Documento Técnico

Proteja su Red Wireless con los Puntos de Acceso con Seguridad Avanzada

Tabla de Contenidos

Introducción

¿Es seguro su entorno inalámbrico SASE?

A medida que las empresas adoptan más SaaS y las opciones de trabajo desde el hogar se vuelven más populares, los administradores de TI corporativos deben considerar cómo asegurarse de que los usuarios legítimos con dispositivos legítimos puedan acceder a los recursos corporativos autorizados, ya sea en la oficina desde el hogar o fuera de ambos. Por lo tanto, se hace necesaria una infraestructura SASE (Perfil de Servicio de Acceso Seguro) con reglas de política de acceso a la red de confianza cero para garantizar que se aplique la misma política a todos los individuos. Sin embargo, la conclusión es que los usuarios legítimos deben poder acceder a la red cableada e inalámbrica de forma segura sin preocuparse de que sus credenciales o datos sean violados o de que los piratas informáticos imiten a los clientes legítimos.

A diferencia de las redes cableadas con dispositivos cliente conectados a un puerto cableado dedicado, las redes de área local inalámbricas (WLAN) transmiten y reciben datos por aire, lo que hace que las WLAN sean vulnerables a interferencias, intercepciones, escuchas ilegales y todo tipo de piratería. Los usuarios WFH (trabajo desde casa) también se exponen a amenazas en un entorno de Wi-Fi doméstico no seguro. Incluso si se aplica un túnel VPN para asegurar la conexión entre la puerta de enlace doméstica y la sede, sigue siendo difícil asegurar una WLAN en el lugar de trabajo de un empleado, incluso si la empresa proporciona un dispositivo de túnel VPN autorizado para los usuarios domésticos.

Figure01 -- La infraestructura SASE también requiere protección de seguridad inalámbrica

Además de las amenazas de WLAN, también nos encontramos con otros tipos de problemas de seguridad, como dejar la credencial del dispositivo con los valores predeterminados de fábrica, dejar el SSID abierto y exponer tramas de administración sin encriptación. La solución EnGenius Cloud proporciona las funciones esenciales para ayudar a los administradores de TI a fortalecer su infraestructura y proteger los activos corporativos.

Problemas de Seguridad de la Red Inalámbrica

Hay tres amenazas de seguridad comunes en las WLAN:

Negación de Servicio

Un ataque de denegación de servicio llena el canal de radio enviando paquetes de desautenticación o desasociación para evitar que los clientes se conecten al AP y accedan a la red. Un inhibidor de RF es una herramienta que normalmente se usa para bloquear el canal de radio, por lo que los clientes válidos no podrán acceder a la red. Los clientes no autorizados también pueden falsificar el SSID y el AP para anular la autenticación o desasociar clientes legítimos.

Frase de Contraseña o Descifrado de Contraseñas

Los piratas informáticos pueden realizar un sniff o "escuchar" el tráfico aéreo para descifrar la frase de contraseña PSK de un SSID y acceder a la red. También pueden quebrar las contraseñas de usuario para cambiar la configuración como administrador o acceder a recursos no autorizados como usuarios autorizados.

Filtración de Datos

Al suplantar la identidad de un SSID o AP legítimo, los piratas informáticos pueden aprovechar el AP falso para recopilar datos de usuario. Las amenazas comunes son los ataques de man-in-the-middle o gemelos malvados (Evil Twin).

Denegación de servicio y Solución EnGenius

Interferencias de Radio

Los usuarios pueden experimentar una fuerte intensidad de la señal de Wi-Fi pero tener problemas para conectarse al punto de acceso o sufrir una velocidad de datos extremadamente baja. Por lo general, se debe a que la tasa de utilización del canal WiFi es tan alta que no hay ancho de banda para clientes válidos. Las fuentes de interferencia pueden provenir del Wi-Fi de sus vecinos o de electrodomésticos sin Wi-Fi, como hornos microondas.

Detección, Análisis y Solución

Tasa de Utilización del Canal Operativo

EnGenius Cloud proporciona una herramienta de análisis de utilización de canales en tiempo real para ver cuántas señales de radio Wi-Fi y no Wi-Fi utilizan el canal operativo, para que los usuarios puedan saber si el problema de conectividad se debe a la alta utilización del canal o a la falta de una señal Wi-Fi cercana.

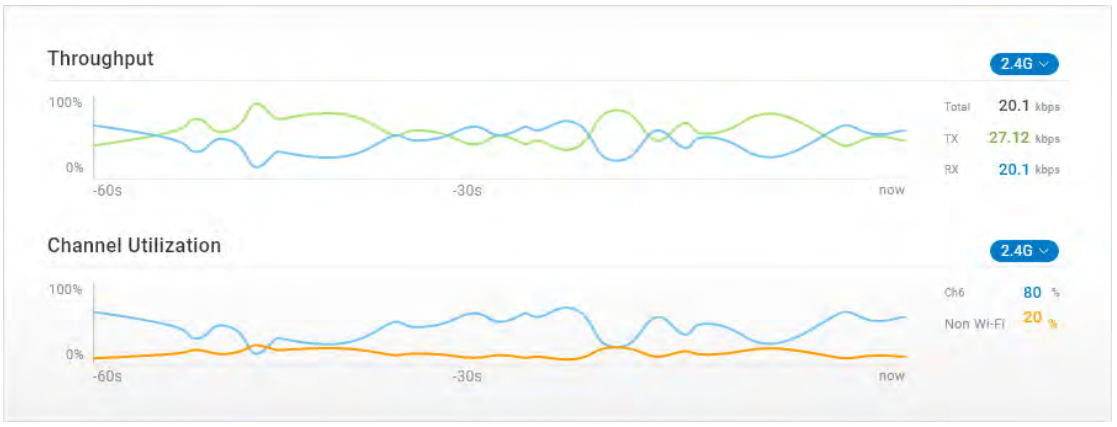

Figura02 -- Ratio de Utilización del Canal Operativo

Herramienta de Diagnóstico de Utiulización de Canal

Cuando el canal operativo está abarrotado, el mejor remedio es pasar a un canal limpio. Además del análisis de utilización del canal en tiempo real para ver el estado de utilización del canal operativo actual, EnGenius Cloud proporciona una herramienta útil adicional para mostrar la utilización completa del canal y el análisis de densidad para ayudarlo a identificar qué canal es el más limpio.

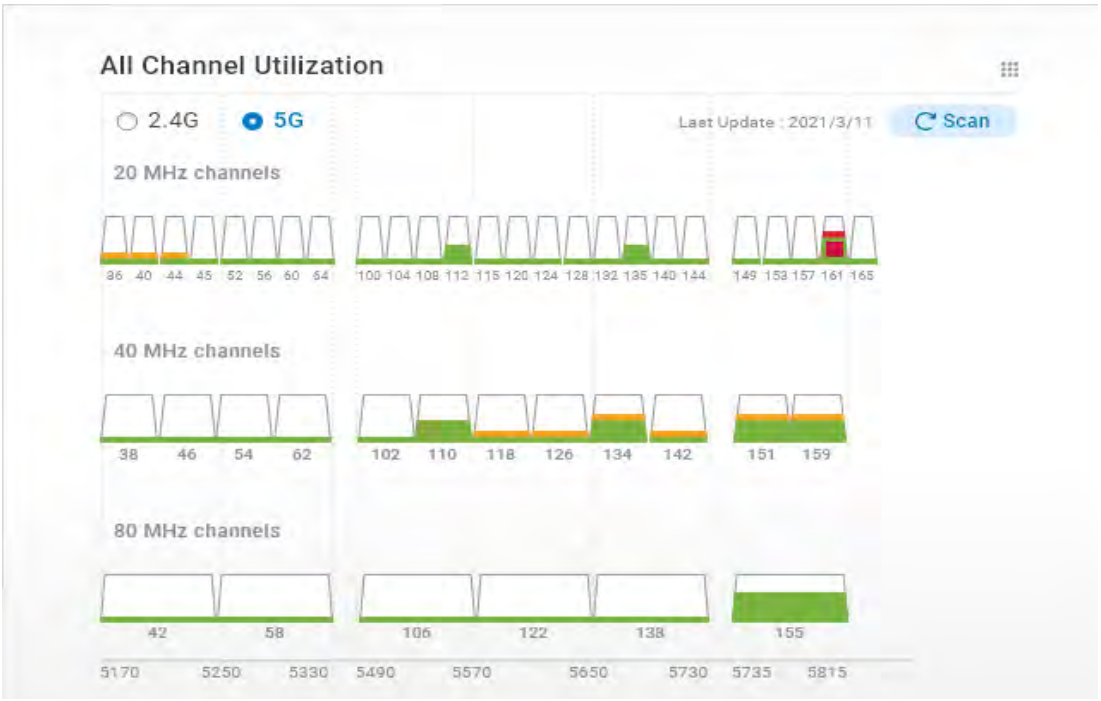

Figura03 -- Análisis de utilización de todos los canales

Análisis de Cascada de Espectro

Al analizar la utilización del canal, el usuario verá la densidad de uso en un momento dado. Sin embargo, una breve interferencia puede inducir al usuario a pensar erróneamente que la interferencia está en curso. La herramienta de análisis de cascada de espectro ayuda a los usuarios a ver la interferencia a lo largo del tiempo con la pantalla de "cascada", para que los usuarios puedan determinar qué canal está más limpio en el tiempo en vez de un momento específico.

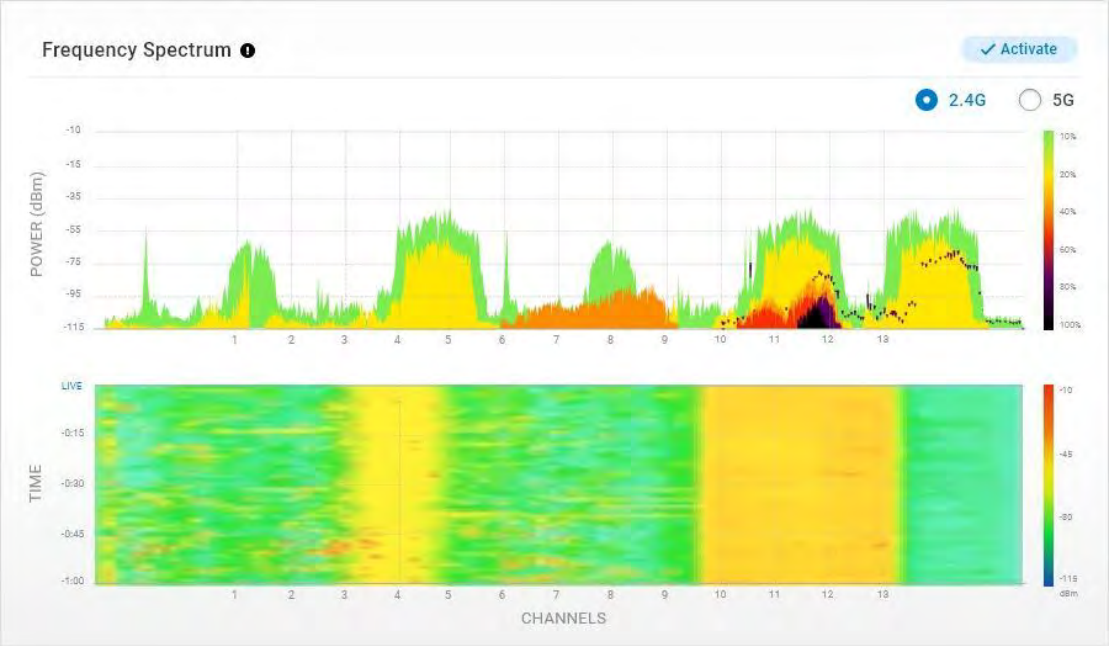

Figura04 -- Análisis de Espectro en Cascada

ACS (Auto Selección de Canal)

Sin la necesidad de seleccionar manualmente el canal del gráfico de utilización de canal completo o el espectro de cascada, los usuarios pueden ejecutar la selección automática de canal (ACS) de EnGenius para que un AP de EnGenius escanee el entorno y, según el algoritmo de EnGenius, identifique y pase automáticamente a un canal más limpio.

DFS de Espera Cero para Entornos de Alta Densidad

En despliegues de alta densidad, muchos canales Wi-Fi que no se superponen requieren que se usen canales DFS para evitar la interferencia de canales. Sin embargo, el AP deberá cambiar a otro canal una vez que se detecte el radar protegido. Dado que los canales que no son DFS son muy densos, cambiar a otro canal DFS es la mejor opción. Sin embargo, generalmente requiere un tiempo de espera de >30 segundos para asegurarse de que el canal DFS se pueda utilizas, lo que provoca el tiempo de inactividad de la sesión del cliente.

La tecnología DFS de espera cero en los modelos EnGenius “S” (ECW220S, ECW230S) utiliza una radio de exploración dedicada para seguir detectando otros canales DFS disponibles a los que el AP puede cambiar de inmediato para mantener conectadas las sesiones del cliente.

RF Jamming (Interferencias de RF)

Hay dos tipos de interferencia de RF: interferencia de radio para simplemente bloquear el canal de radio e inundación de paquetes para generar una gran cantidad de paquetes de Wi-Fi en el canal para que no haya ancho de banda para que los clientes válidos se conecten a la red.

Detección, Análisis y Solución

Detección y Clasificación de interferencias de RF

EnGenius AirGuard proporciona detección de ataques de interferencia de RF y clasifica los ataques como interferencia de radio o inundación de paquetes. El AP especifica qué canal es atacado y detectado, para que los usuarios puedan conocer qué AP detectados podrían tener un bloqueador de RF. Cuando el canal está ocupado, los usuarios pueden usar EnGenius ACS (selección automática de canales) para trasladar el SSID a otro canal sin ser atacados.

Figura05 -- Lista de detección de interferencias de RF

Paquetes de Desautenticación y Disociación anormales

Los clientes deben ser autenticados por el AP con el protocolo de seguridad correcto (por ejemplo, clave PSK personal WPA2) antes de asociarse con el AP. Los clientes normalmente se desconectan cuando reciben marcos de des-autenticación o des-asociación del AP.
Dado que los marcos de administración de autenticación/ desautenticación, asocición/desasociación están desprotegidos la mayor parte del tiempo, los piratas informáticos pueden engañar fácilmente al cliente para seguir enviando solicitudes de des-asociación/des-autenticación al AP o imitar al AP para enviar respuestas de des-asociación/desautenticación a todos los clientes, evitando que puedan acceder al AP.

Detección, Análisis y Solución

Detección y clasificación de desautenticación y disociación maliciosas

EnGenius AirGuard cuenta con un algoritmo para detectar cambios anormales frecuentes en marcos de desautenticación y desvinculación e informar del ataque malicioso en dos categorías: desautenticación y desvinculación. AirGuard también puede detectar si el ataque está dirigido a un cliente específico, el AP atacado mostrará la dirección MAC del cliente. O si el ataque imita el AP para desconectar a todos los clientes, entonces la parte atacada mostrará ff:ff:ff:ff:ff:ff en su lugar.

Category	SSID	Channel	Attacked Party	Connected to AP	Last Seen	First Seen	Network
Dis-association attack	FAtest	2	All Clients (FF:FF:FF:FF:FF:FF)	---	34 sec ago	2 weeks ago	8F
Dis-association attack	FAtest	2	James's NB (92:3E:DE:00:96:42)	Connected	34 sec ago	2 weeks ago	8F
Dis-association attack	FAtest	2	James's NB (92:3E:DE:00:96:42)	Connected	34 sec ago	2 weeks ago	8F
De-Auth attack	FAtest	2	All Clients (FF:FF:FF:FF:FF:FF)	---	34 sec ago	2 weeks ago	8F
De-Auth attack	FAtest	2	James's NB (92:3E:DE:00:96:42)	Unconnected	34 sec ago	2 weeks ago	8F
De-Auth attack	FAtest	2	James's NB (92:3E:DE:00:96:42)	Unconnected	34 sec ago	2 weeks ago	8F

Figura06 -- Lista de detección de ataques maliciosos

Compatibilidad con 802.11w para Proteger el Marco de Gestión

Se recomienda encarecidamente habilitar 802.11w (802.11w-2009 MFP-Management Frame Protection) para proteger los marcos de administración y asegurarse de que el marco de administración sea de un AP legítimo. Tanto los clientes como los puntos de acceso deben ser compatibles con 802.11w para comunicarse.

Filtración de datos, descifrado de contraseñas, y la solución EnGenius

Ataque Honey Pot (SSID Falso)

Todo el mundo puede adquirir un punto de acceso o un enrutador Wi-Fi para generar un SSID no autorizado que tenga exactamente el mismo aspecto que el SSID corporativo legítimo. Se puede colocar, por ejemplo, en el estacionamiento alrededor del

edificio corporativo como un señuelo (Honey Pot) al que podría conectarse inadvertidamente el portátil de un empleado válido.

Es más probable que ocurra un ataque de SSID deshonesto a medida que más empresas utilicen servicios en la nube como Google Suite, Salesforce.com, etc. en general servicios en la nube.

Se vuelve aún más sencillo cuando se implementa una nueva tecnología de roaming en teléfonos móviles y ordenadores portátiles que detectarán la señal más fuerte del mismo SSID y se desplazarán hacia ella. El pirata informático puede situar su punto de acceso deshonesto a un lado del edificio corporativo, mientras que el Wi-Fi corporativo puede tener una cobertura más débil en las esquinas o los laterales del edificio.

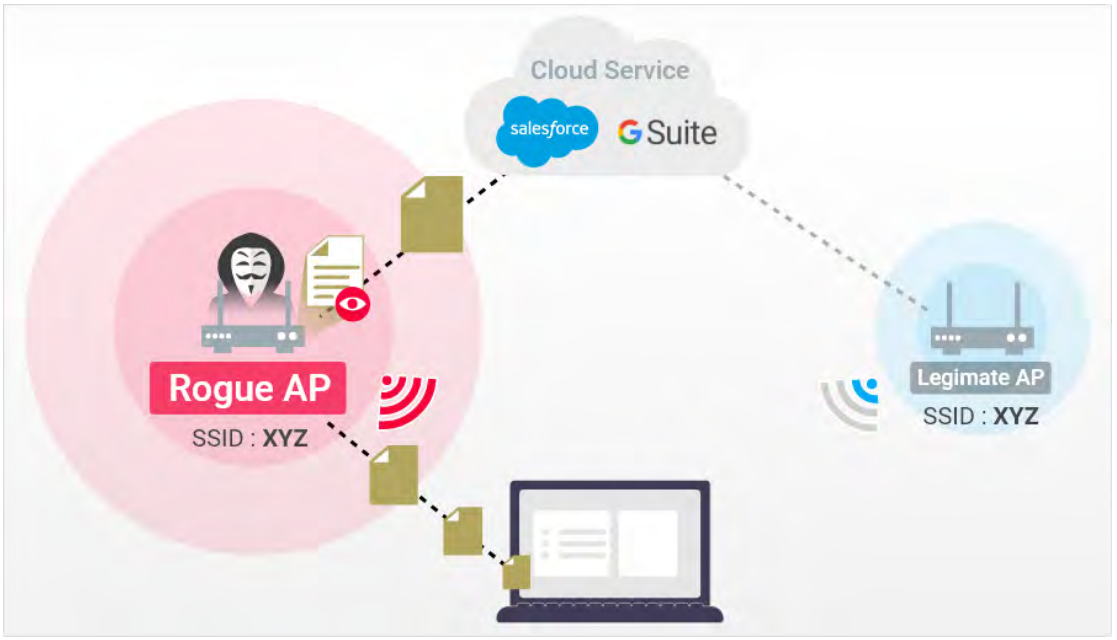

Figura07 -- Ataque Honey Pot (Rogue SSID)

Detección, Análisis y Solución

Detección SSID Falso

EnGenius AirGuard puede verificar el nombre SSID (ESSID) o la radio AP MAC (BSSID) para detectar automáticamente el punto de acceso no autorizado que imita el SSID legítimo pero que no figura entre los puntos de acceso legítimos administrados por EnGenius en la misma red.

Reglas de Lista Blanca/Falsos de EnGenius y Honey Pot para identificar Hackers

Es una buena práctica configurar un entorno trampa en una red corporativa para atraer e identificar a los atacantes malintencionados. Los administradores pueden configurar una red separada de las redes corporativas con un punto de acceso trampa usando un SSID abierto y algunos clientes generando tráfico. Los piratas informáticos malintencionados encontrarán el SSID "débil" del honey pot y lo atacarán.

AirGuard permite a los usuarios establecer reglas no autorizadas y reglas de lista blanca comparando el nombre SSID o la dirección MAC BSSID. En el caso del honeypot, los administradores pueden monitorear qué fuentes MAC imitan el SSID del honeypot, observar cómo intentan atacar la red y tomar las medidas correspondientes. En caso de que haya AP legítimos que no sean EnGenius implementados en la red corporativa, los administradores pueden incluir en la lista blanca la dirección MAC de los AP que no sean EnGenius y separarlos de la lista de SSID falsos.

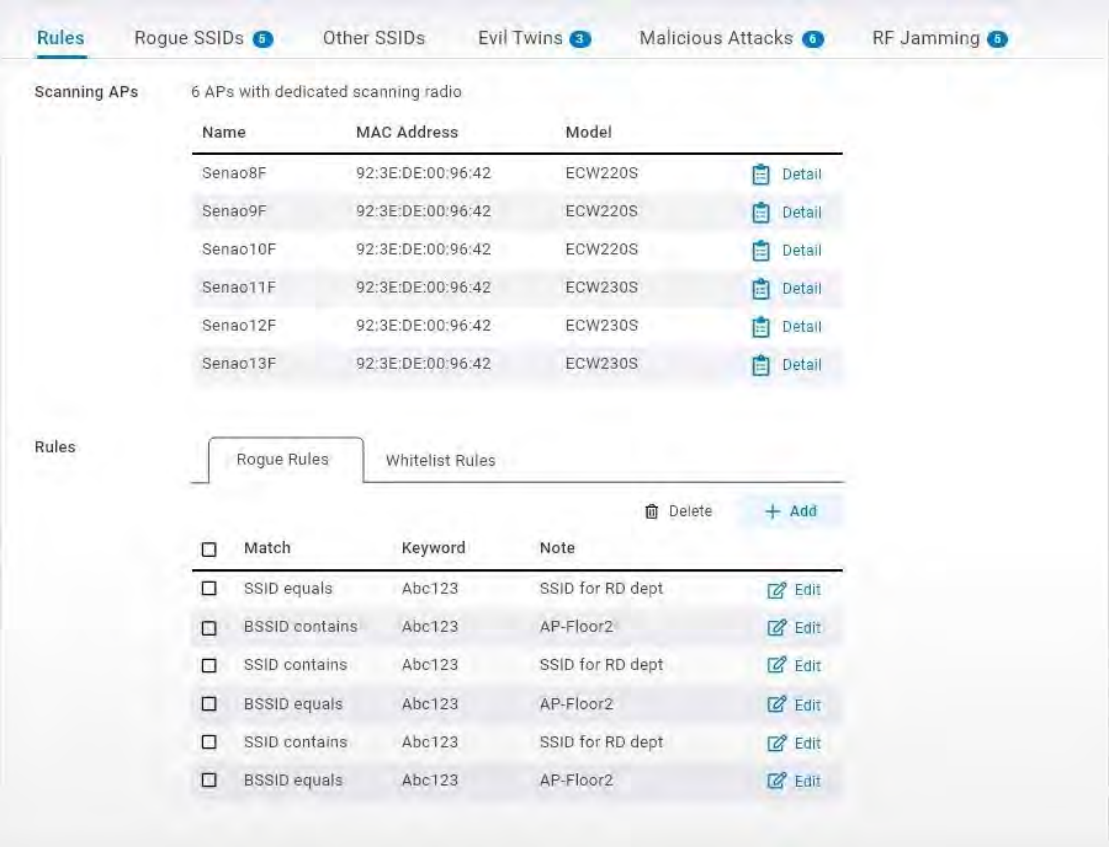

Figure08 -- Rogue Rules and Whitelist Rules of SSIDs

Ataque Man-In-The-Middle

Al atraer a los usuarios válidos para que se conecten al punto de acceso no autorizado, los piratas informáticos pueden conectar un proxy al punto de acceso no autorizado y redirigir todo el tráfico a través del proxy. Los piratas informáticos pueden capturar la información corporativa confidencial mientras el usuario accede a los servicios corporativos en la nube.

Si el pirata informático puede además conectarse a un AP legítimo, entonces puede conectar un AP no autorizado a un AP legítimo e imitar el SSID legítimo. Todo parece igual desde el extremo del cliente cuando se conecta al SSID no autorizado o un punto de acceso no autorizado intermediario.

Hay tres formas sencillas en que un pirata informático puede conectarse a un AP legítimo:

- Credencial de Ddministrador de Dispositivo predeterminada de Fábrica
  Este es el fraude más común que los usuarios pueden encontrar accidentalmente. Usando la credencial predeterminada de fábrica, los piratas informáticos pueden piratear el dispositivo y cambiar la configuración para permitir que un AP no autorizado se conecte a un AP legítimo.

- Cuando el tipo de seguridad SSID está configurado como "Abierto".
  Cuando un SSID está "abierto", todos pueden conectarse al AP legítimo y acceder a las redes y activos corporativos. También es bastante común establecer el tipo de seguridad SSID en Abierto cuando la página de presentación del portal cautivo está configurada para la autenticación de usuarios. El punto de acceso no autorizado puede conectarse fácilmente al punto de acceso legítimo y pasar el tráfico general, incluida la autenticación de la página de inicio, mientras rastrea todos los datos.

- Aprovecha vulnerabilidades de Firware sin actualizar
  Se encontraron algunos problemas de vulnerabilidad en WPA2, como el problema KRACK en el que los piratas informáticos podían aprovechar una secuencia de saludo de cuatro vías de WPA2 y piratear el PSK para robar información confidencial como credenciales, información de tarjetas de crédito, etc. La vulnerabilidad se solucionó, pero los usuarios tenían que actualizar a la versión más actualizada del firmware de su dispositivo. Administrar el firmware del dispositivo en la red corporativa también es una tarea del administrador.

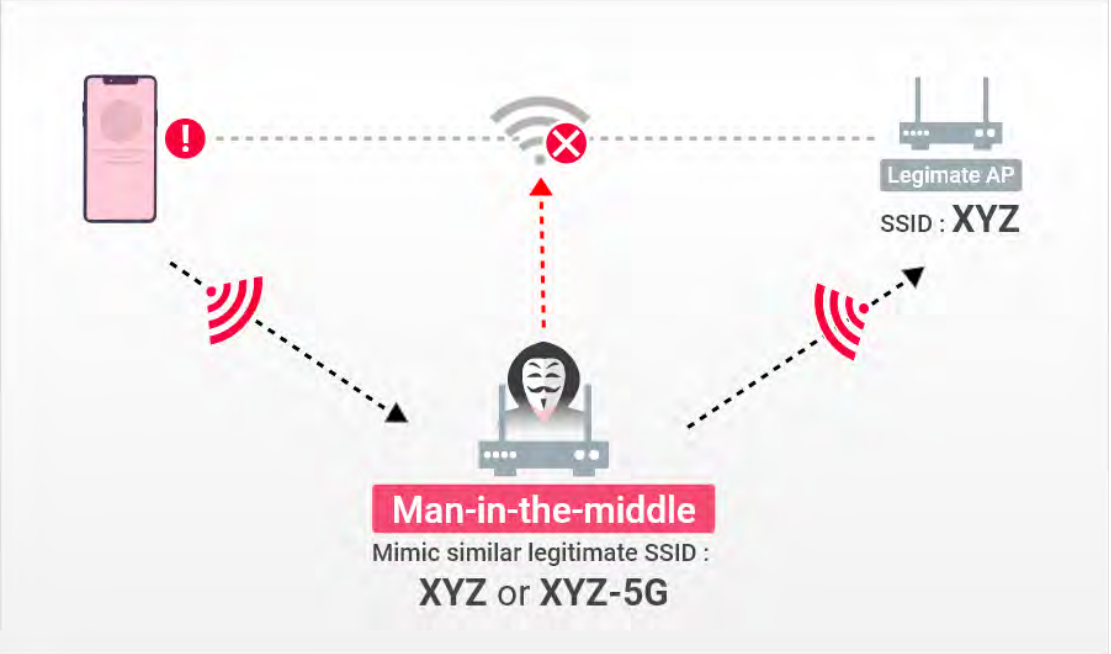

Figura09 -- Ataque Man-in-the-Middle

Por ejemplo, el pirata informático puede iniciar un ataque DoS para romper la conexión entre los clientes y un AP legítimo, de modo que los clientes tengan problemas para conectarse al SSID legítimo. Por ejemplo, si un pirata informático encuentra una red llamada "XYZ", el pirata informático puede crear un SSID similar a "XYZ-5G" para conectarse. (El pirata informático también puede usar exactamente el mismo nombre de SSID para simular un SSID legítimo; sin embargo, esto se encontrará a través de la detección de "SSID falso"). El pirata informático puede redirigir el tráfico a una página web de phishing para robar credenciales o dirigir el el tráfico de regreso a un AP legítimo y capturar todos los datos transferidos en el medio.

Detección, Análisis y Solución

Detección de APs falsos

AirGuard monitoreará todos los SSID con el mismo nombre que el SSID legítimo y verificará si el SSID es de AP legítimos en la red. Los usuarios también pueden establecer reglas de lista blanca agregando listas AP MAC legítimas que no son administradas por EnGenius Cloud para excluirlas de la lista de SSID no autorizados.

myPSK para Proteger la Contraseña de WPA-SSID personal

Es común configurar la frase de contraseña del WPA PSK del SSID para tener un control de acceso de seguridad básico. Sin embargo, una vez que alguien conoce la frase de contraseña, puede acceder al SSID para siempre sin límites. EnGenius myPSK le permite al administrador de la red configurar un PSK único para cada persona y controlar el período válido y la VLAN, de modo que cuando la persona no sea elegible para acceder a la red, el PSK no será válido. Esta función es especialmente adecuada

para residencias escolares donde los estudiantes y profesores van y vienen con diferentes niveles de acceso a los recursos. Los administradores de residencias pueden basar el acceso en el año escolar completo o en ciertos semestres para que a los estudiantes se les asigne un PSK único y accedan a una determinada VLAN durante un período de tiempo limitado.

Todos los dispositivos cuentan con una cuenta y una contraseña predeterminadas para una configuración por primera vez. Si el administrador no cambia la cuenta/contraseña, es sencillo que alguien inicie sesión en el dispositivo y cambie la configuración. Este es el descuido más común que pone en riesgo la seguridad de la red corporativa.

EnGenius alienta a los usuarios a configurar una cuenta de administrador local única para toda la red y una contraseña de inmediato. Cuando se asigna un nuevo dispositivo a la red y se crea una nueva red, la cuenta de administrador local y la contraseña para acceder a la GUI local del dispositivo deben cambiarse en consecuencia. Si no se cambia la credencial predeterminada de fábrica, EnGenius Cloud marcará la red como "insegura" colocando un ícono de advertencia en la red para indicar que los dispositivos de la red están expuestos a fraudes de seguridad.

Soporte WPA3 para una Seguridad Avanzada

WPA3 mejora el mecanismo de seguridad con OWE (Cifrado Inalámbrico Oportunista) para reemplazar el tipo de seguridad abierta. Los clientes no necesitan la frase de contraseña para acceder al AP, porque OWE encriptará la transmisión. Además, WPA3-personal utiliza tecnología SAE para reemplazar el WPA2 clave precompartida, una forma más segura de realizar el intercambio de claves y evitar ataques como el protocolo de enlace de cuatro vías KRACK.

Conexión Segura para Autenticación de Portal Cautivo

EnGenius proporciona una opción HTTPS para que los usuarios cifren la comunicación entre el cliente y el AP antes de que el usuario se autentique a través de un portal cautivo. Sin el cifrado, un intermediario puede capturar fácilmente la credencial durante el proceso de inicio de sesión del portal cautivo.

Actualización Automática de Firmware

Para asegurarse de que el firmware de los dispositivos en la red corporativa sea lo más actualizado y las vulnerabilidades corregidas lo antes posible, la función de actualización automática de firmware de EnGenius Cloud permite a los usuarios establecer intervalos de tiempo cada semana para actualizar. Una vez configurado, los administradores no tendrán que preocuparse por la gestión de la versión de firmware en toda la red.

Ataques Evil Twin

Los piratas informáticos utilizan dispositivos "Gemelos Malvados! (Evil Twin) para piratear redes al engañar a lclientes legítimos para que se conecten. Dado que la detección de seguridad verifica que las tramas provengan de puntos de acceso legítimos, los piratas informáticos cambiarán la dirección MAC e incluso el nombre SSID del gemelo malvado para que coincida con la dirección MAC y el nombre SSID del AP legítimo.

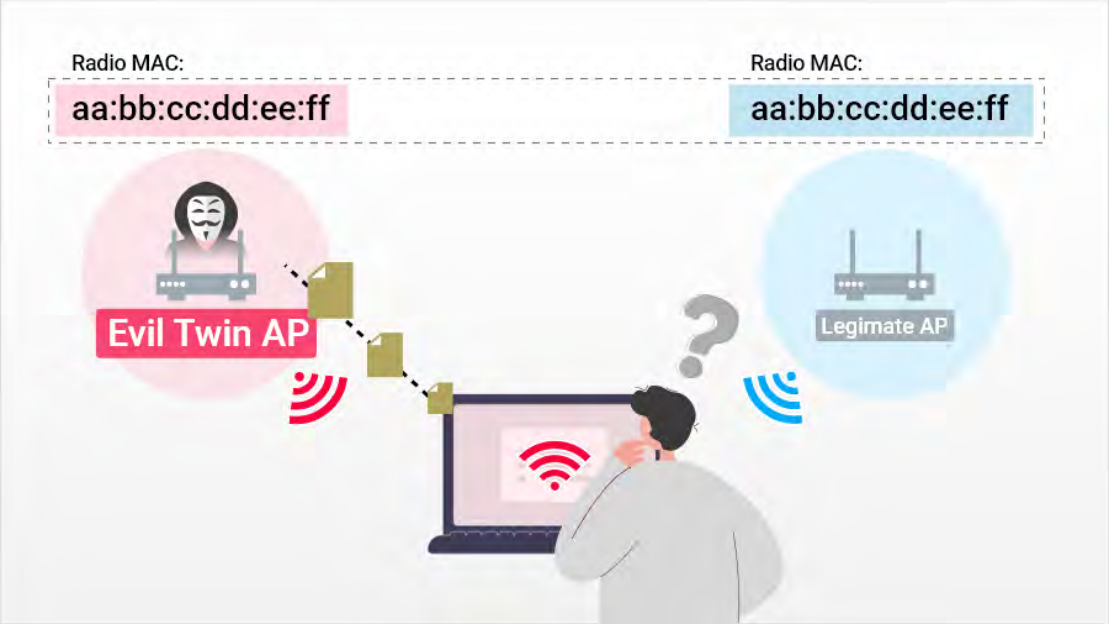

Figure10 -- Evil Twin Attack

Detección, Análisis y Solución

Detección y Clasificación de Gemelos Malvados (Evil Twins)

AirGuard puede detectar el ataque del gemelo malvado con un algoritmo para distinguir si las tramas son de un AP EnGenius legítimo o un AP no autorizado que imita la dirección MAC legítima.

Se clasifican dos categorías:

- AP Spoofing (Suplantación de identidad)
  El AP no autorizado suplantará al AP legítimo mediante el envío de tramas con la misma dirección MAC que el AP legítimo.

- AP impersonation (Imitación de Personalidad)
  El AP no autorizado no solo imita la dirección MAC del AP legítimo, sino también su nombre SSID.

Co-Defensa mejorada Detección de Gemelos Malvados (Evil Twin)

Por lo general, la forma en que un AP puede detectar un gemelo malvado es aprovechando la técnica de "Sé que no eres yo". Entonces, cuando "yo", el AP detector, detecto marcos con mi dirección MAC, sé que no envié el marco, así que sé que hay un gemelo malvado alrededor. Sin embargo, si un gemelo malvado está fuera del alcance de la víctima AP, la víctima AP no podrá identificar si es legítimo o falso.

EnGenius mejora el algoritmo de detección de Gemelos Malvados al permitir que todos los puntos de acceso legítimos de la red sepan quiénes son mis colegas y quién es el gemelo malvado.

Localizando APs Falsos

Con la función EnGenius Cloud Map, los usuarios pueden cargar un plano de planta y colocar un punto de acceso en el mapa de planta para ver el mapa de calor de la cobertura Wi-Fi. Los usuarios también pueden agregar paredes y puertas al plano de planta para ver cómo los obstáculos afectan el mapa de calor.

AirGuard enumerará los puntos de acceso no autorizados con la intensidad de la señal (valor RSSI) para que los usuarios puedan aprovechar el plano de planta para ubicar los puntos de acceso no autorizados y descubrir si la fuente no autorizada podría estar cerca.

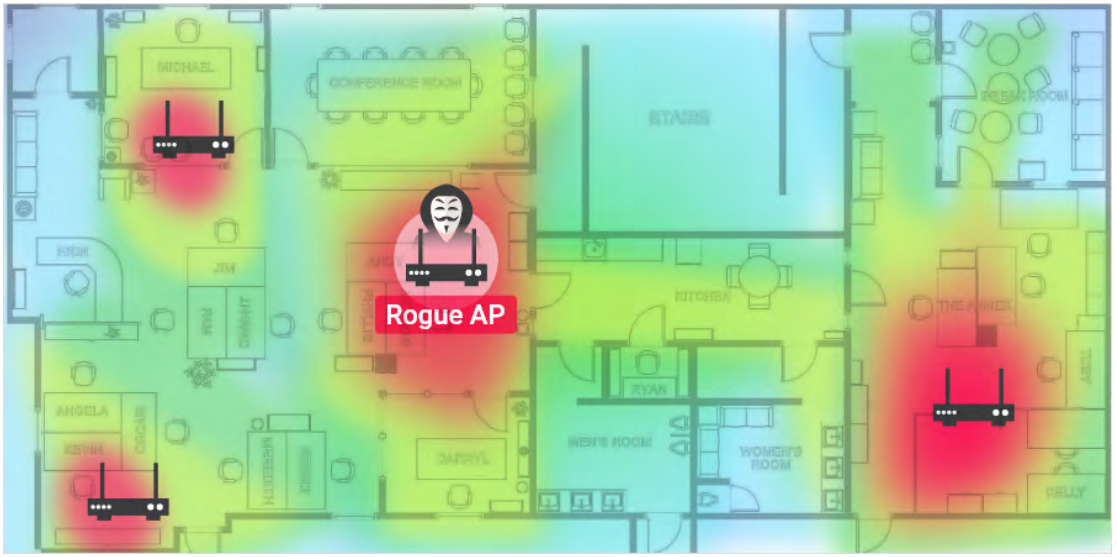

Figura11 -- Localice el punto de acceso no autorizado con el mapa de calor

Certificado Integrado de Fábrica

Cada dispositivo EnGenius Cloud tiene un certificado integrado instalado de fábrica, que es un componente obligatorio cuando se comunica con EnGenius Cloud.

Por lo tanto, un AP rogue Evil Twin puede clonar el mismo MAC que un AP legítimo. Sin embargo, el AP no autorizado no puede conectarse a EnGenius Cloud sin el certificado integrado para acceder a la red corporativa.

MFA para la incorporación de dispositivos.

Para obtener el certificado integrado, el intruso podría comprar un AP EnGenius en el mercado para que funcione como un AP maligno gemelo; sin embargo, el AP debe pasar por el proceso MFA (autenticación de múltiples factores) para poder conectarse a la nube y unirse a la red. Primero, EnGenius Cloud verificará el certificado, la dirección MAC, el número de serie y el proceso de intercambio de claves, y luego verificará si el dispositivo está registrado en una organización o si el dispositivo está asociado con la red.

Protección segura de la Capa de Control, sin Datos de Usuario

Solo la capa de gestión de configuración del dispositivo accede a EnGenius Cloud. Todos los demás datos de usuario no pasarán a través de la nube, por lo que los usuarios no deben preocuparse si EnGenius Cloud capturará o almacenará datos confidenciales del usuario. EnGenius Cloud también cifra la información de la capa de control para evitar que los piratas informáticos detecten el tráfico de administración.

Solución EnGenius - Beneficios

AirGuard para proteger la WLAN

EnGenius AirGuard es la forma en que EnGenius detecta los ataques de interferencia de RF, anula la autenticación y desasociación de marcos anormales, Gemelos Malvados e identifica los SSID no autorizados de los puntos de acceso no autorizados. AirGuard también proporciona formas de establecer reglas no autorizadas y reglas de lista blanca mediante la identificación de nombres SSID o direcciones MAC de radio.

Herramientas de diagnóstico localizar la causa raíz

EnGenius proporciona herramientas de diagnóstico para cada AP con las que ver la utilización del canal de tráfico Wi-Fi y no WiFi, y el espectro de cascada donde ver la congestión del canal con históricos. Las herramientas también brindan la capacidad de hacer ping, traceroute y lista de clientes en vivo.

Dispositivos Protegidos conectados a la nube

Cada dispositivo EnGenius Cloud tiene un certificado incorporado de fábrica y requiere múltiples métodos de autenticación para poder conectarse a EnGenius Cloud. Solo el tráfico de administración fluirá a través de EnGenius Cloud. Todos los demás flujos de datos importantes del usuario no pasarán a través de EnGenius Cloud para proteger la privacidad del usuario.

Funciones para Alta Disponibilidad

El DFS de espera cero de EnGenius Cloud es perfectamente adecuado para un entorno de alta densidad, para aprovechar tantos canales disponibles como sea posible. Además, el algoritmo de selección automática de canales (ACS) permite que el AP encuentre un canal más limpio para una mejor conexión.

Funciones de Cumplimiento de Seguridad

EnGenius Cloud AP es compatible con myPSK. Al configurar un PSK único para cada usuario para proteger la contraseña contra fugas. El punto de acceso en la nube también es compatible con WPA3, 802.11w para una conexión WLAN más segura contra filtraciones. EnGenius Cloud aplica la actualización automática de firmware para asegurarse de que todas las versiones de firmware de AP administrado estén actualizadas para corregir cualquier problema de vulnerabilidad. EnGenius Cloud también sigue comprobando si la credencial predeterminada ha cambiado y seguirá advirtiendo a los usuarios que cambien la contraseña predeterminada. Una herramienta sofisticada de plano de planta ayuda a los usuarios a ver mapas del piso y cómo las paredes, puertas y otros obstáculos afectan la cobertura. Los administradores pueden usar el mapa del piso combinado con AirGuard para encontrar la ubicación de la fuente no autorizada identificando la lista de puntos de acceso detectados en el mapa del piso.

Acerca de EnGenius

EnGenius es un fabricante líder mundial de comunicaciones inalámbricas y de voz . Durante más de 20 años, EnGenius ha brindado las mejores soluciones de voz y datos de su clase que potencian la movilidad, mejoran la productividad y adoptan la simplicidad. EnGenius se enorgullece de brindar a los consumidores las mejores soluciones de red personalizadas, más fiables y ricas en funciones para impulsar el éxito de su negocio.

Obtenga más información sobre EnGenius Cloud : https://www.engenius.ai/cloud