

PREGUNTAS MÁS FRECUENTES SOBRE AIRONET WIRELESS SECURITY

Contenido

[Introducción](#)

[Preguntas Frecuentes Generales](#)

[El resolver problemas y diseño FAQ](#)

[Información Relacionada](#)

Introducción

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

Preguntas Frecuentes Generales

Q. ¿Cuál es la necesidad de la seguridad de red inalámbrica?

A. En una red alámbrica, sigue habiendo los datos en los cables que conectan los dispositivos extremos. Pero las redes inalámbricas transmiten y reciben los datos con un broadcast de las señales RF en el aire libre. Debido a la naturaleza del broadcast que uso WLAN, hay una mayor amenaza de piratas informáticos o los intrusos que pueden acceder o corrompen los datos. Para paliar este problema, todos los WLAN requieren la adición de:

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

Q. ¿Cuáles son los diversos métodos de autenticación que el estándar del 802.11 para la Tecnología inalámbrica LAN define?

A. El estándar del 802.11 define dos mecanismos para autenticación de los clientes del Wireless LAN:

1. Autenticación abierta
2. Clave de autenticación compartida

Hay dos otros mecanismos de uso general también:

1. autenticación SSID-basada
2. Autenticación de la dirección MAC

Q. ¿Cuál es autenticación abierta?

A. La autenticación abierta es básicamente un algoritmo de la autenticación nula, así que significa que no hay verificación del usuario o de la máquina. La autenticación abierta permite cualquier dispositivo que ponga un pedido de autenticación al punto de acceso. La autenticación abierta utiliza la transmisión del texto claro para permitir que un cliente se asocie a un AP. Si se habilita el no encryption, cualquier dispositivo que conozca el SSID de la red inalámbrica (WLAN) puede acceder en la red. Si el Wired Equivalent Privacy (WEP) se habilita en el AP, la clave WEP llega a ser los medios del control de acceso. Un dispositivo que no tiene la clave WEP correcta no puede transmitir los datos con el AP incluso si la autenticación es acertada. Ningunos pueden tales datos del decrypt del dispositivo que el AP envíe.

Q. ¿Qué pasos la autenticación abierta implica para que un cliente asocie al AP?

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

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

A. Aquí están las ventajas y desventajas de la autenticación abierta:

Ventajas: La autenticación abierta es un mecanismo de autenticación básica, que usted puede utilizar con los dispositivos de red inalámbrica que no soportan los algoritmos de autenticación complejos. La autenticación en la especificación del 802.11 Conectividad-se orienta. Por el diseño los requisitos para autenticación permiten que los dispositivos ganen el acceso rápido a la red. En tal caso, usted puede utilizar la autenticación abierta.

Desventajas: La autenticación abierta no proporciona ninguna manera de marcar si un cliente es un cliente válido y no un cliente pirata. Si usted no utiliza la encriptación WEP con la autenticación abierta, cualquier usuario que conozca el SSID de la red inalámbrica (WLAN) puede acceder la red.

Q. ¿Cuál es clave de autenticación compartida?

A. La clave de autenticación compartida funciona similar a la autenticación abierta con una diferencia principal. Cuando usted utiliza la autenticación abierta con la clave de encriptación WEP, la clave WEP se utiliza para cifrar y para descifrar los datos, pero no se utiliza en el paso de la autenticación. En la clave de autenticación compartida, la encriptación WEP se utiliza para la autenticación. Como la autenticación abierta, la clave de autenticación compartida requiere el cliente y el AP tener la misma clave WEP. El AP que utiliza la clave de autenticación compartida envía un paquete de texto de desafío al cliente. El cliente utiliza la clave WEP localmente configurada para cifrar el texto de impugnación y para contestar con una petición de la autenticación subsiguiente. Si el AP puede descifrar el pedido de autenticación y extraer el texto de impugnación original, el AP responde con una respuesta de autenticación que conceda el acceso al cliente.

Q. ¿Qué pasos la clave de autenticación compartida implica para que un cliente asocie al AP?

1. El cliente envía una petición de la sonda a los AP.
2. Los AP devuelven las respuestas de la sonda.
3. El cliente evalúa las respuestas AP y selecciona el mejor AP.
4. El cliente envía un pedido de autenticación al AP.
5. El AP envía una respuesta de autenticación que contenga el texto de impugnación unencrypted.
6. El cliente cifra el texto de impugnación con la clave WEP y envía el texto al AP.
7. El AP compara el texto de impugnación unencrypted con el texto de impugnación cifrado. Si la autenticación puede descifrar y extraer el texto de impugnación original, la autenticación es acertada.

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

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

A. En la clave de autenticación compartida, el cliente y el AP intercambian el texto de impugnación (texto claro) y el desafío cifrado. Por lo tanto, este tipo de autenticación es vulnerable al ataque del intermediario. Un hacker puede escuchar el desafío unencrypted y el desafío cifrado, y extrae la clave WEP (clave compartida) de esta información. Cuando un hacker conoce la clave WEP, se compromete el mecanismo de autenticación entero y el hacker puede acceder la red WLAN. Ésta es la desventaja principal con la clave de autenticación compartida.

Q. ¿Cuál es autenticación de la dirección MAC?

A. Aunque el estándar del 802.11 no especifique la autenticación de la dirección MAC, las redes WLAN utilizan comúnmente esta técnica de autenticación. Por lo tanto, la mayor parte de los vendedores del dispositivo de red inalámbrica, incluyendo Cisco, soportan la autenticación de la dirección MAC.

En la autenticación de la dirección MAC, autentican a los clientes sobre la base de su dirección MAC que las direcciones MAC de los clientes se verifican contra una lista de direcciones MAC salvadas localmente en el AP o en un servidor de autenticación externa. La autenticación de MAC es un mecanismo de seguridad más fuerte que el abierta y las claves de autenticación compartida que el 802.11 proporciona. Esta forma de autenticación más futura reduce la probabilidad de dispositivos no autorizados que puede acceder la red.

Q. ¿Por qué la autenticación de MAC no trabaja con el Acceso protegido de Wi-Fi (WPA) en el Cisco IOS Software Release 12.3(8)JA2?

A. El único nivel de seguridad para la autenticación de MAC es marcar la dirección MAC del cliente contra una lista de direcciones MAC permitidas. Esto se considera muy débil. En versiones de Cisco IOS Software anteriores, usted podría configurar la autenticación de MAC y el WPA para cifrar la información. Pero porque el WPA sí mismo tiene una dirección MAC que marque, Cisco decidía a no permitir los este tipos de configuración en versiones de Cisco IOS Software posteriores y decididos para mejorar solamente las funciones de seguridad.

Q. ¿Puedo utilizar el SSID como método para autenticar los dispositivos de red inalámbrica?

A. El Service Set Identifier (SSID) es un valor único, con diferenciación entre mayúsculas y minúsculas, alfanumérico que los WLAN utilizan como nombre de red. El SSID es a - el mecanismo que permite la separación lógica de la Tecnología inalámbrica LAN. El SSID no proporciona ninguna funciones de la privacidad de los datos, ni el SSID autentica verdad al cliente al AP. El valor SSID se transmite como texto claro en los faros, las respuestas de las peticiones de la sonda, de la sonda, y otros tipos de bastidores. Un eavesdropper puede determinar fácilmente el SSID con el uso de un analizador de paquete del Wireless LAN del 802.11, por ejemplo, Sniffer Pro. Cisco no recomienda que usted utiliza el SSID como método para asegurar su red WLAN.

Q. ¿Si inhabilito el broadcast SSID, puedo alcanzar la seguridad mejorada en una red WLAN?

A. Cuando usted inhabilita el broadcast SSID, el SSID no se envía en los mensajes del faro. Sin embargo, otras tramas por ejemplo, peticiones de la sonda y respuestas de la sonda todavía tienen el SSID en el texto claro. Usted no alcanza tan la seguridad de red inalámbrica aumentada si usted inhabilita el SSID. El SSID no se diseña, ni se piensa para el uso, como mecanismo de seguridad. Además, si usted inhabilita los broadcasts SSID, usted puede encontrar los problemas con la Interoperabilidad del Wi-Fi para las implementaciones del mezclado-cliente. Por lo tanto, Cisco no recomienda que usted utiliza el SSID como modo de seguridad.

Q. ¿Cuáles son las vulnerabilidades encontradas en la Seguridad del 802.11?

A. Las vulnerabilidades principales de la Seguridad del 802.11 pueden ser resumidas como sigue:

- Autenticación débil del dispositivo-solamente: Se autentican los dispositivos del cliente, no los usuarios.
- Encriptación de datos débil: El Wired Equivalent Privacy (WEP) ha sido ineficaz probado como los medios de cifrar los datos.
- Ninguna Integridad del mensaje: El valor de la verificación de la integridad (ICV) ha sido ineficaz probado como los medios de asegurar la Integridad del mensaje.

Q. ¿Cuál es el papel de la autenticación del 802.1x en la red inalámbrica (WLAN)?

A. Para dirigir los defectos y las vulnerabilidades de seguridad en los métodos originales de autenticación que el estándar del 802.11 define, el marco de autenticación del 802.1x se incluye en el proyecto para las mejoras de la seguridad de la capa MAC del 802.11. El Grupo de tareas del IEEE 802.11 i (TG*i*) está desarrollando actualmente estas mejoras. El marco del 802.1x proporciona la capa de link con la autenticación ampliable, considerada normalmente solamente en las capas superiores.

Q. ¿Cuáles son las tres entidades que el marco del 802.1x define?

A. el marco del 802.1x requiere estas tres entidades lógicas validar los dispositivos en una red WLAN.



1. **Supplicant** — El supplicant reside en el cliente del Wireless LAN, y también se conoce como los clientes EAP.
2. **Authenticator** — El authenticator reside en el AP.
3. **Servidor de autenticación** — El servidor de autenticación reside en el servidor de RADIUS.

Q. ¿Cómo una autenticación de cliente de red inalámbrica ocurre cuando utilizo el marco de autenticación del 802.1x?

A. Cuando el cliente de red inalámbrica (clientes EAP) hace activo, el cliente de red inalámbrica autentica con la autenticación abierta o compartida. el 802.1x trabaja con la autenticación abierta y comienza después de que el cliente se asocie con éxito al AP. La estación del cliente puede asociarse, pero puede pasar el tráfico de datos sólo después de la autenticación acertada del 802.1x. Aquí están los pasos en la autenticación del 802.1x:

1. El AP (authenticator) configurado para el 802.1x pide la identidad del usuario del cliente.
2. Los clientes responden con su identidad dentro de un período de tiempo estipulado.
3. El servidor marca 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 autentican al cliente, el servidor adelanta que la clave de encriptación al AP que se utiliza para cifrar/tráfico del decrypt envió a y desde el cliente.
6. En el paso 4, si la identidad del usuario no está presente en la base de datos, el servidor cae la autenticación y envía un mensaje de error al AP.
7. El AP adelanta este mensaje al cliente, y el cliente deben autenticar otra vez con las credenciales correctas.

Nota: En la autenticación del 802.1x, AP apenas adelanta los mensajes de autenticación a y desde el cliente.

Q. ¿Cuáles son las diversas variantes de EAP que puedo utilizar con el marco de autenticación del 802.1x?

A. el 802.1x define el procedimiento para autenticar a los clientes. El tipo EAP usado en el marco del 802.1x define el tipo de credencial y el método de autenticación usados en el intercambio del 802.1x. El marco del 802.1x puede utilizar ninguno de estos variantes de EAP:

- EAP-TLS — Protocolo extensible authentication Transport Layer Security
- EAP-FAST — Autenticación adaptable de EAP vía el túnel asegurado
- EAP-SIM — Módulo de identidad del suscriptor EAP
- Cisco LEAP — Protocolo lightweight extensible authentication
- EAP-PEAP — Protocolo extensible authentication protegido EAP
- EAP-MD5 — Algoritmo 5 de la publicación de mensaje EAP

- EAP-OTP — Contraseña puntual EAP
- EAP-TTLS — Transport Layer Security tunneled EAP

Q. ¿Cómo elijo un método EAP del 802.1x de las diversas variantes disponibles?

A. La mayoría del factor importante que usted debe considerar es si el método EAP es con la red existente o no compatible. Además, Cisco recomienda que usted elige un método que soporte la autenticación recíproca.

Q. ¿Cuál es autenticación EAP local?

A. El EAP local es un mecanismo en el cual el WLC actúa como servidor de autenticación. Los credenciales de usuario se salvan localmente en el WLC para autenticar a los clientes de red inalámbrica, que actúa como proceso backend en las oficinas remotas cuando va el servidor abajo. Los credenciales de usuario se pueden extraer de la base de datos local en el WLC o de un servidor LDAP externo. El SALTO, el EAP-FAST, el EAP-TLS, PEAPv0/MSCHAPv2, y PEAPv1/GTC son diversas autenticaciones EAP soportadas por el EAP local.

Q. ¿Cuál es Cisco LEAP?

A. El protocolo lightweight extensible authentication (SALTO) es un método propietario de Cisco de autenticación. El Cisco LEAP es un tipo de autenticación del 802.1x para la Tecnología inalámbrica LAN (WLAN). El Cisco LEAP soporta la autenticación recíproca fuerte entre el cliente y un servidor de RADIUS con una contraseña del inicio como el secreto compartido. El Cisco LEAP proporciona dinámico por usuario, las claves de encriptación del por session. El SALTO es el menos método complicado para desplegar el 802.1x, y requiere solamente a un servidor de RADIUS. Refiera al [Cisco LEAP](#) para la información sobre el SALTO.

Q. ¿Cómo el EAP-FAST trabaja?

A. El EAP-FAST utiliza los algoritmos de la clave simétrica para alcanzar un proceso de autenticación tunneled. El establecimiento del túnel confía en los credenciales protegidos del acceso (PAC) que ese EAP-FAST puede ser aprovisionado y manejado dinámicamente por el EAP-FAST a través del servidor del Authentication, Authorization, and Accounting (AAA) (tal como el [ACS] v. 3.2.3 del Cisco Secure Access Control Server). Con un túnel mutuamente autenticado, el EAP-FAST ofrece la protección contra los establecimientos de diccionario y las vulnerabilidades hombre-en-medias. Aquí están las fases de EAP-FAST:

El EAP-FAST no sólo atenúa los riesgos de los establecimientos de diccionario y de los ataques del intermediario pasivos, pero también habilita la autenticación segura basada en la infraestructura actualmente desplegada.

- Fase 1: Establezca el túnel mutuamente autenticado — El cliente y el servidor de AAA utilizan el PAC para autenticarse y para establecer un túnel seguro.
- Fase 2: Realice la autenticación de cliente en el túnel establecido — El cliente envía el Nombre de usuario y la contraseña para autenticar y para establecer la política de autorización de clientes.
- Opcionalmente, fase 0 — La autenticación del EAP-FAST utiliza infrecuentemente esta fase para permitir al cliente para ser dinámicamente aprovisionado con un PAC. Esta fase genera por usuario los credenciales del acceso con seguridad entre el usuario y la red. La fase 1 de

la autenticación utiliza estos por usuario credenciales, conocidos como el PAC.
Refiera al [EAP-FAST de Cisco](#) para más información.

Q. ¿Hay los documentos en cisco.com que explican cómo configurar el EAP en una red WLAN de Cisco?

A. Refiera a la [autenticación EAP con el servidor de RADIUS](#) para la información sobre cómo configurar la autenticación EAP en una red WLAN.

Refiera a la [nota de aplicación protegida EAP](#) para la información sobre cómo configurar la autenticación PEAP.

Refiera a la [autenticación LEAP con un servidor de RADIUS local](#) para la información sobre cómo configurar la autenticación LEAP.

Q. ¿Cuáles son los diversos mecanismos de encriptación más de uso general de las redes inalámbricas?

A. Aquí están los esquemas de encriptación más de uso general usados en las redes inalámbricas:

- WEP
- TKIP
- AES

El AES es un método de encriptación por hardware, mientras que el cifrado WEP y TKIP se procesa en el firmware. Con la actualización del firmware un WEP los dispositivos pueden soportar el TKIP así que son interoperables. El AES es el método más seguro y más rápido, mientras que el WEP es el lo más menos posible seguro.

Q. ¿Cuál es encriptación WEP?

A. WEP significa Wired Equivalent Privacy. El WEP se utiliza para cifrar y para descifrar las Señales de datos que transmiten entre los 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. Mientras que el estándar especifica, el WEP utiliza el algoritmo RC4 con una clave 40-bit o del 104-bit. RC4 es un algoritmo simétrico porque RC4 utiliza la misma clave para el cifrado y el descifrado de datos. Cuando se habilita el 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.

Refiera a [configurar el Wired Equivalent Privacy \(WEP\)](#) para la información sobre cómo configurar el WEP.

Q. ¿Cuál es rotación dominante transmitida? ¿Cuál es la frecuencia de la rotación de la clave de broadcast?

A. La rotación dominante del broadcast permite que el AP genere la clave al azar mejor del grupo. Transmite la rotación dominante pone al día periódicamente a todos los clientes capaces de la administración de claves. Cuando usted habilita la rotación de la clave WEP del broadcast, el AP

proporciona una clave WEP dinámica del broadcast y cambia la clave en el intervalo que usted fija. La rotación dominante del broadcast es una excelente alternativa al TKIP si su Wireless LAN soporta los dispositivos de red inalámbrica de cliente o los dispositivos del no Cisco que usted no puede actualizar a la última versión de firmware para los dispositivos del cliente de Cisco. Refiera a [habilitar y a inhabilitar la rotación dominante transmitida](#) para la información sobre cómo configurar la característica de la rotación de la clave del broadcast.

Q. ¿Cuál es TKIP?

A. Protocolo de integridad de clave temporal de la significa TKIP. El TKIP fue introducido para dirigir los defectos en la encriptación WEP. El TKIP también se conoce como función resumen de generación de clave WEP y fue llamado inicialmente WEP2. El TKIP es una solución temporaria que repara el problema de la reutilización de la clave WEP. El TKIP utiliza el algoritmo RC4 para realizar el cifrado, que es lo mismo que el WEP. Una diferencia principal del WEP es que el TKIP cambia la clave temporal cada paquete. Los cambios dominantes temporales cada paquete porque el valor de troceo para cada paquete cambia.

Q. ¿Pueden los dispositivos que utilice el TKIP interoperaron con los dispositivos que utilizan la encriptación WEP?

A. Una ventaja con el TKIP es que los WLAN con los AP WEP-basados existentes y las radios pueden actualizar al TKIP a través de las correcciones simples del firmware. También, el equipo WEP-solamente todavía interopera con los dispositivos TKIP-habilitados que utilizan el WEP.

Q. ¿Cuál es el Message Integrity Check (MIC)?

A. El MIC es otra mejora para dirigir las vulnerabilidades en la encriptación WEP. El MIC previene los ataques del bit-tirón en los paquetes encriptados. Durante un ataque del bit-tirón, un intruso intercepta un mensaje encriptado, altera el mensaje y después retransmite el mensaje alterado. El receptor no sabe que el mensaje es corrupto y no legítimo. Para abordar este problema, la característica MIC agrega un campo MIC a la trama de red inalámbrica. El campo MIC proporciona una verificación de la integridad de la trama que no sea vulnerable a los mismos defectos matemáticos que el ICV. El MIC también agrega un campo del número de secuencia a la trama de red inalámbrica. El AP cae las tramas recibió fuera de servicio.

Q. ¿Cuál es WPA? ¿Cómo es el WPA2 diferente del WPA?

A. El WPA es una solución acerca de la seguridad estándar basada del Wi-Fi Alliance que dirige las vulnerabilidades en los WLAN nativos. El WPA proporciona la protección de datos y el control de acceso aumentados para los sistemas WLAN. El WPA dirige todas las vulnerabilidades sabidas del Wired Equivalent Privacy (WEP) en la instrumentación de seguridad original del IEEE 802.11 y trae una solución acerca de la seguridad inmediata a las redes WLAN en los entornos de la empresa y del oficina pequeña, oficina en el hogar (SOHO).

El WPA2 es la última generación de Seguridad del Wi-Fi. El WPA2 es la implementación interoperable del Wi-Fi Alliance del estándar ratificado de IEEE 802.11i. El WPA2 implementa el National Institute of Standards and Technology (NIST) - algoritmo de encriptación recomendado del Advanced Encryption Standard (AES) con el uso del modo contrario con el protocolo del Message Authentication Code del Cipher Block Chaining (CCMP). El El modo contador AES es un cifrado en bloque que cifra los bloques del 128-bit del en un momento de los datos con una clave de encriptación del 128-bit. El WPA2 ofrece un de alto nivel de la Seguridad que el WPA. El WPA2

crea las claves de la sesión frescas en cada asociación. Las claves de encriptación que el WPA2 utiliza para cada cliente en la red son únicas y específicas a ese cliente. En última instancia, cada paquete que se envía sobre el aire se cifra con una clave única.

WPA1 y el WPA2 pueden utilizar el cifrado TKIP o del CCMP. (Es verdad que algunos Puntos de acceso y algunos clientes restringen las combinaciones, pero allí son cuatro combinaciones posible.). La diferencia entre WPA1 y el WPA2 está en los elementos de información que consiguen puestos en los faros, las tramas de la asociación, y las tramas del apretón de manos 4-way. Los datos en estos elementos de información son básicamente lo mismo, pero el identificador usado es diferente. La diferencia principal en el apretón de manos dominante es que el WPA2 incluye la clave inicial del grupo en el apretón de manos 4-way y el apretón de manos dominante del primer grupo está saltado, mientras que el WPA necesita hacer este apretón de manos adicional para entregar las claves iniciales del grupo. La reintroducción de la clave del grupo sucede de la misma manera. El apretón de manos ocurre antes de la selección y del uso de la habitación de la cifra (TKIP o AES) para la transmisión de los datagramas del usuario. Durante el apretón de manos WPA1 o del WPA2, la habitación de la cifra a utilizar se determina. Una vez que está seleccionada, la habitación de la cifra se utiliza para todo el tráfico de usuarios. Así WPA1 más el AES no es WPA2. WPA1 permite (pero es a menudo limitado lateral del cliente) la cifra TKIP o AES.

Q. ¿Cuál es AES?

A. Advanced Encryption Standard de la significa AES. El AES ofrece un cifrado mucho más fuerte. El AES utiliza el algoritmo Rijndael, que es un cifrado en bloque con 128-, 192-, y el soporte de la clave del 256-bit y es mucho más fuerte que el RC4. Para que los dispositivos WLAN soporten el AES, el hardware debe soportar el AES en vez del WEP.

Q. ¿Qué métodos de autenticación son soportados por un servidor del Internet Authentication Service de Microsoft (IAS)?

A. IAS soporta estos Protocolos de autenticación:

- Protocolo password authentication (PAP)
- Protocolo de autenticación de contraseña Shiva (SPAP)
- Challenge Handshake Authentication Protocol (CHAP)
- Protocolo microsoft challenge handshake authentication (MS-CHAP)
- Protocolo microsoft challenge handshake authentication versión 2 (v2 MS-CHAP)
- GRIETA del Extensible Authentication Protocol Message Digest 5 (GRIETA del EAP-MD5)
- Seguridad de la capa del EAP-transporte (EAP-TLS)
- V2 protegido EAP-MS-CHAP (v2 PEAP-MS-CHAP) (también conocido como PEAPv0/EAP-MSCHAPv2)

PEAP-TLS IAS en Windows 2000 Server soporta el v2 PEAP-MS-CHAP y PEAP-TLS cuando Windows 2000 Server el Service Pack 4 está instalado. Para más información, refiera a los [métodos de autenticación para el uso con IAS](#) .

Q. ¿Cómo el VPN se implementa en un environment sin hilos?

A. El VPN es un mecanismo de seguridad de la capa 3; los mecanismos de encriptación sin hilos se implementan en la capa 2. VPN se implementan sobre el 802.1x, el EAP, el WEP, el TKIP, y el AES. Cuando un mecanismo de la capa 2 existe, el VPN agrega por encima a la implementación.

En los lugares como los hotspots públicos y los hoteles en donde no se implementa ninguna Seguridad, el VPN sería una solución útil a implementar.

El resolver problemas y diseño FAQ

Q. ¿Hay mejores prácticas de desplegar la seguridad de red inalámbrica en las Redes inalámbricas exteriores LAN?

A. Refiera a las [mejores prácticas para la Seguridad de las Redes inalámbricas exteriores](#). Este documento proporciona la información sobre las mejores prácticas de la Seguridad de desplegar las Redes inalámbricas exteriores LAN.

Q. ¿Puedo utilizar un Windows 2000 o un servidor 2003 con el Active Directory para que un servidor de RADIUS autentique a los clientes de red inalámbrica?

A. El Windows 2000 o el servidor 2003 con un Active Directory puede trabajar como servidor de RADIUS. Para la información sobre cómo configurar a este servidor de RADIUS, usted necesita entrar en contacto Microsoft, porque Cisco no soporta la configuración de Servidor Windows.

Q. Mi sitio está a punto de emigrar de una red inalámbrica abierta (350 y 1200 Series AP) a una red PEAP. Quisiera tener el SSID ABIERTO (un SSID configurado para la autenticación abierta) y el trabajo PEAP SSID (un SSID configurado para la autenticación PEAP) sobre el mismo AP al mismo tiempo. Esto nos da la hora de emigrar a los clientes al PEAP SSID. ¿Hay una manera de recibir en paralelo un SSID abierto y un PEAP SSID en el mismo AP?

A. Cisco AP soporta los VLA N (capa 2 solamente). Ésta es realmente la única forma de alcanzar lo que usted quiere hacer. Usted necesita crear dos VLA N, (natural y su otro VLA N). Entonces usted puede tener una clave WEP para una y ninguna clave WEP para otra. Esta manera, usted puede configurar uno de los VLA N para la autenticación abierta y del otro VLA N para la autenticación PEAP. Refiérase [con los VLA N con el equipo de red inalámbrica del Cisco Aironet](#) si usted quiere entender cómo configurar los VLA N.

Observe por favor que usted necesita configurar su Switches para el dot1q y para inter VLAN rutear, su Switch L3 o su router.

Q. Quiero configurar mi Cisco AP1200 VxWorks para tener los usuarios de red inalámbrica autenticar al Cisco 3005 un concentrador VPN. ¿Qué configuración necesita estar presente en el AP y los clientes para lograr esto?

A. No hay configuración específica necesaria en el AP o los clientes para este escenario. Usted debe hacer todas las configuraciones en el concentrador VPN.

Q. Estoy desplegando un AG AP de Cisco 1232. Quisiera conocer el método más seguro que puedo desplegar con este AP. No tengo un servidor de AAA y mis solamente recursos son el AP y un dominio de Windows 2003. Soy familiar con cómo utilizar las claves estáticas del 128-bit WEP, el SSID no-broadcast y las restricciones de la dirección MAC. Los usuarios trabajan sobre todo con los puestos

de trabajo de Windows XP y algunos PDA. ¿Cuál es la implementación más segura para esta configuración?

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

Nota: Mismo un punto importante que usted debe considerar es si usted quiere utilizar a sus clientes con el SALTO o el EAP-FAST. Si es así sus clientes deben tener una utilidad para soportar el SALTO o el EAP-FAST. La utilidad de Windows XP soporta solamente el PEAP o el EAP-TLS.

Q. La autenticación PEAP falla con el error “EAP-TLS o autenticación PEAP fallada durante el contacto SSL”. ¿por qué?

A. Este error puede ocurrir debido al Id. de bug Cisco [CSCee06008 \(clientes registrados solamente\)](#). El PEAP falla con ADU 1.2.0.4. La solución alternativa para este problema es utilizar la última versión del ADU.

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

A. Cisco AP no soporta la autenticación y la clave protegida Wi-Fi de la PRE-parte del acceso (WPA-PSK) del MAC local en el mismo Service Set Identifier (SSID). Cuando usted habilita la autenticación del MAC local con el WPA-PSK, el WPA-PSK no trabaja. Este problema ocurre porque la autenticación del MAC local quita la línea de la contraseña WPA-PSK ASCII de la configuración.

Q. Tenemos actualmente tres Cisco 1231 AP inalámbricos puestos con la encriptación WEP del 128-bit de las cifras para nuestro VLAN de dato. No transmitimos el SSID. No tenemos un servidor de RADIUS separado en nuestro entorno. Alguien podía determinar la clave WEP a través de una herramienta de la exploración, y utilizó la herramienta por un par de semanas para monitorear nuestro tráfico de red inalámbrica. ¿Cómo podemos prevenir esto y hacer la red segura?

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

Hay varias maneras de prevenir el acontecimiento de este problema:

1. Utilice las claves WEP dinámicas.
2. Utilice el WPA.
3. Si usted tiene solamente adaptadores de Cisco, habilite por la clave del paquete y el MIC.

Q. ¿Si tengo dos diversos WLAN, ambos configuraron para el Acceso protegido de Wi-Fi (WPA) - clave previamente compartida (PSK), pueden las claves previamente compartidas ser diferentes por la red inalámbrica (WLAN)? ¿Si son diferentes, afecta a la otra red inalámbrica (WLAN) configurada con una diversa clave previamente compartida?

A. La configuración del WPA-PSK debe estar por la red inalámbrica (WLAN). Si usted cambia un WPA-PSK, no debe afectar a la otra red inalámbrica (WLAN) se configura que.

Q. En mi entorno utilizo sobre todo el Pro/Tecnología inalámbrica, autenticación de Protocol Flexible de la autenticación ampliable vía el Tunelización seguro (EAP-FAST), y Cisco Secure Access Control Server (ACS) 3.3 de Intel conectados a las cuentas del Active Directory de Windows (AD). El problema es cuando la contraseña del usuario es alrededor expirar, Windows no indica al usuario que cambie la contraseña. Eventual, la cuenta expira. ¿Hay una solución para hacer prompt de Windows al usuario para cambiar la contraseña?

A. La característica de la desactualización de contraseña del Cisco Secure ACS le permite para forzar a los usuarios a cambiar sus contraseñas bajo uno o más de estas condiciones:

- Después de un número especificado de días (reglas de la edad-por-fecha)
- Después de un número especificado de logines (reglas de los edad-por-usos)
- La primera vez que un usuario nuevo abre una sesión (regla del cambio de la contraseña)

Para los detalles en cómo configurar el Cisco Secure ACS para esta característica, refiera a [habilitar la desactualización de contraseña para la base de datos de usuarios del CiscoSecure](#).

Q. Cuando un usuario abre una sesión sin hilos usando el SALTO consiguen su script del login asociar los controladores de red. Sin embargo, usando el Acceso protegido de Wi-Fi (WPA) o el WPA2 con la autenticación PEAP, los scripts del login no se ejecutan. El cliente y el Punto de acceso son Cisco al igual que el RADIUS (ACS). ¿Por qué el script del login no se ejecuta en el RADIUS (ACS)?

A. La autenticación de la máquina es obligatoria para que los scripts del login trabajen. Esto permite a los usuarios de red inalámbrica para tener el acceso a la red para cargar los scripts antes de que el usuario abra una sesión.

Para la información sobre cómo configurar la autenticación de la máquina con PEAP-MS-CHAPv2, refiera a [configurar el v3.2 del Cisco Secure ACS for Windows con la autenticación de la máquina PEAP-MS-CHAPv2](#).

Q. Con la utilidad de escritorio del Cisco Aironet (ADU) libere el 3.0, cuando un usuario configura la autenticación de la máquina para la Seguridad de la capa del Protocolo-transporte de la autenticación ampliable (EAP-TLS), ADU no permite que el usuario cree un perfil. ¿por qué?

A. Esto está debido al Id. de bug Cisco [CSCsg32032 \(clientes registrados solamente\)](#). Esto puede suceder si PC del cliente hace el certificado de la máquina instalar y no tiene un Certificado de usuario.

La solución alternativa es copiar el certificado de la máquina al almacén del usuario, crea un perfil del EAP-TLS y después quita el certificado del almacén del usuario para la configuración de la autenticación de la máquina solamente.

Q. ¿Hay manera de asignar el VLA N en el Wireless LAN basado en la dirección

MAC del cliente?

A. No. Esto no es posible. La asignación VLAN del servidor de RADIUS trabaja solamente con el 802.1x, no autenticación de MAC. Usted puede utilizar el RADIUS para avanzar los VSA con la autenticación de MAC, si las direcciones MAC se autentican en el servidor de RADIUS (definido como el userid/contraseña en LEAP/PEAP).

Información Relacionada

- [Seguridad de la red inalámbrica](#)
- [White Paper de la seguridad de red inalámbrica LAN](#)
- [Descripción de la seguridad de red inalámbrica LAN](#)
- [Guía de instrumentación de EAP-TLS para las redes inalámbricas LAN](#)
- [Cisco LEAP](#)
- [Configuración de privacidad equiparable a la de redes cableadas \(WEP\)](#)
- [Soporte de Productos de Red Inalámbrica](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)