Latinoamérica

Microsoft TechNet

Seguridad en LAN inalámbricas con PEAP y contraseñas

Introducción: Elección de una estrategia para la seguridad en LAN inalámbricas

Actualizado: abril 3, aaaa

Ver todos los temas de orientaciones sobre seguridad

En esta página

Descargue la solución completa en

Seguridad en LAN inalámbricas con PEAP y contraseñas

Descargar la solución completa

Guía de defensa en profundidad antivirus

En esta guía

Introducción

La tecnología de red de área local inalámbrica (WLAN) constituye un tema controvertido. Las organizaciones que han implementado WLAN están preocupadas acerca de si son o no seguras; a las que no las han implementado aún les preocupa desaprovechar la oportunidad de aumentar la productividad del usuario y reducir costes de propiedad. Existe todavía una gran confusión en relación con la seguridad de una WLAN en el entorno informático corporativo.

Desde que se detectaron los puntos débiles en la seguridad de WLAN de primera generación, analistas y empresas dedicadas a la seguridad en las redes han procurado resolver estos problemas. Algunos de estos esfuerzos han contribuido de manera significativa a la causa de la seguridad inalámbrica. Otros han participado de los defectos: algunos introducen un conjunto distinto de vulnerabilidades de seguridad; otros precisan hardware propietario costoso; y otros evitan la cuestión de la seguridad de WLAN por completo protegiéndose con otra tecnología de seguridad potencialmente compleja como es la de las redes privadas virtuales (VPN).

Paralelamente, el Instituto de ingenieros eléctricos y electrónicos (IEEE), junto con otros organismos normativos y consorcios, han vuelto a definir y han mejorado con diligencia los estándares de seguridad inalámbrica para permitir que las WLAN hagan frente al entorno de seguridad hostil de principios del siglo veintiuno. Gracias a los esfuerzos de los organismos normativos y los líderes del sector, las palabras "seguridad WLAN" han dejado de ser contradictorias. Las WLAN pueden implementarse y utilizarse actualmente con un gran nivel de confianza en su seguridad.

En este documento se presentan dos soluciones de seguridad de WLAN de Microsoft®, así como las preguntas y respuestas acerca de si las WLAN pueden ser seguras y cuál es la mejor manera de protegerlas.

Descripción general de las soluciones inalámbricas

El principal objetivo de este documento es ayudarle a decidir cuál es el método más adecuado para proteger las WLAN de su organización. Para ello, el documento aborda cuatro áreas principales:

- Motivos para decantarse por las WLAN (y las preocupaciones de seguridad asociadas).
- Utilización de los estándares de WLAN seguras.
- Estrategias alternativas, tales como VPN y seguridad del protocolo Internet (IPSec).
- Selección de las opciones de WLAN correctas.

Microsoft ha elaborado dos soluciones WLAN, basadas en los estándares abiertos de organismos tales como el IEEE, el Grupo de trabajo de ingeniería de Internet (IETF) y la Alianza Wi-Fi. Estas dos soluciones son: *Solución de Seguridad de LAN inalámbricas — Servicios de Certificate Server de Microsoft Windows Server 2003* y *Seguridad en LAN inalámbricas con PEAP y contraseñas*. Como sus propios nombres indican, la primera utiliza certificados de clave pública para autenticar equipos y usuarios en la WLAN mientras que la segunda recurre simplemente a los nombres de usuario y las contraseñas. No obstante, la arquitectura básica de las dos soluciones es muy similar. Ambas se basan en la infraestructura de Microsoft Windows® Server™ 2003 y los clientes Microsoft Windows XP y Microsoft Pocket PC 2003.

Aunque no se deduzca de sus nombres, el público al que están destinadas estas soluciones difiere. *Solución de Seguridad de LAN inalámbricas — Servicios de Certificate Server de Microsoft Windows Server 2003* está orientada sobre todo a organizaciones de gran tamaño con entornos de tecnología de la información (TI) relativamente complejos; mientras que *Seguridad en LAN inalámbricas con PEAP y contraseñas* es una solución bastante más sencilla y se puede implementar con facilidad en organizaciones mucho más pequeñas.

Esto no quiere decir que la autenticación de contraseñas no se pueda utilizar en el caso de organizaciones de gran tamaño (o que la autenticación de certificados no sea adecuada para organizaciones más pequeñas), sólo se trata de reflejar el tipo de organización donde es más probable que se utilice esa tecnología en particular. La siguiente ilustración muestra un árbol de decisión sencillo que le ayuda a seleccionar la solución adecuada para su organización. Las tres opciones principales disponibles son:

- El acceso protegido Wi-Fi (WPA) con clave compartida previamente (PSK) dirigida a empresas muy pequeñas u oficinas domésticas.
- Seguridad de WLAN basada en contraseñas para organizaciones que no utilizan ni necesitan certificados.
- Seguridad de WLAN basada en certificados para organizaciones que necesitan y pueden implementar certificados.

Estas opciones se explicarán más adelante en este documento, ya que es posible combinar las características de las dos últimas opciones para elaborar una solución híbrida.

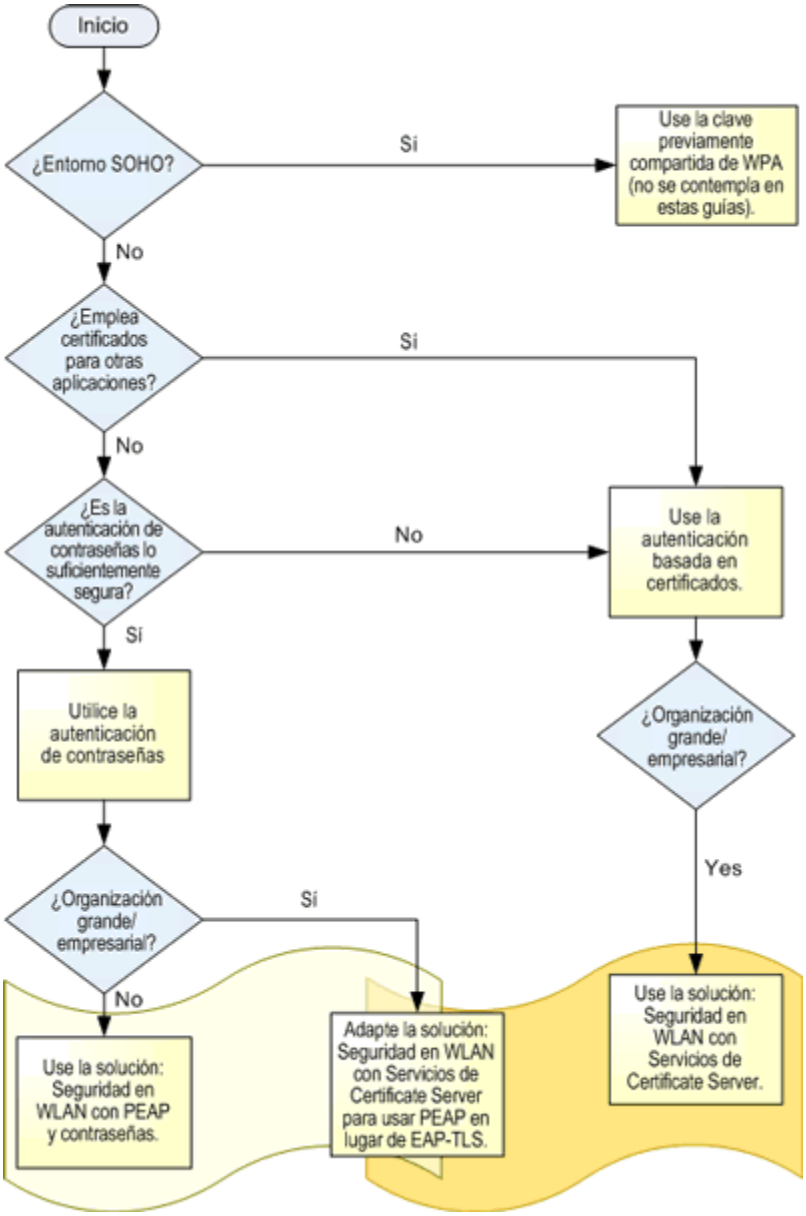

Figura 1. Árbol de decisión para las soluciones de WLAN de Microsoft

Vista de imagen a pantalla completa

Principio de la página

Motivos para decantarse por las redes inalámbricas

No resulta difícil comprender el atractivo que presentan las WLAN para las empresas de hoy en día. La tecnología WLAN se ha respirado en el ambiente de una u otra forma durante cerca de una década, pero curiosamente no ha conseguido hacer mella hasta hace poco. Sólo cuando la tecnología confiable, estandarizada y de bajo coste se ha encontrado con un interés creciente por disponer de métodos más flexibles de trabajo y una conectividad cada vez más omnipresente, se ha hecho realidad la auténtica adopción de la WLAN. No obstante, la adopción rápida de esta tecnología también ha sacado a la luz una serie de puntos débiles en cuanto a seguridad muy graves, con respecto a la primera generación de WLAN. En este apartado se tratarán los pros (funcionalidad) y los contras (seguridad) de las WLAN.

Ventajas de las LAN inalámbricas

Las ventajas de la tecnología WLAN se dividen en dos categorías principales: ventajas empresariales esenciales y ventajas operativas. Las ventajas empresariales esenciales incluyen productividad mejorada de los empleados, procesos empresariales más rápidos y eficaces, y mayor potencial para elaborar funciones corporativas totalmente nuevas. Las ventajas operativas incluyen costes de administración más bajos y un menor gasto de capital.

Ventajas empresariales esenciales

Las ventajas empresariales esenciales de las WLAN derivan de la flexibilidad y la movilidad de la plantilla.

El personal se puede alejar de las mesas de trabajo y moverse fácilmente por las oficinas sin perder la conexión con la red. Es muy práctico observar algunos ejemplos sobre cómo un incremento de la movilidad y de la flexibilidad de la red puede beneficiar a las empresas.

- Los trabajadores móviles que se desplazan de unas oficinas a otras y los teletrabajadores que acuden a la oficina se ahorran mucho tiempo y complicaciones si disponen de un acceso transparente a la red de área local (LAN) corporativa. La conexión es prácticamente instantánea y está disponible desde cualquier lugar con cobertura inalámbrica: no es necesario buscar puertos de red ni cables, ni pedir ayuda al personal de TI para que le ayude a conectarse a la red.
- Los trabajadores expertos pueden permanecer en contacto desde cualquier lugar de la empresa. Utilizando el correo electrónico, los calendarios electrónicos y las tecnologías de chat, el personal puede estar conectado incluso cuando asiste a reuniones o trabaja en otro lugar que no sea su escritorio.
- La información en línea está siempre disponible. Ya no será necesario paralizar las reuniones para que alguien salga disparado a buscar un informe sobre las cifras del último mes o la actualización de una presentación. Todo ello puede mejorar significativamente la calidad y productividad de las reuniones.
- También mejora la flexibilidad de la organización. El personal ya no tendrá que estar siempre en sus escritorios, por lo que los cambios de escritorio o incluso de oficinas enteras serán más rápidos y fáciles, según lo requieran las nuevas estructuras de los equipos o los proyectos.
- La integración de nuevos dispositivos y aplicaciones en el entorno de TI corporativo también mejora considerablemente. Dispositivos como los asistentes digitales personales (PDA) y Tablet PC, que hasta hace poco eran poco más que juguetes de los ejecutivos y no formaban parte importante del departamento de TI, estarán mucho más integrados y serán mucho más útiles cuando las organizaciones dispongan de redes inalámbricas. Los trabajadores y los procesos empresariales que antes no se veían afectados por la tecnología de la información se beneficiarán de los equipos, las aplicaciones y los dispositivos inalámbricos, que se podrán utilizar en áreas que hasta ahora no contaban con redes, como fábricas, hospitales, tiendas y restaurantes.

Cada organización disfrutará de ventajas distintas; determinar cuáles son relevantes para su organización dependerá de diversos factores tales como la naturaleza de la empresa y el tamaño y la distribución geográfica de la plantilla.

Ventajas operativas

Las principales ventajas operativas de la tecnología de WLAN son la reducción de los costes operativos y de capital, y se pueden resumir del siguiente modo:

- El coste de dotar a los edificios de acceso a la red se reduce considerablemente. Aunque la mayoría de las oficinas dispone de cableado de red, muchos otros lugares de trabajo como fábricas, almacenes y tiendas no lo tienen. Las redes podrán suministrarse en ubicaciones donde el cableado de red no se podría llevar a cabo; por ejemplo, al aire libre, en el mar o incluso en el campo de batalla.
- El tamaño de la red se puede modificar con gran facilidad, en respuesta a los distintos niveles de demanda conforme la organización cambia, incluso a diario si es preciso. Es mucho más sencillo implementar una mayor concentración de puntos de acceso inalámbrico en una ubicación concreta que aumentar el número de puertos de red con cable.
- Ya no será necesario que el capital esté ligado a la infraestructura del edificio: la infraestructura de red inalámbrica se puede trasladar a otros edificios con relativa facilidad, mientras que el cableado por el suelo

está permanentemente unido al edificio.

Preocupaciones en cuanto a la seguridad de las LAN inalámbricas

A pesar de todas estas ventajas, una serie de preocupaciones acerca de la seguridad de las WLAN ha frenado su adopción, sobre todo en los sectores más conscientes de la importancia de la seguridad, como son el de las finanzas o los gubernamentales. Aunque parece obvio el riesgo que supone transmitir sin proteger los datos de una red a cualquiera que se encuentre en las cercanías, existe un número sorprendente de WLAN que se han instalado sin ninguna característica de seguridad activada. La mayoría de las empresas han implementado algún tipo de seguridad inalámbrica; no obstante, suele tratarse de características básicas de primera generación, que no ofrecen una protección adecuada según los estándares actuales.

Cuando se desarrollaron los primeros estándares para WLAN, IEEE 802.11, la seguridad no constituía un tema tan preocupante como lo es hoy. El nivel y la sofisticación de las amenazas era muy inferior y la adopción de la tecnología inalámbrica estaba todavía dando sus primeros pasos. Es, en ese momento, cuando surge el esquema de la seguridad de las WLAN de primera generación, conocido como privacidad equivalente por cable (WEP). La WEP subestimó las medidas necesarias para "igualar" la seguridad del aire a la seguridad del cable. En contraposición, los métodos de seguridad de WLAN modernos se diseñaron para trabajar en un entorno hostil como el aire donde no existen unos perímetros físicos o de red claros.

Es importante distinguir entre la WEP estática de primera generación (que utiliza una contraseña compartida para proteger la red) y los esquemas de seguridad que utilizan el cifrado WEP junto con una administración de claves de cifrado y una autenticación segura. El primero es un esquema de seguridad completo que incluye autenticación y protección de datos y que, en este documento, se denomina "WEP estática". Por otra parte, la WEP dinámica, define sólo el cifrado de datos y el método de integridad empleado como parte de soluciones más seguras que se describirán más adelante en este mismo documento.

Los puntos débiles de seguridad descubiertos en la WEP estática implican que las WLAN protegidas por ella son vulnerables a diversos tipos de amenazas. Las herramientas de "auditoría" disponibles de forma gratuita, como Airsnort y WEPCrack, logran que sea posible introducirse con facilidad en redes inalámbricas protegidas por WEP estáticas. Las WLAN que no han sido protegidas se encuentran expuestas obviamente a las mismas amenazas también; la diferencia radica en que se precisan menos conocimientos, tiempo y recursos para llevar a cabo los ataques.

Antes de ver cómo funcionan las soluciones de seguridad de las WLAN modernas, merece la pena revisar las principales amenazas a las que se enfrentan las WLAN. Estas amenazas se resumen en la siguiente tabla.

Tabla 1. Principales amenazas para la seguridad de las WLAN

Amenaza	Descripción de la amenaza
Interceptación (revelación de datos)	La interceptación de transmisiones de la red puede dar lugar a la revelación de datos confidenciales y de credenciales de usuario sin protección, además de a una posible usurpación de la identidad. Permite también que intrusos expertos recopilen información sobre los entornos de TI y la utilicen para atacar otros sistemas o datos que, de otra forma, no serían vulnerables.
Interceptación y modificación de los datos transmitidos	Si un atacante logra obtener acceso a la red, puede introducir un equipo falso que intercepte y modifique los datos comunicados entre dos usuarios autorizados.
Imitación	El acceso directo a la red interna permite que el intruso falsifique datos que parecen legítimos de manera que no sería posible desde fuera de la red, por ejemplo, un mensaje de correo electrónico de un usuario imitado. Los usuarios, incluso los administradores de sistemas, suelen confiar en los elementos originados dentro de la red mucho más que en los que proceden del exterior de la red corporativa.
Denegación del servicio (DoS)	Un agresor determinado puede activar un ataque de DoS de diversas

	maneras. Por ejemplo, la interrupción de las señales de radio se puede activar mediante algo tan simple como un microondas. Existen ataques más complejos cuyo objetivo son los protocolos inalámbricos de bajo nivel, y otros menos complejos cuyo objetivo son las redes mediante un gran incremento del tráfico aleatorio en la WLAN.
Carga libre (o robo de recursos)	Es posible que los intrusos sólo deseen utilizar su red como punto de libre acceso a Internet. Si bien esto no es tan grave como las demás amenazas, hará que, como mínimo, no sólo empeore el nivel de servicio prestado a los usuarios autorizados sino también que puedan introducirse virus y otras amenazas.
Amenazas accidentales	Algunas características de las WLAN facilitan la aparición de amenazas no intencionadas. Por ejemplo, un visitante autorizado podría iniciar el equipo portátil sin la intención de conectarse a la red, pero se conecta a su WLAN automáticamente. Así, el equipo portátil del visitante se convierte en un punto de entrada de virus en la red. Este tipo de amenaza sólo se da en WLAN desprotegidas.
WLAN no autorizadas	Si su empresa no dispone oficialmente de una WLAN, es posible que siga estando bajo la amenaza de las WLAN sin administrar que surjan en su red. El hardware de WLAN adquirido a bajo precio por parte de empleados entusiastas puede abrir vulnerabilidades no intencionadas en su red.

Las preocupaciones sobre seguridad en las WLAN, centradas en la WEP estática, han recibido mucha atención por parte de los medios. A pesar del hecho de que existen buenas soluciones de seguridad para combatir estas amenazas, organizaciones de distintos tamaños recelan de las WLAN. Muchas de ellas han detenido su implementación o han prohibido el uso de la tecnología de WLAN por completo. A continuación, se enumeran algunos factores que contribuyen a difundir esta confusión y el error extendido de que las WLAN y la inseguridad de las redes van de la mano:

- Existe una incertidumbre generalizada acerca de qué tecnología WLAN es segura y cuál no lo es. Las empresas desconfían de todas las medidas de seguridad de WLAN después de la serie de defectos encontrados en las WEP estáticas. La desconcertante lista de estándares oficiales y soluciones de propiedad que dicen solucionar los problemas ha ayudado muy poco a aclarar la confusión.
- Inalámbrica equivale a invisible. Para los administradores de la seguridad de la red, no se trata sólo de una cuestión perturbadora desde un punto de vista psicológico, sino que plantea un problema de administración de la seguridad real. Mientras que es posible *ver* cómo un intruso conecta un cable a una red convencional, la intrusión en las WLAN es mucho menos tangible. Las tradicionales paredes y puertas de defensa física de la seguridad, que ayudan a proteger la red con cable, no constituyen protección frente a un atacante "inalámbrico".
- En la actualidad se tiene una mayor conciencia de la necesidad de proteger la información. Las empresas demandan niveles de seguridad mucho mayores para sus sistemas y desconfían de cualquier tecnología que conlleve vulnerabilidades de la seguridad.
- Como corolario de esta creciente toma de conciencia de la seguridad, existe una serie de requisitos legales y normativos que rigen la seguridad de los datos en un número de países y sectores de la industria que sigue en aumento. Uno de los mejores ejemplos que se conocen de este fenómeno es la Ley de portabilidad y responsabilidad de seguros de salud (HIPAA) de 1996, que regula el manejo de historiales sanitarios personales en Estados Unidos.

Principio de la página

Protección real de la WLAN

Desde el descubrimiento de las vulnerabilidades de seguridad de las WLAN que se han descrito hasta el

momento, los principales proveedores de redes, los organismos reguladores y los analistas han centrado gran parte de sus esfuerzos en encontrar soluciones para hacer frente a estos problemas. De esta forma, se han generado una serie de respuestas a las preocupaciones sobre la seguridad de las WLAN. Las principales opciones son:

- No implementar tecnología de WLAN.
- Mantenerse fiel a la seguridad WEP estática 802.11.
- Utilizar VPN para proteger los datos de la WLAN.
- Utilizar IPSec para proteger el tráfico de la WLAN.
- Utilizar la autenticación 802.1X y el cifrado de datos para proteger la WLAN.

Estas estrategias se detallan en orden de menor a mayor grado de satisfacción, basándose en una combinación de seguridad, funcionalidad y aprovechamiento; aunque, hasta cierto punto, se trata de un juicio subjetivo. La opción recomendada por Microsoft es la última: utilizar la autenticación 802.1X y el cifrado de WLAN. Este enfoque se tratará en la siguiente sección y entonces, se evaluará con respecto a la lista de las principales amenazas de WLAN que se han identificado con anterioridad (tabla 1). Las principales ventajas e inconvenientes de los demás enfoques también se abordarán más adelante en este documento, después de esta sección.

Protección de la WLAN mediante la autenticación 802.1X y el cifrado de datos

Este enfoque posee muchos puntos positivos para poder recomendarlo (aunque su nombre y el despliegue de términos oscuros no se encuentren entre ellos). Antes de tratar las ventajas de las soluciones basadas en este enfoque, es importante aclarar algunos términos y explicar cómo funciona la solución.

Comprensión de la seguridad de WLAN

La protección de una WLAN implica tres elementos fundamentales:

- Autenticación del usuario (o dispositivo) que se conecta a la red, de manera que se tenga un elevado grado de confianza en quién o qué está intentando conectarse.
- Autorización del usuario o dispositivo que va a utilizar la WLAN para poder controlar quién obtiene acceso a ella.
- Protección de los datos transmitidos en la red de manera que estén a salvo de interceptaciones y modificaciones no autorizadas.

Es posible que precise también una función de auditoría junto con estas opciones, aunque la auditoría es principalmente una manera de comprobar y reforzar estos otros tres elementos.

Autenticación y autorización de la red

La seguridad WEP estática se basa en un mero secreto compartido (clave o contraseña) para la autenticación en la WLAN. Todo el que posea esta clave secreta podrá contar con acceso a la WLAN. La WEP estándar original no proporciona ningún método para automatizar la actualización o distribución de estas claves; por lo tanto, resulta extremadamente difícil cambiarlas con regularidad. Los defectos de cifrado en la WEP implican que un atacante puede descubrir las claves WEP estáticas mediante herramientas sencillas.

Con el fin de proporcionar un método más sólido de autenticación y autorización, Microsoft y una serie de proveedores han propuesto un marco de seguridad de WLAN mediante el protocolo 802.1X. 802.1X es un estándar del IEEE para realizar la autenticación del acceso a una red y, si se desea, administrar las claves utilizadas para proteger el tráfico. Su uso no se limita a las redes inalámbricas y, de hecho, también se implementan en muchos conmutadores de LAN de categoría superior.

El protocolo 802.1X implica al usuario de la red, un dispositivo de acceso a la red (o puerta de enlace) como un punto de acceso inalámbrico y un servicio de autenticación y autorización en forma de servidor RADIUS (Servicio de usuario de acceso telefónico de autenticación remota). El servidor RADIUS desempeña la labor de autenticar las credenciales de los usuarios y de autorizar el acceso de éstos a la WLAN.

1X se basa en un protocolo IETF denominado "protocolo de autenticación extensible" (EAP) para llevar a cabo la

comunicación de autenticación entre el cliente y el servidor RADIUS (transmitida por el punto de acceso). EAP es un protocolo general para la autenticación que admite diversos métodos de autenticación, basados en contraseñas, certificados digitales o bien otros tipos de credenciales.

Puesto que EAP es un método de autenticación conectable, no existe un único tipo de autenticación estándar EAP que se pueda utilizar. Distintos métodos de EAP, con distintos tipos de credenciales y protocolos de autenticación, pueden resultar apropiados en distintas circunstancias. La utilización de métodos de EAP en la autenticación de WLAN se tratará en una sección más adelante.

Protección de datos de WLAN
La autenticación y el acceso a la red 1X constituyen sólo una parte de la solución. El otro componente significativo es la protección del tráfico de redes inalámbricas.

Los defectos del cifrado de datos WEP descritos con anterioridad se podrían haber mejorado si la WEP estática hubiera incluido un método para actualizar automáticamente las claves de cifrado con regularidad. Las herramientas para descifrar la WEP estática precisan recopilar entre uno y diez millones de paquetes cifrados con la misma clave. Dado que las claves WEP estáticas permanecen invariables a menudo durante semanas o meses, suele ser fácil para un atacante recopilar esa cantidad de datos. Puesto que todos los equipos de una WLAN comparten la misma clave estática, las transmisiones de datos desde todos los equipos de la WLAN pueden cosecharse para ayudarle a descubrir la clave.

Al utilizar una solución basada en 802.1X, se permite que las claves de cifrado se modifiquen con frecuencia. Como parte del proceso de autenticación segura 802.1X, el método de EAP genera una clave de cifrado que es exclusiva de cada cliente. Para evitar los ataques de descifrado WEP (descritos previamente), el servidor RADIUS fuerza con regularidad la generación de claves de cifrado nuevas. Esto permite que se empleen algoritmos de cifrado WEP (encontrados en la mayoría del hardware de WLAN actual) de una manera mucho más segura.

WPA y 802.11i
Aunque la WEP con el cambio dinámico de claves 802.1X resulta segura para la mayoría de los fines prácticos, existe un conjunto de problemas persistentes entre los que se incluyen:

- WEP utiliza una clave estática aparte para las transmisiones globales como los paquetes de difusión. A diferencia de las claves por usuario, la clave global no se renueva con regularidad. Pese a que es poco probable que los datos confidenciales se transmitan mediante difusión, al emplear una clave estática para la transmisión global se ofrece a los atacantes la oportunidad de descubrir información acerca de la red, como por ejemplo, direcciones IP y nombres de usuario y de equipo.
- Los marcos de redes protegidas por WEP poseen una protección de escasa integridad. Mediante las técnicas criptográficas, un atacante puede modificar la información del marco de WLAN y actualizar el valor de comprobación de la integridad del marco sin que el receptor lo detecte.
- A medida que se mejora la velocidad de transmisión de la WLAN y se mejora la capacidad informática y las técnicas criptoanalíticas, las claves WEP deberán renovarse con mayor frecuencia. De esta forma, se depositará una carga inaceptable en los servidores RADIUS.

Para afrontar estos problemas, el IEEE está trabajando en un nuevo estándar de seguridad para las WLAN denominado 802.11i; también conocido como "red de seguridad sólida" (RSN). La Alianza Wi-Fi, un consorcio formado por proveedores de fidelidad inalámbrica (Wi-Fi), ha publicado en un estándar del sector denominado "Acceso protegido Wi-Fi" (WPA) lo que es, básicamente, una versión previa del 802.11i. WPA incluye un amplio subconjunto de funciones de 802.11i. Al publicar el WPA, la Alianza Wi-Fi ha podido exigir la adherencia a la WPA de todos los equipos que lleven el logotipo Wi-Fi y ha permitido que los proveedores de hardware de redes de Wi-Fi ofrezcan una opción de alta seguridad estandarizada con anterioridad a la publicación del 802.11i. WPA reúne un conjunto de características de seguridad ampliamente aceptadas como las técnicas más seguras disponibles en la actualidad para proteger las WLAN.

WPA incluye dos modos: uno, que emplea 802.1X y la autenticación RADIUS (conocida simplemente como WPA) y otro esquema más sencillo para entornos SOHO que emplea una clave compartida previamente (conocida como WPA PSK). WPA asocia el cifrado seguro con la autenticación fuerte y el mecanismo de autorización de 802.1X. La protección de datos de WPA elimina las vulnerabilidades conocidas de WEP con los siguientes

métodos:

- Utilización de una clave de cifrado única para cada paquete.
- Utilización de un vector de inicialización mucho más largo, duplicando de forma eficaz el espacio de clave al agregar 128 bits adicionales de material para claves.
- Adición de un valor de comprobación de integridad de mensaje firmado que no sea vulnerable a la alteración de datos o la suplantación.
- Incorporación de un contador de marcos cifrado para impedir los ataques de reproducción.

No obstante, dado que WPA utiliza algoritmos criptográficos similares a los empleados por WEP, se puede implementar en el hardware existente con una sencilla actualización de firmware.

El modo PSK de WPA también permite que las pequeñas organizaciones y los trabajadores domésticos utilicen una WLAN de clave compartida carente de las vulnerabilidades de la WEP estática (siempre que la clave compartida previamente que se haya elegido sea lo bastante segura como para evitar meros ataques de adivinación de contraseña). Al igual que la WEP dinámica y el WPA basado en RADIUS, las claves de cifrado individuales se generan para cada cliente inalámbrico. La clave que se ha compartido previamente se emplea como una credencial de autenticación; si dispone de esa clave, entonces tendrá autorización para emplear la WLAN y recibir una clave de cifrado exclusiva con el fin de proteger los datos.

802.11i (RSN) le proporcionará niveles de seguridad todavía más elevados para las WLAN, incluida una mejor protección contra los ataques de DoS. Su lanzamiento está previsto para mediados de 2004.

Métodos de autenticación de EAP

El protocolo de autenticación extensible (EAP) tal y como la palabra "extensible" de su nombre implica, es compatible con muchos métodos de autenticación. Estos métodos pueden emplear distintos protocolos de autenticación tales como Kerberos, seguridad de la capa de transporte (TLS) y el protocolo de autenticación por desafío mutuo de Microsoft (MS-CHAP) con una amplia gama de tipos de credenciales como contraseñas, certificados, token de contraseñas de un solo uso y datos biométricos. Aunque, en teoría, cualquier método de EAP puede utilizarse con 802.1X, no todos son adecuados para su uso con WLAN. En especial, el método empleado debe ser adecuado para su uso en un entorno desprotegido y poder generar claves de cifrado.

Los métodos de EAP principales para su uso en WLAN son EAP-TLS, EAP protegido (PEAP), túnel de TLS (TTLS) y EAP ligero (LEAP). De estos, tanto PEAP como EAP-TLS son compatibles con Microsoft.

EAP-TLS

EAP-TLS es un estándar de IETF (RFC 2716) y es, probablemente, el de uso más generalizado, tanto en clientes inalámbricos como en servidores RADIUS. Emplea certificados de clave pública para autenticar tanto los clientes inalámbricos como los servidores RADIUS estableciendo una sesión de TLS cifrada entre los dos.

PEAP

PEAP es un método de autenticación en dos fases. En la primera fase se establece una sesión de TLS para el servidor y se permite que el cliente autentique al servidor mediante el certificado digital del servidor. La segunda fase precisa un segundo método de EAP con túnel dentro de la sesión de PEAP para autenticar al cliente en el servidor RADIUS. De esta forma se permite que PEAP utilice una variedad de métodos de autenticación de cliente, que incluyen contraseñas con el protocolo MS-CHAP versión 2 (MS-CHAP 2) y los certificados que emplean EAP-TLS con túnel dentro de PEAP. La seguridad de los tipos de EAP (tales como MS-CHAP 2) no es suficiente para poder ser utilizados sin la protección de PEAP porque serían vulnerables a los ataques de diccionario sin conexión. La compatibilidad con PEAP está muy extendida dentro de la industria y Microsoft Windows XP Service Pack 1 y Pocket PC 2003 cuentan con compatibilidad integrada para PEAP.

TTLS

TTLS es un protocolo de dos fases similar a PEAP que emplea una sesión de TLS con el fin de proteger una autenticación de cliente con túnel. Además de los métodos de EAP con túnel, TTLS también puede utilizar versiones ajenas a EAP de los protocolos de autenticación como CHAP, MS-CHAP y otros. Microsoft y Cisco no

admiten TTLS, aunque otros proveedores suministran clientes de TTLS para una serie de plataformas.

LEAP

LEAP es un método de EAP de propiedad desarrollado por Cisco, que emplea contraseñas para autenticar clientes. Pese a estar muy extendido, LEAP sólo funciona con hardware y software de Cisco y algunos proveedores más. LEAP también presenta diversas vulnerabilidades de seguridad tales como propensión a ataques de diccionario sin conexión (que permiten que los atacantes descubran las contraseñas de los usuarios) y los ataques de intermediario. En un entorno de dominio, LEAP sólo puede autenticar al *usuario* en la WLAN, pero no al *equipo*. Sin la autenticación de equipos, las directivas de grupo de equipos no se ejecutarán correctamente, la configuración de instalación del software, los perfiles de itinerancia y las secuencias de comandos de inicio de sesión pueden fallar y no será posible que los usuarios cambien las contraseñas caducadas.

Existen soluciones de seguridad para las WLAN que emplean 802.1X junto con otros métodos de EAP. Algunos de estos métodos de EAP, tales como EAP-MD5, presentan puntos débiles significativos en cuanto a seguridad cuando se emplean en un entorno de WLAN, así que no deberían utilizarse nunca. Existen otros que admiten la utilización de tokens de contraseña de un solo uso y otros protocolos de autenticación como Kerberos. Estos siguen teniendo un impacto considerable en el mercado de WLAN.

Ventajas de 802.1X con la protección de datos de WLAN

Las ventajas clave de una solución 802.1X se resumen en la siguiente lista:

- **Nivel de seguridad alto:** se trata de un esquema de autenticación de seguridad elevado porque puede emplear certificados de cliente o nombres de usuario y contraseñas.
- **Cifrado más seguro:** permite un cifrado muy seguro de los datos de la red.
- **Transparencia:** proporciona una autenticación y una conexión a la WLAN transparentes.
- **Autenticación de usuarios y de equipos:** permite la autenticación por separado de usuario y de equipo. La autenticación por separado de un equipo permite administrarlo incluso cuando ningún usuario ha iniciado la sesión.
- **Bajo coste:** bajo coste del hardware de red.
- **Alto rendimiento:** dado que el cifrado se lleva a cabo en el hardware de WLAN y no en la CPU del equipo cliente, el cifrado de WLAN no influirá en el nivel de rendimiento del equipo cliente.

La solución 802.1X también cuenta con algunas advertencias.

- Aunque 802.1X disfruta de una aceptación casi universal, el uso de distintos métodos de EAP implica que la interoperabilidad no siempre está garantizada.
- WPA está todavía en las primeras fases de adopción así que es posible que no se encuentre disponible en hardware más antiguo.
- La RSN (802.11i) de próxima generación está todavía pendiente de ratificación y precisará la implantación de actualizaciones de hardware y software (por lo general, el hardware de red necesitará una actualización de firmware).

No obstante, éstos son problemas relativamente menores y se ven compensados con facilidad por las ventajas; sobre todo, cuando se comparan con los defectos más graves de los enfoques alternativos que se comentan más adelante.

Resistencia de la solución 802.1X a las amenazas de la seguridad

Las principales amenazas de la seguridad para las WLAN se detallaron con anterioridad en este documento (en la tabla 1). Estas amenazas se vuelven a valorar en la siguiente tabla en comparación con una solución basada en 802.1X y la protección de datos de WLAN.

Tabla 2. Amenazas contra la seguridad valoradas en función de la solución propuesta

Amenaza	Mitigación
Interceptación (revelación de datos)	La asignación y modificación dinámicas de las claves de cifrado con regularidad y el hecho de que las claves sean exclusivas para cada sesión de usuario implica que siempre y cuando la actualización de la clave se realice con suficiente frecuencia, no se podrán descubrir las claves ni disponer de acceso a los datos de ninguna forma conocida. WPA ofrece mayor seguridad al cambiar las claves de cifrado por paquete. La clave global (que protege el tráfico de difusión) se cambia por paquete.
Interceptación y modificación de datos transmitidos	La aplicación de la integridad de datos y el cifrado de datos de alta seguridad entre el cliente inalámbrico y el punto de acceso inalámbrico garantiza que un usuario malicioso no pueda interceptar y modificar los datos en tránsito. La autenticación mutua entre el cliente, el servidor RADIUS y el punto de acceso inalámbrico hace que sea muy difícil que un atacante pueda suplantar a alguno de ellos. WPA mejora la integridad de los datos con el protocolo Michael.
Imitación	La autenticación segura en la red impide que usuarios no autorizados se conecten a la red e introduzcan datos imitados desde el interior.
Denegación de servicio (DoS)	Los ataques de exceso de datos y otros ataques de DoS en la red se pueden evitar si se controla el acceso a la WLAN mediante 802.1X. No existe defensa contra los ataques de DoS de 802.11 de bajo nivel ya sea WEP dinámica o WPA. Este problema se ha afrontado con el estándar 802.11i. No obstante, incluso este estándar nuevo no será inmune a la interrupción de la capa física (nivel de radio) de las redes. Estas vulnerabilidades son una característica de las WLAN 802.11 actuales y común a todas las demás opciones que se tratarán más adelante en este documento.
Carga libre (robo de recursos)	El requisito de autenticación segura impide la utilización no autorizada de la red.
Amenazas accidentales	El requisito de autenticación segura impide la conexión accidental a la WLAN.
WLAN no autorizadas	Si bien la solución no se ocupa directamente de los puntos de acceso inalámbrico no autorizados, la implementación de una solución inalámbrica segura como ésta elimina, casi por completo, los motivos para establecer una WLAN no oficial. No obstante, debería planear la creación y publicación de una directiva que prohibiese la utilización de WLAN sin aprobar. Puede aplicar la directiva mediante herramientas de software que exploren la red en busca de direcciones de hardware de puntos de acceso inalámbrico y los equipos portátiles de detección de WLAN.

Otros enfoques para la seguridad de WLAN

En la sección anterior se trató la autenticación 802.1X con la protección de datos de WLAN con más

detenimiento. En esta sección se describirán las cuatro alternativas a la seguridad de WLAN citadas con anterioridad (al comienzo de la sección "Protección real de la WLAN").

Los otros cuatro enfoques enumerados eran:

- No implementar tecnología de WLAN.
- Mantenerse fiel a la seguridad WEP estática 802.11.
- Utilizar VPN para proteger los datos de la WLAN.
- Utilizar IPSec para proteger el tráfico de la WLAN.

Los factores diferenciadores más importantes entre estos enfoques y una solución basada en 802.1X se resumen en la siguiente tabla (aunque la opción "Sin WLAN" no se incluye puesto que no se puede comparar directamente con las demás). Estas opciones se abordan con más detalle en las secciones siguientes.

Tabla 3. Comparación de los enfoques de seguridad de WLAN

Característica	WLAN 802.1X	WEP estática	VPN	IPSec
Autenticación segura (1)	Sí	No	Sí, pero no las VPN que utilicen autenticación de clave compartida.	Sí, si se emplea autenticación de certificados o Kerberos.
Cifrado de datos de alta seguridad	Sí	No	Sí	Sí
Conexión transparente y reconexión a la WLAN	Sí	Sí	No	Sí
Autenticación de usuario	Sí	No	Sí	Sí
Autenticación de equipo (2)	Sí	Sí	No	Sí
Difusión y tráfico de multidifusión protegidos	Sí	Sí	Sí	No
Se requieren dispositivos de red adicionales	Servidores RADIUS	No	Servidores VPN, servidores RADIUS	No
Acceso seguro a la propia WLAN	Sí	Sí	No	No

(1) Muchas implementaciones de VPN que utilizan el modo de túnel IPSec emplean un esquema de autenticación de clave compartida débil, conocido como XAuth.

(2) La autenticación de equipo se refiere a que el equipo permanecerá conectado a la WLAN y a la red corporativa incluso si no hay ningún usuario que haya iniciado la sesión en el equipo. Esta capacidad es necesaria para que las siguientes funciones de dominio de Windows actúen correctamente:

- Perfiles de itinerancia de usuario.
- Configuración de directiva de grupo de equipos (en especial secuencias de comandos de inicio y software

implementado).

- Secuencias de comandos de inicio de sesión de usuario y software implementado mediante la directiva de grupo.

Alternativa 1: No implementar la tecnología WLAN

Quizás la manera más evidente de lidiar con las amenazas de la seguridad en las WLAN sea evitarlas por completo al no implementar ninguna WLAN. Además de tener que renunciar a los beneficios de las WLAN esbozados con anterioridad en este documento, esta estrategia no está libre de dificultades. Las organizaciones que siguen este enfoque deben tratar con lo que el grupo META denomina el "precio de la demora", que es más que un mero coste de la oportunidad. El estudio del grupo META basó sus hallazgos en el análisis del método no administrado con el que se desarrolló el uso de las redes locales por cable en muchas organizaciones durante una década. En la mayoría de los casos, los departamentos de TI centrales se vieron obligados a dar el paso y tomar el control de la implementación de la LAN a posteriori. Como suele ocurrir, el coste de volver a implementar las numerosas redes locales de departamentos independientes y, a menudo, incompatibles, fue enorme. Si desea obtener más información, consulte el artículo "How Do I Limit My Exposure Against the Wireless LAN Security Threat? The New Realities of Protecting Corporate Information" publicado por el grupo META el 18 de diciembre de 2002.

Ésta es la misma amenaza que ha emergido con las WLAN, sobre todo en empresas grandes donde, con frecuencia, no se puede ver físicamente lo que sucede en cada ubicación. La implementación de bases no administradas de WLAN, posible debido al coste extremadamente bajo de los componentes, es con toda probabilidad la peor situación. De esta forma, las organizaciones quedan expuestas a todas las amenazas de la seguridad descritas con anterioridad, y además, no disponen del grupo de TI central que conoce todo lo necesario acerca de ellas o que es capaz de dar los pasos precisos para combatir las amenazas.

Por tanto, si su estrategia es la de no adoptar la tecnología de WLAN, tendrá que llevarla a cabo de forma activa y no pasiva. Debe respaldar esta decisión con una directiva clara publicada y asegurarse de que todos los empleados conocen tanto esta directiva como las consecuencias de no cumplirla. Podría interesarle disponer de equipamiento de exploración y monitores de paquetes de red para detectar el uso no autorizado de equipos inalámbricos en su red.

Alternativa 2: Utilizar seguridad básica mediante 802.11 (WEP estática)

La seguridad 802.11 básica (WEP estática) emplea una clave compartida para controlar el acceso a la red y usa la misma clave para cifrar el tráfico inalámbrico. Este modelo de autorización simple se complementa a menudo con el uso del filtrado de puertos basado en direcciones de hardware de tarjeta de WLAN, aunque no forma parte de la seguridad de 802.11 como tal. El principal atractivo de este enfoque es su sencillez. Si bien ofrece un nivel de seguridad algo mejor que las WLAN sin proteger, cuenta con grandes inconvenientes de administración y seguridad, sobre todo en organizaciones de gran tamaño.

Entre los inconvenientes de utilizar WEP se incluyen los siguientes:

- Las claves WEP estáticas se pueden averiguar en cuestión de horas en una red con bastante tráfico si se utiliza un equipo con un adaptador de WLAN y herramientas de pirateo, como Airsnort o WEPCrack.
- El punto débil más grave de WEP es que no existe ningún mecanismo para asignar o actualizar dinámicamente la clave de cifrado de la red. Sin 802.1X ni EAP para aplicar las actualizaciones de clave regulares, el algoritmo de cifrado empleado por la WEP será vulnerable a los ataques de recuperación de claves tal y como se ha descrito con anterioridad.
- Las claves estáticas se pueden cambiar, pero el proceso para hacerlo en los puntos de acceso y los clientes inalámbricos es, por lo general, manual y laborioso. Para empeorar la situación, las actualizaciones de clave se deben efectuar en los clientes y los puntos de acceso simultáneamente con el fin de evitar que se interrumpa la conexión de los clientes. En la práctica, esto resulta tan difícil que las claves se suelen dejar sin modificar.
- La clave estática precisa que se comparta entre todos los usuarios de la WLAN y todos los puntos de acceso inalámbrico. Un secreto compartido entre un gran número de personas y dispositivos es poco probable que permanezca a salvo durante mucho tiempo.

WEP proporciona a las WLAN un mecanismo de control del acceso muy limitado, basado en el conocimiento de la clave WEP. Si se descubre el nombre de la red (algo muy sencillo) y la clave WEP, es posible conectarse a la red.

Una manera de intentar mejorar esta situación es configurar los puntos de acceso inalámbrico de forma que sólo admitan un conjunto predefinido de direcciones de adaptadores de red cliente. Esto suele conocerse como filtrado de direcciones de control de acceso de medios (MAC). La capa MAC hace referencia al firmware de bajo nivel del adaptador de red.

El filtrado de direcciones de adaptadores de red para controlar el acceso conlleva sus propios problemas:

- La facilidad de administración es extremadamente pobre. Mantener una lista de direcciones de hardware de todo menos de un número pequeño de clientes es difícil. Además, distribuir esta lista a todos los puntos de acceso y sincronizarla a través de ellos constituye un reto importante.
- La escalabilidad es escasa. Los puntos de acceso tienen un límite del tamaño de la tabla de filtros finito, lo que restringe el número de clientes que se pueden admitir.
- No hay forma de asociar una dirección de MAC a un nombre de usuario, por lo que sólo se puede autenticar por identidad de equipo y no por identidad de usuario.
- Un usuario malintencionado podría imitar una dirección de MAC "autorizada". Si se puede descubrir una dirección de MAC legítima, resulta muy fácil para un intruso utilizarla en lugar de la predefinida grabada en el adaptador.

Las soluciones de claves compartidas previamente sólo resultan prácticas cuando se trata de un número reducido de usuarios y puntos de acceso debido a la dificultad de administrar actualizaciones de claves a través de diversas ubicaciones. Los defectos del cifrado de WEP implican que su utilidad es extremadamente cuestionable, incluso en entornos muy reducidos.

No obstante, el modo de claves compartidas previamente de WPA proporciona un buen nivel de seguridad con una carga de infraestructura muy baja para las pequeñas organizaciones. Una amplia gama de hardware es compatible con WPA PSK y los clientes WLAN se pueden configurar manualmente. Debería considerarse la configuración de la elección de entornos SOHO.

Alternativa 3: Redes privadas virtuales

Las VPN son probablemente la manera más popular de cifrado de red; mucha gente confía en las tecnologías de VPN probadas y de confianza para proteger la confidencialidad de los datos enviados a través de Internet. Cuando se detectaron las vulnerabilidades de la WEP estática, VPN se propuso rápidamente como *la* manera de proteger los datos que viajan a través de una WLAN. Algunos analistas, como el Grupo Gartner, promocionaron este enfoque y, lógicamente, los distribuidores de soluciones para VPN lo fomentaron con entusiasmo.

VPN es una solución excelente para atravesar una red hostil como Internet (aunque la calidad de las implementaciones de VPN varíe). Sin embargo, no es necesariamente la mejor solución para asegurar las WLAN internas. Para este tipo de aplicaciones, una VPN ofrece poca o ninguna seguridad adicional en comparación con las soluciones 802.1X; al mismo tiempo que incrementan de manera significativa la complejidad y los costes, reducen el aprovechamiento y hacen que partes importantes de las funciones no estén operativas.

Nota: se distingue de la utilización de VPN para asegurar el tráfico a través de zonas interactivas de la LAN pública inalámbrica. La protección de los datos de red de usuarios que se conectan a través de redes remotas hostiles constituye un uso legítimo de las VPN. En estos escenarios, los usuarios esperan que las conexiones seguras sean más molestas y menos funcionales que las conexiones LAN; algo inesperado dentro de las propias instalaciones de la empresa.

Entre las ventajas de utilizar VPN para proteger las WLAN se incluyen:

- La mayoría de las organizaciones ya han implementado una solución de VPN, así que tanto los usuarios como el personal de TI estarán familiarizados con la solución.
- La protección de los datos de la VPN suele emplear el cifrado de software que permite que los algoritmos se

modifiquen y se actualicen con mayor facilidad que el cifrado basado en el hardware.

- Es posible utilizar hardware relativamente menos costoso porque la protección de VPN es independiente del hardware de WLAN (aunque el aumento de precio que conlleva el hardware de red apto para 802.1X no ha desaparecido en absoluto).

Entre los inconvenientes de utilizar VPN en lugar de la seguridad de WLAN nativa se incluyen:

- Las VPN carecen de transparencia para el usuario. Por regla general, los clientes VPN precisan que el usuario inicie manualmente una conexión con el servidor de VPN; por lo tanto, la conexión nunca será tan transparente como una conexión LAN con cable. Los clientes de VPN ajenos a Microsoft también pueden solicitar credenciales de inicio de sesión al conectarse además del inicio de sesión a la red estándar o al dominio. Si la VPN se desconecta, debido a una señal de WLAN escasa o como consecuencia de que el cliente se esté moviendo entre los puntos de acceso, el usuario deberá volver a conectarse.
- Dado que la conexión de VPN sólo la puede iniciar el usuario, un equipo inactivo o desconectado no se conectará a la VPN (y por lo tanto, tampoco a la LAN corporativa). En consecuencia, un equipo no se puede administrar o supervisar remotamente a menos que un usuario inicie la sesión. Determinadas configuraciones de objeto de directiva de grupo de equipos (GPO), tales como las secuencias de comandos de inicio y el software asignado al equipo, no se aplicarán nunca.
- Es posible que los perfiles de itinerancia, las secuencias de comandos de inicio de sesión y el software implementado para el usuario mediante el GPO no funcionen como se esperaba. A menos que el usuario elija iniciar la sesión mediante la conexión de VPN desde el mensaje de inicio de sesión de Windows, el equipo no se conectará a la LAN corporativa hasta después de que el usuario haya iniciado la sesión y haya iniciado la conexión de VPN. Los intentos anteriores de obtener acceso a la red segura darán error. En el caso de un cliente VPN que no sea de Microsoft, puede ser imposible realizar un inicio de sesión de dominio completo a través de la conexión de VPN.
- Si se reanuda desde un estado de espera o hibernación, la conexión de VPN no se volverá a establecer de forma automática, sino que el usuario deberá hacerlo manualmente.
- Aunque los datos del interior del túnel VPN están protegidos, la VPN no ofrece protección para la propia WLAN. Un intruso podría seguir conectado a la WLAN e intentar sondear o atacar dispositivos conectados a la WLAN.
- Los servidores de la VPN se pueden convertir en un cuello de botella. Todo el acceso de clientes WLAN a la LAN corporativa se realiza a través del servidor. Los dispositivos VPN suelen prestar servicio a una gran cantidad de clientes remotos con velocidades relativamente bajas; de ahí, que la mayoría de las puertas de enlace VPN no puedan hacer frente a las decenas o cientos de clientes que se ejecutan con toda la velocidad de una LAN.
- Los gastos de hardware adicional y de administración continua de los dispositivos de VPN son probablemente muy superiores a los de una solución de WLAN nativa. Cada sitio necesitará, habitualmente, su propio servidor VPN junto con los puntos de acceso de WLAN.
- Las sesiones de VPN son más susceptibles de desconectarse cuando los clientes se mueven entre puntos de acceso. Aunque las aplicaciones admitirán a menudo desconexiones momentáneas al cambiar de un punto de acceso inalámbrico a otro, las sesiones de VPN se interrumpirán con frecuencia y necesitarán que el usuario las vuelva a conectar manualmente.
- El coste del servidor VPN y de las licencias de software del cliente, así como el coste de implementar el software, pueden constituir un problema en el caso de soluciones de VPN ajenas a Microsoft. Es posible también que le preocupe la compatibilidad del software del cliente VPN ya que, a menudo, los clientes que no son de Microsoft sustituyen funciones principales de Windows.
- Muchos analistas y proveedores suponen, sin manifestarlo abiertamente, que la seguridad de las VPN siempre es mejor que la de las WLAN. Aunque esto puede ser cierto en el caso de la WEP estática, no tiene por qué ser necesariamente el caso de las soluciones basadas en EAP 802.1X que se describen en este documento. En especial los métodos de autenticación de VPN son, a menudo, *muy poco* seguros y, en el mejor de los casos,

no suelen ser mucho más seguros. Por ejemplo, las soluciones de WLAN compatibles con Microsoft utilizan exactamente los mismos métodos de autenticación de EAP que sus soluciones de VPN (EAP-TLS y MS-CHAP versión 2). Muchas de las implementaciones de VPN, sobre todo las que se basan en el modo de túnel IPSec, emplean la autenticación de claves compartidas previamente (una contraseña de grupo). Ésta se ha desprestigiado ampliamente y se ha mostrado que posee graves vulnerabilidades de seguridad (irónicamente, comparte algunas de estas vulnerabilidades con la WEP estática).

- Una VPN no protege la WLAN propiamente dicha. Aunque los datos del interior de los túneles VPN son seguros, cualquiera puede seguir conectándose a la WLAN e intentando atacar a clientes inalámbricos legítimos u otros dispositivos de la WLAN.

VPN se adapta de manera ideal para asegurar el paso del tráfico a través de redes hostiles, tanto si el usuario se ha conectado a través de una conexión de banda ancha doméstica o desde una zona interactiva inalámbrica. No obstante, las VPN nunca se diseñaron para proteger el tráfico de la red en las redes internas. Para la mayoría de las organizaciones, las VPN con este papel serían demasiado voluminosas y estarían limitadas en cuanto a las funciones para el usuario; además de ser demasiado costosas y complejas para el departamento de TI encargado de mantenerlas.

En los casos excepcionales donde se precisa seguridad más elevada para una conexión concreta o un tipo de tráfico, dicha seguridad se puede suministrar mediante un túnel VPN o un modo de transporte IPSec *además de* la protección de WLAN nativa. Se trata de la utilización más sensata de los recursos de la red.

Alternativa 4: Seguridad IP

IPSec permite que dos partes de una red se autentiquen la una a la otra de forma segura y autentiquen o cifren paquetes de red individuales. IPSec se puede utilizar tanto para abrir un túnel seguro de una red a otra, como para simplemente proteger los paquetes IP que se transmiten entre dos equipos.

Los túneles IPSec se suelen utilizar en el acceso de cliente o las conexiones de VPN de sitio a sitio. El modo de túnel IPSec es una forma de VPN y funciona con la encapsulación de un paquete de IP completo dentro de un paquete protegido mediante IPSec. Esto agrega una carga a la comunicación, al igual que otras soluciones de VPN, que no es realmente necesaria para la comunicación entre sistemas de la misma red. Los pros y los contras del modo de túnel IPSec se han desarrollado en la sección anterior sobre VPN.

IPSec también puede asegurar el tráfico de un extremo a otro entre dos equipos (sin túnel) mediante el *modo de transporte* IPSec. Al igual que VPN, IPSec es una solución excelente en muchas circunstancias, si bien, como se aclarará en esta sección, no puede sustituir directamente a la protección de WLAN nativa que se distribuye en la capa de hardware de red.

Algunas de las ventajas de la protección del modo de transporte IPSec son:

- Es transparente para los usuarios. Al contrario de las VPN, no se precisa ningún procedimiento de inicio de sesión especial.
- La protección de IPSec es independiente del hardware de WLAN. Sólo precisa una WLAN abierta y sin autenticar. A diferencia de las VPN, no se necesitan servidores ni dispositivos adicionales porque la seguridad se negocia entre los equipos en cada extremo de la comunicación.
- La utilización de algoritmos de cifrado no se encuentra limitada por el hardware de WLAN.

Entre los inconvenientes de utilizar IPSec en lugar de la seguridad de WLAN nativa se incluyen:

- IPSec utiliza sólo la autenticación de nivel de equipo y no existe manera de implementar a la vez un esquema de autenticación basado en el usuario. Para muchas organizaciones, esto no supondrá ningún problema pero permite que los usuarios *no autorizados* se conecten a otros equipos protegidos con IPSec de la red si inician la sesión en un equipo *autorizado*.

  Nota: algunas implementaciones de IPSec en plataformas que no son de Windows utilizan sólo la autenticación de usuario. No obstante, al igual que ocurre con la solución de VPN, el equipo no se conectará a la red cuando el usuario no haya iniciado la sesión; de este modo, impide determinadas operaciones de administración y se desactivan las funciones de la configuración del usuario.

- La administración de directivas IPSec puede ser muy complicada en grandes organizaciones. Si se trata de imponer la protección general del tráfico IP, se podrían poner en peligro otros usos más especializados de IPSec, donde la protección de un extremo a otro es necesaria.
- La seguridad completa exige el cifrado de todo el tráfico de un extremo a otro, pero algunos dispositivos pueden ser incompatibles con IPSec. De este modo, se obligaría a que el tráfico hacia estos dispositivos se transmita sin cifrar. IPSec no ofrecerá protección para estos dispositivos, que quedarán expuestos a todos los usuarios que se conecten a la WLAN.
- Dado que la protección de IPSec se produce en la red en lugar de la capa de MAC, no es totalmente transparente para los dispositivos de red, tales como los servidores de seguridad. Algunas implementaciones de IPSec no funcionarán a través de un dispositivo de traducción de direcciones de red (NAT).
- IPSec de un extremo a otro no puede proteger el tráfico de difusión o multidifusión porque IPSec depende de dos partes que se autentican e intercambian claves mutuamente.
- Aunque los datos del interior de los paquetes IPSec se encuentran protegidos, la propia WLAN no está protegida. Un intruso podría seguir conectándose a la WLAN e intentar sondear o atacar cualquier dispositivo conectado a la WLAN; o bien escuchar el tráfico que no esté protegido con IPSec.
- El cifrado y descifrado de tráfico de la red IPSec carga la CPU del equipo. Esto puede sobrecargar en exceso los servidores utilizados. Aunque esta carga de procesamiento se puede desviar hacia tarjetas de red especializadas, es habitual que no se encuentren integradas de forma predeterminada.

Al igual que las VPN, IPSec constituye una solución excelente para muchas situaciones de seguridad pero no afronta la seguridad de la WLAN ni tampoco la protección de WLAN nativa.

Principio de la página

Selección de las opciones de WLAN correctas

A raíz del debate anterior, debería ser obvio que una solución de WLAN 802.1X es, con diferencia, la mejor opción disponible. Sin embargo y como se indica en la sección "Comprensión de la seguridad de WLAN", una vez que se ha decidido emplear una solución 802.1X, es preciso elegir entre una serie de opciones que conformarán la solución.

Las dos elecciones principales son:

- Si se emplean contraseñas o certificados para autenticar los equipos y los usuarios.
- Si se emplea la WEP dinámica o la protección de datos de WLAN de WPA.

Estos dos elementos son independientes el uno del otro.

Como se comentó con anterioridad en este documento, Microsoft posee dos guías sobre la solución de seguridad de WLAN; una, que emplea autenticación de contraseña y otra, que emplea autenticación de certificados. Estas soluciones funcionan tanto con WEP dinámica como con WPA.

Decisión de la solución de seguridad para WLAN correcta

El siguiente diagrama de flujo resume la elección entre las dos soluciones de seguridad de WLAN.

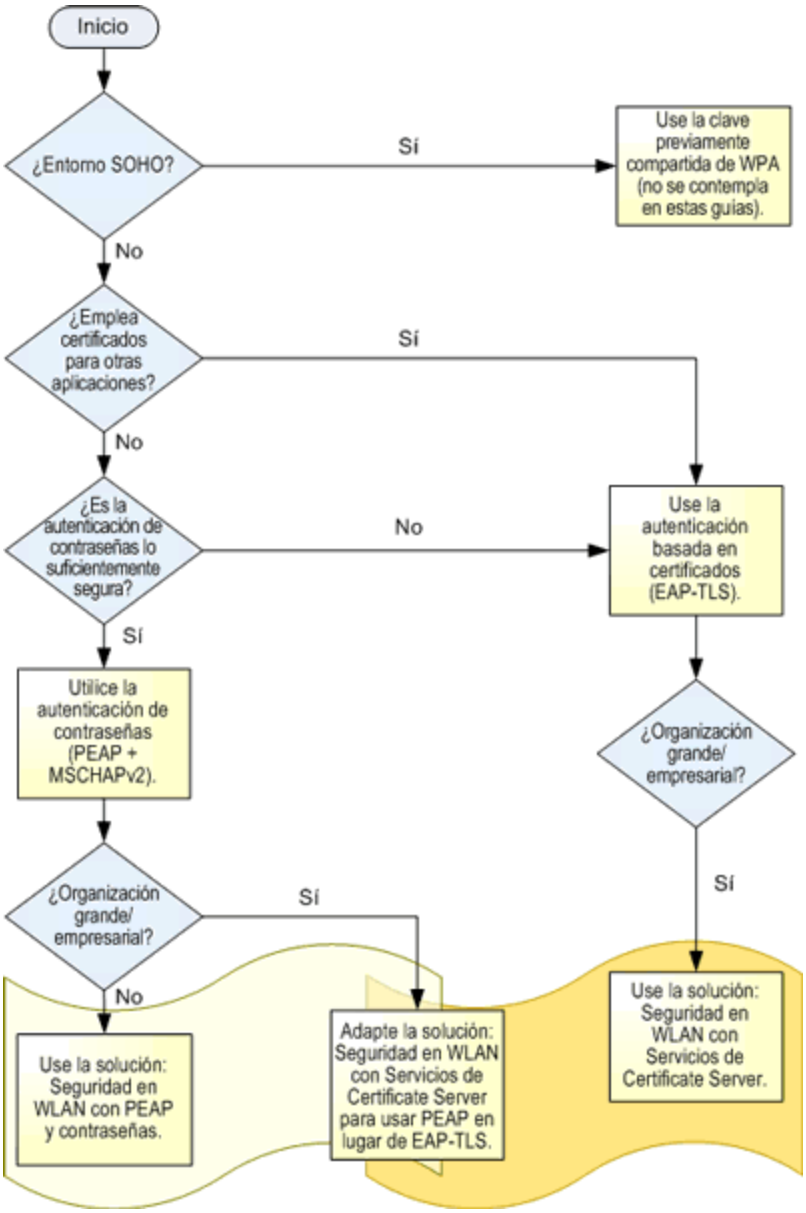

Figura 2. Árbol de decisión para las soluciones de seguridad de WLAN

Vista de imagen a pantalla completa

El resultado de este árbol de decisión depende del tamaño y de los requisitos de seguridad específicos de su organización. La mayoría de las organizaciones serán capaces de utilizar una u otra solución de WLAN de Microsoft sin ninguna modificación. Por ejemplo, la mayoría de las empresas, desde pequeñas a medianas, elegirá la solución más sencilla, basada en contraseñas, que se describe en la guía de la solución *Seguridad en LAN inalámbricas con PEAP y contraseñas*. Las empresas más grandes es más probable que se inclinen por la solución basada en certificados digitales: *Solución de Seguridad de LAN inalámbricas — Servicios de Certificate Server de Microsoft Windows Server 2003*.

Aunque cada una de las soluciones se desarrolló teniendo en mente dicho público, ambas son muy flexibles. Tanto las empresas que disponen de decenas de usuarios como las que cuentan con varios miles pueden implementar la *Seguridad en LAN inalámbricas con PEAP y contraseñas*. *Solución de Seguridad de LAN inalámbricas — Servicios de Certificate Server de Microsoft Windows Server 2003* se aplica a organizaciones con centenares o decenas de miles de usuarios (las empresas con menos de quinientos usuarios no suelen disponer

de suficientes recursos de TI para implementar y mantener las autoridades emisoras de certificados).

Un caso muy común y que no se ha tratado directamente en ninguna de las guías es el de las grandes empresas que implementan soluciones de WLAN basadas en contraseñas. Aunque los detalles técnicos de la solución *Seguridad en LAN inalámbricas con PEAP y contraseñas* son igualmente aplicables a las empresas grandes y pequeñas, muchos de los detalles de diseño, programación y funcionamiento necesarios para las organizaciones más grandes se han omitido por sencillez. Afortunadamente, las similitudes entre la arquitectura y los componentes técnicos empleados en ambas soluciones permite mezclar y ajustar partes de las soluciones con relativa facilidad. La solución *Seguridad en LAN inalámbricas con PEAP y contraseñas* dispone de un apéndice que le ofrece una guía acerca de las partes importantes de cada solución.

Elección entre WEP dinámica y WPA

La protección de datos de WEP, cuando se combina con la autenticación segura y la actualización de clave dinámica proporcionada por 802.1X y EAP, proporciona un nivel de seguridad que es más que adecuado para la mayoría de las organizaciones. No obstante, el estándar WPA mejora por encima de esto y ofrece mejores niveles de seguridad.

Las diferencias entre emplear WPA y una WEP dinámica en cualquiera de las soluciones son mínimas y la migración de un entorno WEP dinámico a un entorno WPA es muy sencilla. Los cambios fundamentales al pasar de una WEP dinámica al WPA son:

- Si su hardware de red (puntos de acceso inalámbrico y adaptadores de red inalámbricos) no admite el WPA actualmente, deberá obtener e implementar las actualizaciones de firmware necesarias para ello. Las actualizaciones de firmware para los adaptadores de red inalámbricos se incluyen a menudo en las actualizaciones de controladores de red.
- Deberá activar el WPA en sus puntos de acceso inalámbrico.
- La configuración de cliente WLAN debe modificarse para negociar el WPA en lugar de la seguridad de WEP.
- La directiva de acceso remoto sobre el tiempo de espera de la sesión en el servicio de autenticación de Internet (IAS), que se emplea para imponer una actualización de claves WEP, debería incrementarse con el fin de reducir la carga en el servidor IAS.

  Nota: IAS es la implementación del servidor RADIUS de Microsoft y se incluye en Windows Server 2003, aunque no se instala de forma predeterminada.

WPA debería ser la primera elección, si se encuentra disponible. No obstante, debería reflexionar acerca de si alguno de los siguientes problemas pudiese complicar más el empleo de WPA:

- Es posible que su hardware de red no sea compatible todavía con WPA (es poco probable que ocurra con los nuevos dispositivos, pero es posible que tenga una base amplia de hardware previo a WPA instalada).
- La compatibilidad con la configuración controlada por el GPO sólo se encuentra disponible en el Service Pack 1 de Windows Server 2003 (previsto para la segunda mitad de 2004); las versiones anteriores no eran compatibles así que la configuración de WPA debe establecerse manualmente en los clientes de Windows XP.
- Es posible que WPA no sea compatible con todos sus clientes; por ejemplo, Windows 2000 y anteriores o Pocket PC no disponen en la actualidad de compatibilidad integrada para WPA.

Si decide que todavía no se encuentra en condiciones de implementar WPA, debería implementar una solución de WEP dinámica y planear la migración a WPA cuando lo permitan las circunstancias.

Principio de la página

Resumen

Este documento ha intentado proporcionarle la información que necesita para elaborar su estrategia de seguridad para LAN inalámbricas. En la primera parte del documento se han examinado las ventajas empresariales de las redes inalámbricas y también las amenazas de la seguridad para las WLAN escasamente protegidas. En la sección intermedia se ha repasado cómo funciona la seguridad de WLAN basada en 802.1X,

EAP y la protección segura de datos para combatir estas amenazas. Las ventajas y desventajas relativas de las distintas opciones tales como VPN, IPSec y seguridad de WEP estática también se han abordado. La sección final incluye orientación sobre qué opciones de seguridad de WLAN seleccionar y cuáles de las soluciones de seguridad de WLAN de Microsoft se ajustaría mejor a su empresa.

Principio de la página

Referencias

Esta sección ofrece referencias a otra información complementaria importante u otro material informativo de relevancia para este documento.

- La solución de Microsoft para *Seguridad en LAN inalámbricas con PEAP y contraseñas* se encuentra disponible en la siguiente dirección URL:

  http://go.microsoft.com/fwlink/?LinkId=23459

- La solución de Microsoft para *Solución de Seguridad de LAN inalámbricas — Servicios de Certificate Server de Microsoft Windows Server 2003* se encuentra disponible en la siguiente dirección URL:

  http://go.microsoft.com/fwlink/?LinkId=14843

- Si precisa información técnica más detallada acerca de IEEE 802.11 y de las tecnologías relacionadas, consulte la sección "802.11 Wireless" del documento de referencia técnica de Windows Server 2003 disponible en la dirección URL:

  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/techref/w2k3tr_wir_intro.mspx

- Para obtener más información sobre 802.11, consulte la página Web de IEEE 802.11 en:

  http://www.ieee802.org/11/

- Para obtener más información sobre 802.1X, consulte la página Web de IEEE 802.1X en:

  http://www.ieee802.org/1/pages/802.1x.html

- Para obtener más información sobre el estándar EAP, consulte RFC 2284 en:

  http://www.ietf.org/rfc/rfc2284.txt?number=2284

- Para ver una descripción general del estándar WPA de la Alianza Wi-Fi, consulte la siguiente dirección URL:

  http://www.wi-fialliance.org/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf

- Para obtener más información sobre las redes inalámbricas, consulte el sitio de redes inalámbricas de Microsoft en la siguiente dirección URL:

  http://www.microsoft.com/wifi

- Para conocer una descripción detallada de PEAP y cómo se compara con LEAP (además de con EAP-TLS y EAP-MD5), consulte el artículo "The Advantages of Protected Extensible Authentication Protocol (PEAP): A Standard Approach to User Authentication for IEEE 802.11 Wireless Network" en la siguiente dirección URL:

  http://www.microsoft.com/windowsserver2003/techinfo/overview/peap.mspx

- El artículo "How Do I Limit My Exposure Against the Wireless LAN Security Threat? The New Realities of Protecting Corporate Information" del grupo META se encuentra disponible en:

  http://www.metagroup.com/cgi-bin/inetcgi/jsp/displayArticle.do?oid=35725

(Este artículo contiene referencias a guías de otros productos y vínculos a sitios Web que sólo están disponibles en inglés.)

Principio de la página

Administre su perfil