Preguntas más Frecuentes sobre Aironet Wireless Security

Contenido

[Introducción](#)
[Preguntas Frecuentes Generales](#)
[Preguntas frecuentes sobre Troubleshooting y Diseño](#)
[Información Relacionada](#)

Introducción

Este documento proporciona información sobre las preguntas más frecuentes(FAQ) relacionadas con la seguridad inalámbrica de Cisco Aironet.

Preguntas Frecuentes Generales

P. ¿Cuál es la necesidad de seguridad inalámbrica?

A. En una red con cables, los datos permanecen en los cables que conectan los dispositivos finales. Pero las redes inalámbricas transmiten y reciben datos a través de una difusión de señales de RF al aire libre. Debido a la naturaleza de la transmisión que utilizan las WLAN, existe una mayor amenaza de hackers o intrusos que pueden acceder o corromper los datos. Para aliviar este problema, todas las WLAN requieren la adición de:

1. Autenticación de usuario para evitar el acceso no autorizado a los recursos de red.
2. Privacidad de datos para proteger la integridad y privacidad de los datos transmitidos (también conocidos como cifrado).

P. ¿Cuáles son los diferentes métodos de autenticación que define el estándar 802.11 para las LAN inalámbricas?

A. El estándar 802.11 define dos mecanismos para la autenticación de clientes LAN inalámbricos:

1. Autenticación abierta
2. Autenticación de clave compartida

También hay otros dos mecanismos de uso común:

1. Autenticación basada en SSID
2. Autenticación de dirección MAC

P. ¿Qué es la autenticación abierta?

A. La autenticación abierta es básicamente un algoritmo de autenticación nulo, lo que significa que no hay verificación del usuario o la máquina. La autenticación abierta permite cualquier dispositivo que realice una solicitud de autenticación en el punto de acceso (AP). La autenticación abierta utiliza la transmisión de texto sin cifrar para permitir que un cliente se asocie a un AP. Si no se habilita ninguna encriptación, cualquier dispositivo que conozca el SSID de la WLAN puede obtener acceso a la red. Si se habilita la privacidad equivalente a conexión con cables (WEP) en el AP, la clave WEP se convierte en un medio de control de acceso. Un dispositivo que no tiene la clave WEP correcta no puede transmitir datos a través del AP aunque la autenticación sea exitosa. Tampoco puede un dispositivo de este tipo descifrar los datos que envía el AP.

P. ¿Qué pasos implica la autenticación abierta para que un cliente se asocie con el AP?

1. El cliente envía una solicitud de sonda a los AP.
2. Los AP envían respuestas de sonda de retorno.
3. El cliente evalúa las respuestas AP y selecciona el mejor AP.
4. El cliente envía una solicitud de autenticación al AP.
5. El AP confirma la autenticación y registra el cliente.
6. El cliente entonces envía una solicitud de asociación al AP.
7. El AP confirma la asociación y registra al cliente.

P. ¿Cuáles son las ventajas y desventajas de la autenticación abierta?

A. Estas son las ventajas y desventajas de la autenticación abierta:

Ventajas: La autenticación abierta es un mecanismo de autenticación básico, que puede utilizar con dispositivos inalámbricos que no admiten los algoritmos de autenticación complejos. La autenticación en la especificación 802.11 está orientada a la conectividad. Por diseño, los requisitos de autenticación permiten a los dispositivos obtener acceso rápido a la red. En tal caso, puede utilizar la autenticación abierta.

Desventajas: La autenticación abierta no permite comprobar si un cliente es un cliente válido y no un cliente hacker. Si no utiliza la encriptación WEP con la autenticación abierta, cualquier usuario que conozca el SSID de la WLAN podrá acceder a la red.

P. ¿Qué es la autenticación de clave compartida?

A. Shared Key Authentication funciona de forma similar a Open Authentication con una diferencia importante. Cuando utiliza la autenticación abierta con la clave de encriptación WEP, la clave WEP se utiliza para cifrar y descifrar los datos, pero no se utiliza en el paso de autenticación. En la autenticación de clave compartida, se utiliza la encriptación WEP para la autenticación. Al igual que la autenticación abierta, la autenticación de clave compartida requiere que el cliente y el AP tengan la misma clave WEP. El AP que utiliza la autenticación de clave compartida envía un paquete de texto de desafío al cliente. El cliente utiliza la clave WEP configurada localmente para cifrar el texto del desafío y responder con una solicitud de autenticación posterior. Si el AP puede descifrar la solicitud de autenticación y recuperar el texto de desafío original, el AP responde con una respuesta de autenticación que otorga acceso al cliente.

P. ¿Qué pasos implica la autenticación de clave compartida para que un cliente se asocie con el AP?

1. El cliente envía una solicitud de sonda a los AP.
2. Los AP envían respuestas de sonda de retorno.
3. El cliente evalúa las respuestas AP y selecciona el mejor AP.
4. El cliente envía una solicitud de autenticación al AP.
5. El AP envía una respuesta de autenticación que contiene el texto de desafío no cifrado.
6. El cliente cifra el texto del desafío con la clave WEP y envía el texto al AP.
7. El AP compara el texto de desafío no cifrado con el texto de desafío cifrado. Si la autenticación puede descifrar y recuperar el texto de desafío original, la autenticación es correcta.

La autenticación de clave compartida utiliza la encriptación WEP durante el proceso de asociación del cliente.

P. ¿Cuáles son las ventajas y desventajas de la autenticación de clave compartida?

A. En Shared Key Authentication (Autenticación de clave compartida), el cliente y el AP intercambian el texto del desafío (texto sin cifrar) y el desafío cifrado. Por lo tanto, este tipo de autenticación es vulnerable a ataques de intrusos. Un hacker puede escuchar el desafío no cifrado y el desafío cifrado, y extraer la clave WEP (clave compartida) de esta información. Cuando un hacker conoce la clave WEP, todo el mecanismo de autenticación se ve comprometido y el hacker puede acceder a la red WLAN. Esta es la principal desventaja con la autenticación de clave compartida.

P. ¿Qué es la autenticación de dirección MAC?

A. Aunque el estándar 802.11 no especifica la autenticación de dirección MAC, las redes WLAN suelen utilizar esta técnica de autenticación. Por lo tanto, la mayoría de los proveedores de dispositivos inalámbricos, incluido Cisco, admiten la autenticación de direcciones MAC.

En la autenticación de dirección MAC, los clientes se autentican en función de su dirección MAC. Las direcciones MAC de los clientes se verifican en una lista de direcciones MAC almacenadas localmente en el AP o en un servidor de autenticación externo. La autenticación MAC es un mecanismo de seguridad más sólido que las autenticaciones de clave abierta y compartida que ofrece 802.11. Esta forma de autenticación reduce aún más la probabilidad de que los dispositivos no autorizados puedan acceder a la red.

P. ¿Por qué la autenticación MAC no funciona con el acceso Wi-Fi protegido (WPA) en la versión 12.3(8)JA2 del software Cisco IOS?

A. El único nivel de seguridad para la autenticación MAC es verificar la dirección MAC del cliente con una lista de direcciones MAC permitidas. Esto se considera muy débil. En versiones anteriores del software Cisco IOS, puede configurar la autenticación MAC y WPA para cifrar la información. Pero como WPA tiene una dirección MAC que verifica, Cisco decidió no permitir este tipo de configuración en versiones posteriores del software Cisco IOS y decidió solo mejorar las funciones de seguridad.

P. ¿Puedo utilizar SSID como método para autenticar dispositivos inalámbricos?

A. El identificador de conjunto de servicios (SSID) es un valor alfanumérico único que distingue entre mayúsculas y minúsculas que las WLAN utilizan como nombre de red. El SSID es un mecanismo -que permite la separación lógica de las LAN inalámbricas. El SSID no proporciona

ninguna función de privacidad de datos, ni el SSID autentica verdaderamente al cliente al AP. El valor SSID se transmite como texto claro en Beacons, Probe Requests (Solicitudes de sondeo), Probe response (Respuestas de sondeo) y otros tipos de tramas. Un explorador puede determinar fácilmente el SSID con el uso de un analizador de paquetes LAN inalámbrica 802.11, por ejemplo, Sniffer Pro. Cisco no recomienda utilizar el SSID como método para proteger la red WLAN.

P. Si inhabilito la difusión SSID, ¿puedo lograr una seguridad mejorada en una red WLAN?

A. Cuando inhabilita la difusión de SSID, el SSID no se envía en los mensajes de baliza. Sin embargo, otras tramas como Solicitudes de sondeo y Respuestas de sondeo aún tienen el SSID en texto claro. Por lo tanto, no puede lograr una seguridad inalámbrica mejorada si desactiva el SSID. El SSID no está diseñado, ni está destinado para su uso, como mecanismo de seguridad. Además, si inhabilita las difusiones SSID, puede encontrar problemas con la interoperabilidad Wi-Fi para implementaciones de clientes mixtos. Por lo tanto, Cisco no recomienda que utilice el SSID como modo de seguridad.

P. ¿Cuáles son las vulnerabilidades encontradas en la seguridad 802.11?

A. Las principales vulnerabilidades de la seguridad 802.11 se pueden resumir de la siguiente manera:

- Autenticación débil sólo para dispositivos: Los dispositivos cliente se autentican, no los usuarios.
- Cifrado de datos débil: Se ha demostrado que la privacidad equivalente a conexión con cables (WEP) no es eficaz como medio para cifrar los datos.
- No hay integridad del mensaje: Se ha demostrado que el valor de comprobación de integridad (ICV) es ineficaz como medio para garantizar la integridad del mensaje.

P. ¿Cuál es la función de la autenticación 802.1x en la WLAN?

A. Para abordar las deficiencias y vulnerabilidades de seguridad en los métodos originales de autenticación que define el estándar 802.11, el marco de autenticación 802.1X se incluye en el borrador para las mejoras de seguridad de la capa MAC 802.11. El grupo de tareas i (TGi) IEEE 802.11 está desarrollando actualmente estas mejoras. El marco de trabajo 802.1X proporciona la capa de link con autenticación extensible, que normalmente se ve sólo en las capas superiores.

P. ¿Cuáles son las tres entidades que define la estructura 802.1x?

A. El marco 802.1x requiere que estas tres entidades lógicas validen los dispositivos en una red WLAN.

1. **Suplicante**: el suplicante reside en el cliente de LAN inalámbrica y también se conoce como cliente EAP.
2. **Authenticator**: el autenticador reside en el AP.
3. **Servidor de autenticación**: el servidor de autenticación reside en el servidor RADIUS.

P. ¿Cómo se produce la autenticación de un cliente inalámbrico cuando uso el marco de autenticación 802.1x?

A. Cuando el cliente inalámbrico (cliente EAP) se activa, el cliente inalámbrico se autentica con autenticación abierta o compartida. 802.1x funciona con la autenticación abierta y comienza después de que el cliente se asocia correctamente al AP. La estación cliente puede asociarse, pero sólo puede pasar tráfico de datos después de una autenticación 802.1x exitosa. Estos son los pasos en la autenticación 802.1x:

1. AP (Authenticator) configurado para 802.1x solicita la identidad del usuario al cliente.
2. Los clientes responden con su identidad dentro de un período de tiempo estipulado.
3. El servidor comprueba la identidad del usuario y comienza la autenticación con el cliente si la identidad del usuario está presente en su base de datos.
4. El servidor envía un mensaje de éxito al AP.
5. Una vez que se autentica el cliente, el servidor reenvía la clave de cifrado al AP que se utiliza para cifrar/descifrar el tráfico enviado desde y hacia el cliente.
6. En el paso 4, si la identidad del usuario no está presente en la base de datos, el servidor descarta la autenticación y envía un mensaje de falla al AP.
7. AP reenvía este mensaje al cliente, y el cliente debe autenticarse nuevamente con las credenciales correctas.

Nota: A lo largo de la autenticación 802.1x , AP solamente reenvía los mensajes de autenticación hacia y desde el cliente.

P. ¿Cuáles son las diferentes variantes EAP que puedo utilizar con el marco de autenticación 802.1x?

A. 802.1x define el procedimiento para autenticar clientes. El tipo EAP utilizado en el marco de trabajo 802.1x define el tipo de credenciales y el método de autenticación utilizado en el intercambio 802.1x. El marco 802.1x puede utilizar cualquiera de estas variantes EAP:

- EAP-TLS: seguridad de la capa de transporte del protocolo de autenticación extensible
- EAP-FAST: autenticación EAP flexible a través de túnel seguro
- EAP-SIM: módulo de identidad de suscriptor EAP
- Cisco LEAP: protocolo de autenticación extensible ligero
- EAP-PEAP: protocolo de autenticación extensible protegido EAP
- EAP-MD5: algoritmo EAP-Message Digest 5
- EAP-OTP: contraseña EAP a tiempo
- EAP-TTLS: seguridad de la capa de transporte tunelizada EAP

P. ¿Cómo elijo un método EAP 802.1x de las diferentes variantes disponibles?

A. El factor más importante que debe tener en cuenta es si el método EAP es compatible con la red existente o no. Además, Cisco recomienda que elija un método que admita la autenticación

mutua.

P. ¿Qué es la autenticación EAP local?

A. EAP local es un mecanismo en el que el WLC actúa como servidor de autenticación. Las credenciales del usuario se almacenan localmente en el WLC para autenticar a los clientes inalámbricos, que actúa como un proceso de respaldo en las oficinas remotas cuando el servidor se desactiva. Las credenciales de usuario se pueden recuperar desde la base de datos local en el WLC o desde un servidor LDAP externo. LEAP, EAP-FAST, EAP-TLS, PEAPv0/MSCHAPv2 y PEAPv1/GTC son autenticaciones EAP diferentes admitidas por EAP local.

P. ¿Qué es Cisco LEAP?

A. El protocolo de autenticación extensible ligero (LEAP) es un método de autenticación propietario de Cisco. Cisco LEAP es un tipo de autenticación 802.1X para LAN inalámbricas (WLAN). Cisco LEAP admite una autenticación mutua sólida entre el cliente y un servidor RADIUS a través de una contraseña de inicio de sesión como secreto compartido. Cisco LEAP proporciona claves de cifrado dinámicas por usuario y por sesión. LEAP es el método menos complicado para implementar 802.1x y sólo requiere un servidor RADIUS. Consulte Cisco LEAP para obtener información sobre LEAP.

P. ¿Cómo funciona EAP-FAST?

A. EAP-FAST utiliza algoritmos de clave simétrica para lograr un proceso de autenticación tunelizado. El establecimiento del túnel se basa en un protocolo de credenciales de acceso protegido (PAC) que EAP-FAST puede aprovisionarse y administrarse de forma dinámica mediante EAP-FAST a través del servidor de autenticación, autorización y contabilidad (AAA) (como Cisco Secure Access Control Server [ACS] v. 3.2.3). Con un túnel mutuamente autenticado, EAP-FAST ofrece protección frente a ataques de diccionario y vulnerabilidades intermedias. Estas son las fases de EAP-FAST:

EAP-FAST no solo mitiga los riesgos de los ataques de diccionario pasivos y los ataques de intrusos, sino que también permite una autenticación segura basada en la infraestructura implementada actualmente.

- Fase 1: Establecer túnel mutuamente autenticado: el cliente y el servidor AAA utilizan PAC para autenticarse mutuamente y establecer un túnel seguro.
- Fase 2: Realizar autenticación de cliente en el túnel establecido: el cliente envía el nombre de usuario y la contraseña para autenticar y establecer la política de autorización del cliente.
- Opcionalmente, Fase 0: la autenticación EAP-FAST utiliza esta fase con poca frecuencia para permitir que el cliente se aprovisione dinámicamente con un PAC. Esta fase genera una credencial de acceso por usuario de forma segura entre el usuario y la red. La fase 1 de la autenticación utiliza esta credencial por usuario, conocida como PAC.

Consulte Cisco EAP-FAST para obtener más información.

P. ¿Hay documentos en cisco.com que expliquen cómo configurar EAP en una red WLAN de Cisco?

A. Refiérase a Autenticación EAP con Servidor RADIUS para obtener información sobre cómo configurar la autenticación EAP en una red WLAN.

Consulte Nota de Aplicación EAP Protegida para obtener información sobre cómo configurar la autenticación PEAP.

Consulte Autenticación LEAP con un servidor RADIUS local para obtener información sobre cómo configurar la autenticación LEAP.

P. ¿Cuáles son los diferentes mecanismos de encriptación que se utilizan más comúnmente en las redes inalámbricas?

A. Estos son los esquemas de cifrado más utilizados en las redes inalámbricas:

- WEP
- TKIP
- AES

AES es un método de cifrado de hardware, mientras que el cifrado WEP y TKIP se procesa en el firmware. Con una actualización de firmware, los dispositivos WEP pueden admitir TKIP para que sean interoperables. AES es el método más seguro y rápido, mientras que WEP es el menos seguro.

P. ¿Qué es la encriptación WEP?

A. WEP significa Wired Equivalent Privacy. WEP se utiliza para cifrar y descifrar señales de datos que se transmiten entre dispositivos WLAN. WEP es una función IEEE 802.11 opcional que previene la divulgación y la modificación de los paquetes en tránsito, y también proporciona control de acceso para el uso de la red. WEP hace a un link WLAN tan seguro como un link cableado. Como el estándar especifica, WEP utiliza el algoritmo RC4 con una clave de 40 bits o 104 bits. RC4 es un algoritmo simétrico porque RC4 utiliza la misma clave para el cifrado y el descifrado de datos. Cuando se habilita WEP, cada "estación" de radio tiene una clave. La clave se utiliza para codificar los datos antes de la transmisión de estos a través de las ondas. Si una estación recibe un paquete que no se revuelva con la clave apropiado, la estación desecha el paquete y nunca entrega tal paquete al host.

Consulte Configuración de Privacidad Equivalente con Cable (WEP) para obtener información sobre cómo configurar WEP.

P. ¿Qué es la rotación de clave de difusión? ¿Cuál es la frecuencia de rotación de claves de difusión?

A. La rotación de la clave de difusión permite que el AP genere la mejor clave de grupo aleatoria posible. La rotación de la clave de difusión actualiza periódicamente todos los clientes capaces de gestionar las claves. Cuando habilita la rotación de la clave WEP de difusión, el AP proporciona una clave WEP de difusión dinámica y cambia la clave en el intervalo establecido. La rotación de la clave de difusión es una excelente alternativa a TKIP si su LAN inalámbrica admite dispositivos cliente inalámbricos que no sean de Cisco o dispositivos que no pueda actualizar al firmware más reciente para los dispositivos cliente de Cisco. Consulte Habilitación e Inhabilitación de la Rotación de Clave de Broadcast para obtener información sobre cómo configurar la función de rotación de clave de broadcast.

P. ¿Qué es TKIP?

A. TKIP significa protocolo de integridad de clave temporal. TKIP se introdujo para abordar las deficiencias en la encriptación WEP. TKIP también se conoce como hash de clave WEP y se llamó inicialmente WEP2. TKIP es una solución temporal que soluciona el problema de reutilización de claves WEP. TKIP utiliza el algoritmo RC4 para realizar el cifrado, que es el mismo que WEP. Una diferencia importante de WEP es que TKIP cambia la clave temporal cada paquete. La clave temporal cambia cada paquete porque el valor hash para cada paquete cambia.

P. ¿Pueden los dispositivos que utilizan TKIP interoperar con los que utilizan la encriptación WEP?

A. Una ventaja con TKIP es que las WLAN con AP y radios basados en WEP existentes pueden actualizarse a TKIP a través de simples parches de firmware. Además, el equipo solo WEP sigue interoperando con los dispositivos habilitados para TKIP que utilizan WEP.

P. ¿Qué es Message Integrity Check (MIC)?

A. MIC es otra mejora para abordar las vulnerabilidades del cifrado WEP. MIC evita ataques de giro de bits en los paquetes cifrados. Durante un ataque de giro de bits, un intruso intercepta un mensaje cifrado, altera el mensaje y luego retransmite el mensaje alterado. El receptor no sabe que el mensaje está dañado y no es legítimo. Para solucionar este problema, la función MIC agrega un campo MIC a la trama inalámbrica. El campo MIC proporciona una verificación de integridad de trama que no es vulnerable a las mismas deficiencias matemáticas que el ICV. El MIC también agrega un campo de número de secuencia a la trama inalámbrica. El AP descarta las tramas recibidas fuera de orden.

P. ¿Qué es WPA? ¿En qué se diferencia WPA 2 de WPA?

A. WPA es una solución de seguridad basada en estándares de Wi-Fi Alliance que aborda las vulnerabilidades de las WLAN nativas. WPA proporciona protección de datos mejorada y control de acceso para los sistemas WLAN. WPA aborda todas las vulnerabilidades conocidas de privacidad equivalente a conexión con cables (WEP) en la implementación de seguridad IEEE 802.11 original y aporta una solución de seguridad inmediata a las redes WLAN en entornos empresariales y de oficinas pequeñas, oficinas domésticas (SOHO).

WPA2 es la última generación de seguridad Wi-Fi. WPA2 es la implementación interoperable de Wi-Fi Alliance del estándar IEEE 802.11i ratificado. WPA2 implementa el algoritmo de cifrado estándar de cifrado avanzado (AES) recomendado por el Instituto Nacional de Normas y Tecnología (NIST) con el uso del modo de contador con el protocolo de código de autenticación de mensajes de encadenamiento de bloques de cifrado (CCMP). AES Counter Mode es un cifrado de bloques que cifra bloques de datos de 128 bits a la vez con una clave de cifrado de 128 bits. WPA2 ofrece un mayor nivel de seguridad que WPA. WPA2 crea nuevas claves de sesión en cada asociación. Las claves de encriptación que WPA2 utiliza para cada cliente de la red son únicas y específicas para ese cliente. En última instancia, cada paquete que se envía por el aire se cifra con una clave única.

Tanto WPA1 como WPA2 pueden utilizar la encriptación TKIP o CCMP. (Es cierto que algunos puntos de acceso y algunos clientes restringen las combinaciones, pero hay cuatro combinaciones posibles). La diferencia entre WPA1 y WPA2 se encuentra en los elementos de información que se ponen en las balizas, las tramas de asociación y las tramas de entrada en contacto de 4 vías. Los datos de estos elementos de información son básicamente los mismos,

pero el identificador utilizado es diferente. La diferencia principal en el intercambio de señales de clave es que WPA2 incluye la clave de grupo inicial en el intercambio de señales de 4 direcciones y se omite el primer intercambio de señales de clave de grupo, mientras que WPA necesita realizar este intercambio de señales adicional para entregar las claves de grupo iniciales. El reajuste de la clave del grupo ocurre de la misma manera. El intercambio de señales se produce antes de seleccionar y utilizar el conjunto de cifrado (TKIP o AES) para la transmisión de datagramas de usuario. Durante el intercambio de señales WPA1 o WPA2, se determina el conjunto de claves que se utilizará. Una vez seleccionado, el conjunto de cifrado se utiliza para todo el tráfico de usuarios. Por lo tanto, WPA1 más AES no es WPA2. WPA1 permite (pero a menudo está limitado en el lado del cliente) el cifrado TKIP o AES.

P. ¿Qué es AES?

A. AES significa estándar de cifrado avanzado. AES ofrece una encriptación mucho más fiable. AES utiliza el algoritmo Rijndael, que es un cifrado de bloques con soporte de claves de 128, 192 y 256 bits y es mucho más fuerte que RC4. Para que los dispositivos WLAN admitan AES, el hardware debe soportar AES en lugar de WEP.

P. ¿Qué métodos de autenticación admite un servidor de Servicio de autenticación de Internet (IAS) de Microsoft?

A. IAS admite estos protocolos de autenticación:

- Protocolo de autenticación de contraseña (PAP)
- Protocolo de autenticación de contraseña Shiva (SPAP)
- Protocolo de autenticación por desafío mutuo (CHAP)
- Protocolo de autenticación por desafío mutuo de Microsoft (MS-CHAP)
- Protocolo de autenticación por desafío mutuo de Microsoft versión 2 (MS-CHAP v2)
- Protocolo de autenticación extensible: resumen de mensajes 5 CHAP (EAP-MD5 CHAP)
- EAP-seguridad de la capa de transporte (EAP-TLS)
- EAP-MS-CHAP v2 protegido (PEAP-MS-CHAP v2) (también conocido como PEAPv0/EAP-MSCHAPv2)

PEAP-TLS IAS en Windows 2000 Server soporta PEAP-MS-CHAP v2 y PEAP-TLS cuando se instala Windows 2000 Server Service Pack 4. Para obtener más información, consulte Métodos de Autenticación para su uso con IAS .

P. ¿Cómo se implementa VPN en un entorno inalámbrico?

A. VPN es un mecanismo de seguridad de Capa 3; los mecanismos de cifrado inalámbrico se implementan en la capa 2. VPN se implementa a través de 802.1x , EAP , WEP , TKIP y AES. Cuando hay un mecanismo de Capa 2 en funcionamiento, la VPN agrega sobrecarga a la implementación. En lugares como los hotspots públicos y los hoteles donde no se implementa ninguna seguridad, VPN sería una solución útil para implementar.

Preguntas frecuentes sobre Troubleshooting y Diseño

P. ¿Existen prácticas recomendadas para implementar la seguridad inalámbrica en una LAN inalámbrica exterior?

A. Consulte Prácticas Recomendadas Para La Seguridad Inalámbrica Exterior. Este documento proporciona información sobre las prácticas recomendadas de seguridad para implementar una LAN inalámbrica exterior.

P. ¿Puedo utilizar un servidor Windows 2000 o 2003 con Active Directory para que un servidor RADIUS autentique a los clientes inalámbricos?

A. El servidor Windows 2000 o 2003 con un directorio activo puede funcionar como servidor RADIUS. Para obtener información sobre cómo configurar este servidor RADIUS, debe ponerse en contacto con Microsoft, ya que Cisco no admite la configuración del servidor de Windows.

P. Mi sitio está a punto de migrar de una red inalámbrica abierta (AP de las series 350 y 1200) a una red PEAP. Me gustaría que el SSID ABIERTO (un SSID configurado para la autenticación abierta) y el SSID PEAP (un SSID configurado para la autenticación PEAP) funcionen en el mismo AP al mismo tiempo. Esto nos da tiempo para migrar los clientes al PEAP SSID. ¿Hay alguna manera de alojar simultáneamente un SSID abierto y un SSID PEAP en el mismo AP?

A. Los AP de Cisco admiten VLAN (sólo capa 2). Esta es en realidad la única manera de lograr lo que quieres hacer. Debe crear dos VLAN (nativa y la otra VLAN). A continuación, puede tener una clave WEP para una y ninguna clave WEP para otra. De esta manera, puede configurar una de las VLAN para la autenticación abierta y la otra VLAN para la autenticación PEAP. Consulte Uso de VLAN con Cisco Aironet Wireless Equipment si desea entender cómo configurar las VLAN.

Tenga en cuenta que debe configurar los switches para dot1Q y para el ruteo entre VLAN, su switch L3 o su router.

P. Deseo configurar mi Cisco AP 1200 VxWorks para que los usuarios inalámbricos se autentiquen en un Cisco 3005 VPN Concentrator. ¿Qué configuración debe estar presente en el AP y los clientes para lograr esto?

A. No hay una configuración específica necesaria en el AP o los clientes para este escenario. Debe realizar todas las configuraciones en el concentrador VPN.

P. Estoy implementando un Cisco 1232 AG AP. Me gustaría conocer el método más seguro que puedo implementar con este AP. No tengo un servidor AAA y mis únicos recursos son el AP y un dominio Windows 2003. Conozco cómo utilizar claves WEP estáticas de 128 bits, restricciones de dirección MAC y SSID no broadcast. La mayoría de los usuarios trabajan con estaciones de trabajo de Windows XP y algunos PDA. ¿Cuál es la implementación más segura para esta configuración?

A. Si no tiene un servidor RADIUS como el Cisco ACS, puede configurar su AP como un servidor RADIUS local para la autenticación LEAP, EAP-FAST o MAC.

Nota: Un punto muy importante que debe tener en cuenta es si desea utilizar sus clientes con LEAP o EAP-FAST. Si es así, sus clientes deben tener una utilidad para soportar LEAP o EAP-FAST. La utilidad de Windows XP sólo admite PEAP o EAP-TLS.

P. La autenticación PEAP falla con el error "Error de autenticación EAP-TLS o PEAP durante el intercambio de señales SSL". ¿Por qué?

A. Este error puede ocurrir debido al ID de bug Cisco CSCee06008 **(sólo clientes registrados).** PEAP falla con ADU 1.2.0.4. La solución temporal para este problema es utilizar la última versión de la ADU.

P. ¿Puedo tener autenticación WPA y MAC local en el mismo SSID?

A. El punto de acceso de Cisco no admite la autenticación MAC local ni la clave precompartida de acceso Wi-Fi protegido (WPA-PSK) en el mismo identificador de conjunto de servicios (SSID). Cuando habilita la autenticación MAC local con WPA-PSK, WPA-PSK no funciona. Este problema ocurre porque la autenticación MAC local elimina la línea de contraseña ASCII WPA-PSK de la configuración.

P. Actualmente tenemos tres puntos de acceso inalámbricos Cisco 1231 configurados con cifrado WEP de 128 bits Ciphers para nuestra VLAN de datos. No transmitimos el SSID. No tenemos un servidor RADIUS separado en nuestro entorno. Alguien pudo determinar la clave WEP mediante una herramienta de análisis y la utilizó durante un par de semanas para supervisar el tráfico inalámbrico. ¿Cómo podemos evitarlo y proteger la red?

A. El WEP estático es vulnerable a este problema y se puede derivar si un hacker captura suficientes paquetes y puede obtener dos o más paquetes con el mismo vector de inicialización (IV).

Hay varias maneras de evitar que ocurra este problema:

1. Utilice claves WEP dinámicas.
2. Utilice WPA.
3. Si sólo tiene adaptadores Cisco, active Per Packet Key y MIC.

P. Si tengo dos WLAN diferentes, ambas configuradas para Wi-Fi Protected Access (WPA)-Pre-Shared Key (PSK), ¿las claves previamente compartidas pueden ser diferentes por WLAN? Si son diferentes, ¿afecta a la otra WLAN configurada con una clave previamente compartida diferente?

A. La configuración de WPA-PSK debe ser por WLAN. Si cambia un WPA-PSK, no debería afectar a la otra WLAN configurada.

P. En mi entorno utilizo principalmente Intel Pro/Wireless, Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) y Cisco Secure Access Control Server (ACS) 3.3 enlazados a cuentas de Windows Active Directory (AD). El problema es que cuando la contraseña de usuario está a punto de caducar, Windows no le pide al usuario que cambie la contraseña. Finalmente, la cuenta vence. ¿Hay alguna solución para que Windows pida al usuario que cambie la contraseña?

A. La función de envejecimiento de la contraseña de Cisco Secure ACS le permite obligar a los usuarios a cambiar sus contraseñas en una o más de estas condiciones:

- Después de un número de días especificado (reglas de antigüedad por fecha)
- Después de un número especificado de inicios de sesión (reglas de antigüedad por uso)
- La primera vez que un nuevo usuario inicia sesión (regla de cambio de contraseña)

Para obtener detalles sobre cómo configurar Cisco Secure ACS para esta función, refiérase a Habilitación del Antigüedad de la Contraseña para la Base de Datos de Usuario de CiscoSecure.

P. Cuando un usuario inicia sesión de forma inalámbrica con LEAP, obtiene su secuencia de comandos de inicio de sesión para asignar unidades de red. Sin embargo, mediante el acceso Wi-Fi protegido (WPA) o WPA2 con autenticación PEAP, los scripts de inicio de sesión no se ejecutan. Tanto el cliente como el punto de acceso son Cisco, al igual que RADIUS (ACS). ¿Por qué el script de inicio de sesión no se ejecuta en RADIUS (ACS)?

A. La autenticación del equipo es obligatoria para que los scripts de inicio de sesión funcionen. Esto permite a los usuarios inalámbricos obtener acceso a la red para cargar scripts antes de que el usuario inicie sesión.

Para obtener información sobre cómo configurar la autenticación de la máquina con PEAP-MS-CHAPv2, refiérase a Configuración de Cisco Secure ACS para Windows v3.2 con autenticación de la máquina PEAP-MS-CHAPv2.

P. Con la versión 3.0 de Cisco Aironet Desktop Utility (ADU), cuando un usuario configura la autenticación de equipo para el protocolo de autenticación ampliable-seguridad de capa de transporte (EAP-TLS), ADU no permite al usuario crear un perfil. ¿Por qué?

A. Esto se debe al Id. de bug Cisco CSCsg32032 (sólo clientes registrados) . Esto puede suceder si el equipo cliente tiene instalado el certificado de equipo y no tiene un certificado de usuario.

La solución alternativa es copiar el certificado de la máquina en el almacén de usuarios, crear un perfil EAP-TLS y, a continuación, quitar el certificado del almacén de usuarios para la configuración de autenticación de la máquina solamente.

P. ¿Hay alguna manera de asignar VLAN en la LAN inalámbrica basada en la dirección MAC del cliente?

A. Esto no es posible. La asignación de VLAN desde el servidor RADIUS sólo funciona con 802.1x, no con la autenticación MAC. Puede utilizar RADIUS para pulsar VSA con autenticación MAC, si las direcciones MAC se autentican en el servidor RADIUS (definido como ID de usuario/contraseña en LEAP/PEAP).

Información Relacionada

- Seguridad de red inalámbrica
- Informe técnico de seguridad de LAN inalámbrica

- Descripción general de la seguridad de LAN inalámbrica
- Guía de implementación de EAP-TLS para redes LAN inalámbricas
- LEAP de Cisco
- Configuración de Privacidad equivalente al cableado (WEP)
- Soporte de Productos de Red Inalámbrica
- Soporte Técnico y Documentación - Cisco Systems