestión centralizada de monitorización y gestión

- Se deberán proveer tantas licencias con soporte de 5 años como puntos de acceso ofertados. Estas licencias deberán incrementar el software actual de monitorización Aruba Airwave que dispone el Gobierno de Navarra para monitorizar y gestionar su infraestructura.
- Queda excluido del presente contrato el software de monitorización y gestión, ya que se utilizará el que dispone el Gobierno de Navarra, como se indica en el párrafo anterior. Solamente se necesitan las licencias de los APs para que sean monitorizados y gestionados.
- La solución ofertada deberá ser gestionable de manera centralizada (monitorización y configuración vía interfaz web) desde una única plataforma de gestión. Dicha plataforma tendrá que cumplir como mínimo con las siguientes características:
 - La solución ofertada deberá monitorizar el análisis de la información de los sistemas externos a la propia red wifi que son imprescindibles para un buen funcionamiento de los usuarios de movilidad como el tiempo de asociación, tiempo de autenticación (801.1x, MAC o portal cautivo), tiempo de respuesta de DNS y del DHCP tanto a nivel general como para cada usuario.

- La solución irá una máquina virtual “on premise” sin opción a soluciones cloud por lo que únicamente se proveerán licencias que serán perpetúas.
- La solución deberá ser capaz de monitorizar y gestionar soluciones de diferentes fabricantes tanto de Wireless como de wired.
- Actualización centralizada del firmware de los dispositivos. Esta tarea podrá realizarse automáticamente de forma programada o mediante actuaciones puntuales.
- Auto-Descubrimiento de dispositivos.
- Auto-Configuración de los puntos de acceso que se vayan incorporando a la red.
- Comprobación de las políticas de seguridad configuradas en los Puntos de Acceso, detectando violaciones o deficiencias en la configuración del SSID, broadcasts, 802.1x o WEP.
- Permitirá la creación de grupos de dispositivos en función de distintos criterios definidos por el administrador. Estos grupos pueden tener una organización jerárquica o definir macro grupos seleccionando múltiples grupos.
- Permitirá la funcionalidad PnP para el despliegue remoto de dispositivos de forma automatizada.
- Permitirá la detección de Puntos de Acceso instalados sin autorización (Rogue Access Points).
- Permitir la configuración y administración completa de todos los elementos de la red WLAN
- Permitirá su integración con sistemas de gestión mediante SNMP.
- Dispondrá de diversos métodos de acceso:
 - Interfaz de operación basado en HTML
 - Mediante líneas de código (CLI) a través de consola
 - Telnet
 - Secure Shell (SSH).
- Permitirá la notificación y seguimiento de fallos a través de notificaciones en distintos formatos (Syslog, e-mail y SNMP Traps).
- Permitirá almacenar, al menos, el último fichero de configuración, facilitando la “marcha atrás” en caso de ser necesario.
- Permitirá la supervisión y control de toda la infraestructura WiFi mediante la recolección de alarmas y eventos de los elementos de la misma y su representación visual, así como su exportación a otras plataformas mediante protocolos SNMP o Syslog.
- Permitirá elaborar informes personalizados sobre la actividad de la red con periodicidad configurable y entregables en varios formatos (PDF y CSV)
- Permitirá monitorización proactiva de incidencias basada en umbrales para la generación de eventos y alarmas en base a variables críticas.
- Soportará la funcionalidad de mapa de red en donde se presente el estado de todos los elementos de la red wifi, así como su estado de operación con tiempos de refresco no superiores a 5 minutos. Esto debe incluir la representación, al menos, de los siguientes elementos:
 - Estado operativo de los elementos de la red wifi.
 - Interferencias, zonas de cobertura, potencia, señal, ruido, interferencias, etc.
 - Análisis de estudio de coberturas y mapas de calor.
 - Voice Network.
 - Wifi TDOA Receivers y Tags.
 - Clientes, Rouge APs, Rouge Adhocs, Rouge Clientes.
- El sistema debe proporcionar estudios de cobertura en tiempo real. Debe mostrar los mapas de calor con la distribución de frecuencias y potencias en tiempo real, a partir de la información que capturan todos los Puntos de Acceso. Se valorará que también permita hacer análisis de coberturas futuros modificando o agregando nuevos APs solo en el plano, sin necesidad de su despliegue, actuando como una herramienta de estudio de cobertura.

- El sistema debe disponer de un sistema de localización y seguimiento de forma que vaya actualizando la posición del elemento a seguir.
- Permitirá monitorizar los conmutadores a los que están conectados los APs, facilitando información sobre disponibilidad y utilización de los puertos, CPU, memoria y toda la información de conectividad para un dispositivo dado, permitiendo analizar y comparar su configuración actual con la anterior para analizar cómo pudo influir un determinado cambio.
- Permitirá detectar equipamiento con versiones de software no actualizadas, permitiendo distribuir las actualizaciones a todos los equipamientos que lo necesiten.

2.10 – Garantía

La empresa adjudicataria contraerá el compromiso formal, que deberá asumir de modo expreso, de garantizar todos y cada uno de los suministros a realizar, así como de los materiales que lo componen.

Garantía de por vida para los puntos de acceso de interior de tal manera que el fabricante garantice su reemplazo por uno nuevo en la vida útil del producto.

La garantía incluirá la reposición de todos los equipos defectuosos o inadecuados. Esta garantía incluirá también el transporte de los mismos a la dirección que se indica en el punto 3 del presente pliego.

Asimismo, la garantía cubrirá la indemnización de los perjuicios que por razones de los defectos mencionados pudieran producirse.

2.11 - Soporte de hardware, software y licencias

El alcance de este soporte incluye las controladoras, los licenciamientos de los puntos de acceso, el elemento de gestión y el elemento de control de acceso de red. Por consiguiente, se excluye de este soporte hardware de los puntos de acceso, lo que se resolverá mediante la reserva de un stock dedicado a repuestos.

Se solicita soporte de cinco años con las siguientes características:

- Reemplazo avanzado de piezas averiadas tipo NBD (Next Business Day)
- Acceso a centro de asistencia técnica del fabricante con posibilidad de abrir casos.
- Acceso a las últimas versiones y a parches de resolución de fallos.

Se deberá entregar en formato digital, la relación del material suministrado, con al menos el nº de serie y la dirección física (MAC) de los APs.

2.12 - Mejoras en el suministro

Se valorará positivamente, tal y como indica el apartado 7 “Criterios de Adjudicación” del Pliego de condiciones administrativas, la inclusión en la oferta de un número superior al exigido en pliego de puntos de acceso, plenamente licenciados en prestaciones y en gestión.

3.- DIRECCIÓN DE ENTREGA DE LOS EQUIPOS

Los equipos deberán entregarse en:

Almacén del Departamento de Educación

C/Sarriguren Bidea nº 9 (polígono de Areta Sur)

C.P. 31620, Huarte-Pamplona
Tf: 689 80 10 44