Latinoamérica

Microsoft TechNet

Capítulo 2: Determinación de una estrategia segura para redes inalámbricas

Publicado: octubre 11, aaaa | Actualizado: 24/11/04

En esta página

Introducción

La tecnología de redes de área local inalámbrica (WLAN, Wireless Local Area Network) constituye un tema polémico. La seguridad de este tipo de redes preocupa a las organizaciones que cuentan con una implementación de WLAN. Al mismo tiempo, las empresas que no han adoptado la tecnología muestran su inquietud por no poder aprovechar los beneficios que aporta en cuanto a la productividad de los usuarios y a la reducción del costo total de propiedad (TCO). Adicionalmente, existe cierto grado de confusión en lo que respecta a la seguridad del uso de WLAN en entornos corporativos.

Analistas y compañías de seguridad de redes dedican su tiempo a la resolución de las vulnerabilidades descubiertas en la primera generación de software de seguridad de WLAN. Muchos de estos esfuerzos han contribuido considerablemente a incrementar el nivel de seguridad inalámbrica. Otros, sin embargo, no han producido resultados tan acertados: unos introducen una serie diferente de vulnerabilidades de seguridad; otros requieren el uso de componentes de hardware muy caros; algunos incluso esquivan completamente el tema de la seguridad de WLAN mediante la adición de otra tecnología de seguridad potencialmente compleja, como la constituida por las redes privadas virtuales (VPN).

El Instituto de ingenieros eléctricos y electrónicos (IEEE, Institute of Electrical and Electronic Engineers) y otras organizaciones de estándares se han encargado diligentemente de redefinir y mejorar los estándares de seguridad inalámbrica de modo que la tecnología WLAN pueda hacer frente al entorno de seguridad hostil que caracteriza a este comienzo de siglo. Gracias al trabajo de estas organizaciones y líderes del sector, la expresión "seguridad de WLAN" ha perdido su condición de oxímoron. Ahora ya puede implementar y utilizar WLAN con un nivel de confianza en su seguridad muy alto.

Este capítulo sirve de introducción a dos soluciones de seguridad de WLAN de Microsoft y ofrece respuestas a multitud de preguntas sobre prácticas recomendadas para la seguridad de esta tecnología.

Descripción general de redes inalámbricas

El objetivo principal de este capítulo consiste en ayudarle a decidir la forma más apropiada de proteger la estructura de WLAN en su organización. Para ello, el documento cubre cuatro áreas principales:

- solución de problemas de seguridad asociados con WLAN.
- uso de estándares de WLAN seguros.
- adopción de estrategias alternativas, como la red privada virtual (VPN, Virtual Private Network) y la seguridad del protocolo Internet (IPsec, Internet Protocol security).

- selección de las opciones de WLAN adecuadas para su organización.

Microsoft ha desarrollado dos soluciones de WLAN a partir de estándares abiertos de organizaciones como el IEEE, el IETF y la Wi-Fi Alliance. Se trata de *Seguridad en LAN inalámbricas con Servicios de Certificate Server* y *Seguridad en LAN inalámbricas con PEAP y contraseñas*. Tal y como sugieren los nombres aplicados a estas soluciones, la primera utiliza certificados de claves públicas para llevar a cabo la autenticación de usuarios y equipos en la WLAN, mientras que la segunda hace uso simplemente de nombres de usuario y contraseñas. Por otro lado, la arquitectura básica de las dos soluciones es muy similar. Ambas toman como base la infraestructura de Microsoft® Windows Server™ 2003 y equipos cliente con Microsoft Windows® XP y Microsoft Pocket PC 2003.

Sin embargo, cada una de estas soluciones va dirigida a un grupo de usuarios diferente. La solución *Seguridad en LAN inalámbricas con Servicios de Certificate Server* está diseñada principalmente para organizaciones grandes con entornos de TI relativamente complejos, mientras que *Seguridad en LAN inalámbricas con PEAP y contraseñas* es una solución mucho más simple que puede implementarse fácilmente en empresas más pequeñas.

Esto no quiere decir que las organizaciones de mayor tamaño no puedan utilizar el sistema de autenticación por contraseñas ni que la autenticación por certificados no sea apropiada para organizaciones pequeñas. El uso de estas tecnologías refleja simplemente el tipo de organización en que suelen aplicarse con más frecuencia. El gráfico que aparece a continuación incluye un árbol de decisiones muy sencillo para ayudarle a seleccionar la solución de WLAN más apropiada para su organización.

Las tres opciones tecnológicas principales a su disposición para implementar seguridad de WLAN hacen referencia al uso de:

- clave previamente compartida (PSK, Pre-shared Key) con cifrado de acceso inalámbrico protegido (WPA, Wi-Fi Protected Access) para empresas pequeñas y oficinas domésticas.
- seguridad de WLAN basada en contraseñas para organizaciones que desean evitar el uso de certificados.
- seguridad de WLAN basada en certificados para organizaciones que desean implementar certificados.

Estas opciones de implementación se explican detalladamente más adelante en este capítulo, así como la posibilidad de combinar características de las dos últimas opciones para producir una solución híbrida.

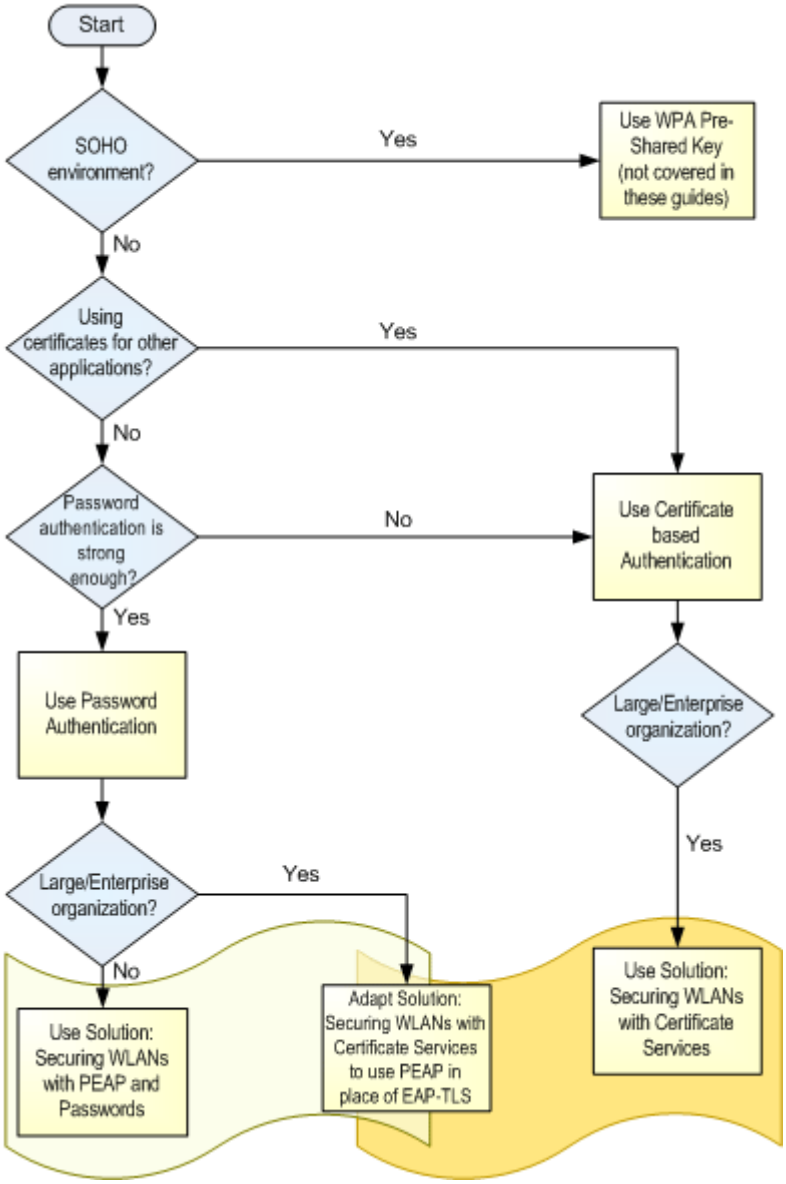

Figura 2.1 Árbol de decisiones para las dos soluciones de LAN inalámbrica de Microsoft

Principio de la página

Razones para el uso de redes inalámbricas

Resulta sencillo comprender el atractivo que presenta el uso de la tecnología WLAN para las organizaciones de hoy. De una forma u otra, la tecnología WLAN ha estado presente durante casi una década pero su uso solamente ha logrado aceptación recientemente. La adopción de WLAN empezó a adquirir popularidad cuando pudo producirse una tecnología fiable, basada en estándares y de bajo costo que respondiera a la creciente demanda de formas más flexibles de conseguir mayor conectividad en el trabajo. Sin embargo, el rápido incremento en el uso de este sistema ha revelado una serie de vulnerabilidades serias en la primera generación de WLAN. Esta sección presenta las ventajas (funcionalidad) y los inconvenientes (seguridad) de la tecnología WLAN.

Ventajas de las LAN inalámbricas

Las ventajas de la tecnología WLAN pueden dividirse en dos categorías principales: ventajas empresariales esenciales y ventajas operativas. Ventajas empresariales esenciales son aquellas que mejoran la productividad

de los empleados, permiten que los procesos empresariales sean más rápidos y eficaces o posibilitan la aparición de procesos empresariales totalmente nuevos. Las ventajas operativas están relacionadas con aspectos como la reducción de los costos administrativos o de los gastos de capital.

Ventajas empresariales esenciales

Las ventajas empresariales esenciales de la tecnología WLAN derivan del aumento en cuanto a flexibilidad y movilidad de los usuarios. Los empleados pueden alejarse de las mesas de trabajo y moverse por la oficina sin perder la conexión con la red. Puede resultar de utilidad estudiar algunos ejemplos sobre el modo en que las organizaciones se benefician del incremento en movilidad y flexibilidad en la red.

- Los trabajadores móviles que se desplazan de unas oficinas a otras se ahorran mucho tiempo y complicaciones gracias a la conexión permanente con la red de área local (LAN) corporativa. Los usuarios pueden conectarse de forma prácticamente inmediata desde cualquier ubicación física con cobertura inalámbrica y no necesitan andar buscando puertos de red, cables ni personal de TI que les 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 interrumpir las reuniones para que alguien vaya a buscar el informe correspondiente a las cifras del mes pasado 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. Las modificaciones en estructuras de equipos y proyectos, los cambios de estaciones de trabajo e incluso las mudanzas de oficina se llevan a cabo de forma más rápida y sencilla porque los empleados ya no están "encadenados" a sus mesas de trabajo.
- La integración de nuevos dispositivos y aplicaciones en el entorno de TI corporativo mejora de forma igualmente considerable. Dispositivos como los asistentes digitales personales (PDA) y Tablet PC, que hasta ahora 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, dispositivos y aplicaciones inalámbricos, que se podrán utilizar en áreas hasta ahora poco informatizadas, como fábricas, hospitales, tiendas y restaurantes.

Diferentes organizaciones experimentarán beneficios distintos, lo que variará en función de la naturaleza de la compañía y del tamaño y distribución geográfica de la plantilla, entre otros factores.

Ventajas operativas

Las ventajas operativas de la tecnología WLAN, es decir, las características que reducen los costos de capital y operativos, se pueden resumir de la siguiente manera:

- El costo de dotar a los edificios de acceso a la red se reduce considerablemente. Aunque la mayoría de las oficinas disponen de cableado para redes, muchos otros lugares de trabajo, como fábricas, almacenes y tiendas, no cuentan con esta comodidad. Ahora existe la posibilidad de utilizar redes en lugares donde el uso de una red por cable no sería práctico, por ejemplo, al aire libre, en el mar e incluso en el campo de batalla.
- El tamaño de la red se puede modificar con gran facilidad, en función de la demanda según va cambiando la organización o incluso diariamente, si es necesario. Es mucho más sencillo implementar una mayor concentración de puntos de acceso (AP) inalámbricos en una ubicación concreta que aumentar el número de puertos de red con cable.
- El costo de capital ya no se presenta ligado a la infraestructura del edificio, ya que la infraestructura de red inalámbrica se puede trasladar a otro edificio con relativa facilidad. El cableado suele constituir un costo permanente.

Problemas de seguridad asociados con WLAN

A pesar de todas las ventajas ofrecidas, las WLAN presentan ciertos problemas de seguridad que han llevado a muchas organizaciones a evitar la adopción de esta tecnología, sobre todo en sectores particularmente sensibles

a aspectos de seguridad, como el financiero y gubernamental. El riesgo que representa la difusión de datos de la red corporativa sin protección parece obvio; aun así, existen multitud de instalaciones de WLAN en funcionamiento sin ningún tipo de seguridad activada. La mayoría de las empresas han implementado algún método de seguridad inalámbrica. Sin embargo, esta seguridad suele presentarse únicamente en la forma de características básicas de primera generación que no ofrecen la protección adecuada en consonancia con los estándares de hoy.

Cuando se crearon los primeros estándares de WLAN IEEE 802.11, la seguridad no constituía una preocupación tan grande como en la actualidad, ni mucho menos. El nivel de amenazas era bastante inferior, al igual que su grado de sofisticación, y la adopción de tecnología inalámbrica aún era un proceso inusual. Este entorno vio el desarrolló del esquema de seguridad de WLAN de primera generación: el estándar de privacidad equivalente cableada (WEP, Wired Equivalent Privacy). WEP subestimó las medidas necesarias para conseguir un nivel de seguridad del aire “equivalente” al nivel de seguridad de un cable. Sin embargo, los métodos de seguridad de WLAN modernos están diseñados para funcionar perfectamente en entornos hostiles, como el aire, donde no existen perímetros de red o físicos obvios.

Es importante distinguir entre estructuras de WEP estática de primera generación (que hace uso de una contraseña compartida para proteger la red) y los esquemas de seguridad que utilizan cifrado WEP junto con administración de claves de cifrado y autenticación segura. Las primeras constituyen un esquema de seguridad completo que incluye autenticación y protección de datos; en este capítulo utilizaremos el término “*WEP estática*” para hacer referencia a este tipo de estructura. Por otro lado, el término “*WEP dinámica*” define únicamente el método de integridad y cifrado de datos que se usa en soluciones más seguras descritas más adelante en este capítulo.

Los puntos débiles de seguridad descubiertos en WEP estática crean vulnerabilidades para las WLAN protegidas por esta estructura que las convierten en víctimas de varios tipos de ataques. Herramientas de “auditoría” disponibles de forma gratuita, como Airsnort y WEPCrack, convierten la infiltración en redes inalámbricas protegidas por WEP estática en una tarea muy sencilla. Obviamente, las WLAN sin seguridad se encuentran expuestas a estas mismas amenazas; la única diferencia es que para llevar a cabo ataques de este tipo en WLAN desprotegidas se necesita menos tiempo, recursos y experiencia.

Antes de adentrarnos en el funcionamiento de las soluciones de seguridad de WLAN modernas, puede resultar útil repasar las amenazas principales a las que puede verse sometida una WLAN. La tabla siguiente presenta un resumen de estas amenazas:

Tabla 2.1: Principales amenazas físicas para WLAN

Amenaza	Descripción de la amenaza
Interceptación (revelación de datos)	La interceptación de datos trasmitidos puede resultar en la revelación de datos confidenciales y de credenciales de usuario sin protección, además de la usurpación de la identidad. Permite también que usuarios malintencionados con cierto grado de sofisticación puedan recopilar información sobre su entorno de TI y la utilicen para atacar sistemas o datos que, de otra forma, no serían vulnerables.
Interceptación y modificación de datos transmitidos	si un atacante consigue acceso a la red, puede introducir un equipo falso que intercepte y modifique las comunicaciones entre dos usuarios o equipos legítimos.
Imitación	El acceso fácil a la red interna permite a posibles atacantes falsificar datos aparentemente legítimos de modos que no sería posible hacerlo desde fuera de la red; por ejemplo, pueden imitarse mensajes de correo electrónico. Los usuarios, incluso los administradores de sistemas, suelen confiar en los elementos originados dentro de la red corporativa mucho más que en los procedentes del exterior.

Denegación del servicio (DoS)	Un atacante puede provocar un ataque de denegación de servicio de varios modos. Por ejemplo, la interrupción de las señales de radio se puede conseguir utilizando algo tan simple como un microondas. Existen ataques más complejos cuyo objetivo son los protocolos inalámbricos de nivel bajo, y otros menos complejos cuyo objetivo son las redes mediante un gran incremento del tráfico aleatorio en la WLAN.
Carga libre (robo de recursos)	Es posible que el objetivo del intruso sea algo tan simple como el uso de su red como punto de libre acceso a Internet. Aunque este tipo de amenaza no es tan preocupante como las anteriores, la carga libre no sólo reducirá el nivel de servicio disponible para los usuarios legítimos, sino que podría dar lugar a la introducción de virus y otras amenazas.
Amenazas accidentales	Algunas características de WLAN facilitan la incidencia de amenazas no intencionadas. Por ejemplo, un visitante autorizado podría iniciar su equipo portátil sin la intención de conectarse a la red pero la conexión a la WLAN de la compañía se produce de forma automática. 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 falsas	Aunque su organización no disponga oficialmente de una WLAN, existe el riesgo de amenazas por parte de WLAN no administradas que pueden hacer su aparición en la red. Hoy día es posible comprar hardware de WLAN muy barato, con lo que pueden introducirse vulnerabilidades no intencionadas en la red.

Los problemas de seguridad de las WLAN, sobre todo en lo que respecta a WEP estática, han recibido bastante atención por parte de los medios de comunicación. A pesar de que existen buenas soluciones de seguridad para hacer frente a estas amenazas, organizaciones de todos los tamaños se resisten a confiar plenamente en esta tecnología, hasta el punto de poner fin a su implementación o incluso prohibirla. Éstos son algunos de los factores clave que han contribuido a la confusión y a la falsa idea de que la tecnología WLAN equivale a redes desprotegidas:

- Falta de conocimientos sobre las tecnologías WLAN seguras y aquellas que no lo son. Tras el descubrimiento de una serie de errores en WEP estática, las empresas desconfían de todas las medidas de seguridad de WLAN. La desconcertante lista de estándares oficiales y soluciones de propiedad que dicen solucionar los problemas ha ayudado muy poco a aclarar la confusión.
- La conexión inalámbrica es invisible; para los administradores de seguridad de la red, este hecho no es solamente perturbador, sino que presenta un problema de administración de seguridad real. Con la tecnología convencional, es posible *ver* a un atacante que intenta conectar un cable a la red; la intrusión en una WLAN no se detecta tan fácilmente. Las defensas de seguridad físicas tradicionales de paredes y puertas utilizadas para proteger la red por cable no sirven de nada ante un intruso en entorno inalámbrico.
- En la actualidad se da mucha más importancia a la seguridad de la información. Las empresas exigen niveles de seguridad superiores en sus sistemas y no confían en tecnologías que podrían introducir vulnerabilidades.
- La aparición de requisitos normativos y legislativos que controlan la seguridad de los datos en una lista cada vez más extensa de países y sectores de industria es el resultado de la creciente preocupación por la seguridad de la información. Uno de los ejemplos más conocidos es la ley estadounidense HIPAA (Health Insurance Portability and Accountability Act) de 1996, que controla el manejo de la información sanitaria privada.

Principio de la página

Protección real de la WLAN

Desde el descubrimiento de las vulnerabilidades de seguridad de WLAN, proveedores de redes, organismos de estándares y analistas han dedicado gran parte de sus esfuerzos a la búsqueda de remedios para hacer frente a estos problemas. Esto ha dado lugar a diferentes reacciones en lo que respecta a la preocupación por la seguridad de la tecnología. Las alternativas principales son:

- no implementar tecnología WLAN.
- continuar usando la seguridad de WEP estática 802.11.
- utilizar una red privada virtual para proteger los datos en la WLAN.
- utilizar IPsec para proteger el tráfico de la WLAN.
- utilizar cifrado de datos y autenticación 802.1X para proteger la WLAN.

Estas estrategias alternativas se presentan ordenadas de menor a mayor según su eficacia, tomando como base una combinación de las características de seguridad, funcionalidad y capacidad de uso, aunque esto sea algo subjetivo. Microsoft recomienda la última de estas alternativas: cifrado WLAN y autenticación 802.1X. En la sección siguiente se ofrece una descripción de este enfoque y analizaremos su eficacia contra las amenazas principales mencionadas anteriormente en la tabla 2.1. El capítulo también incluye una mención de las ventajas e inconvenientes principales derivados del resto de las estrategias.

Protección de WLAN mediante cifrado de datos y autenticación 802.1X

Existen muy buenas razones para recomendar este enfoque (aunque su título y los términos poco claros que se utilizan para describirlo no sean una de ellas). Antes de pasar a la descripción de las ventajas que ofrecen las soluciones basadas en este enfoque, es importante esclarecer la terminología y explicar el funcionamiento de esta solución.

La seguridad de WLAN

La protección de una WLAN se compone de tres elementos principales:

- autenticación del usuario (o dispositivo) que se conecta a la red, lo que le permitirá disfrutar de un alto grado de confianza en lo que respecta a intentos de conexión a la red.
- autorización del usuario o dispositivo para utilizar la WLAN, lo que le permitirá controlar el acceso a la red.
- protección de la información transmitida en la red contra interceptaciones y modificaciones no autorizadas.

Adicionalmente es posible que requiera una función de auditoría para su WLAN, aunque la auditoría constituye principalmente un modo de comprobar y reforzar el resto de los elementos de seguridad.

Autorización y autenticación de red

La seguridad de WEP estática se basa en un sistema sencillo de secretos compartidos (contraseña o clave) para la autenticación de usuarios y dispositivos en la WLAN. Cualquier usuario que posea la clave secreta podrá acceder a la WLAN. Los defectos de cifrado de WEP presentan una gran oportunidad para cualquier atacante dispuesto a descubrir la clave de WEP estática en uso en la WLAN mediante herramientas que pueden conseguirse fácilmente. Además, el estándar WEP original no proporciona un método para actualizar o distribuir la clave de WEP, con lo que resulta muy difícil cambiarla. Una vez que se ha conseguido acceso no autorizado a una WLAN de WEP estática, resulta muy difícil restaurar la seguridad.

Con el objetivo de proporcionar un método de autenticación y autorización mucho más seguro, Microsoft y otros proveedores propusieron un marco de seguridad de WLAN con el protocolo 802.1X. El protocolo 802.1X es un estándar del IEEE que sirve para realizar la autenticación del acceso a una red y, si se desea, para administrar las claves utilizadas en la protección del tráfico. Su uso no se limita a las redes inalámbricas, sino que se implementa frecuentemente en conmutadores de LAN por cable de alto nivel.

El protocolo 802.1X hace uso del usuario de la red, un dispositivo de acceso a la red (o puerta de enlace) como, por ejemplo, un punto de acceso inalámbrico, y un servicio de autenticación y autorización llevado a cabo por un servidor de servicio de usuario de acceso telefónico de autenticación remota (RADIUS, Remote

Authentication Dial-In User Service). El servidor RADIUS se ocupa de autenticar las credenciales de los usuarios y autorizar su acceso a la WLAN.

El protocolo 802.1X se basa en el protocolo de autenticación extensible (EAP, Extensible Authentication Protocol) del IETF para llevar a cabo el intercambio de autenticación entre el cliente y el servidor RADIUS. El punto de acceso retransmite este intercambio. EAP es un protocolo general de autenticación compatible con muchos métodos de autenticación, basados en contraseñas, certificados digitales u otros tipos de credenciales.

EAP proporciona opciones de métodos de autenticación, de modo que no existe un único tipo de autenticación estándar de EAP. Diferentes circunstancias pueden requerir métodos de EAP igualmente diferentes, con diferentes tipos de credenciales y protocolos de autenticación. El uso de métodos de EAP en la autenticación de WLAN se describe más adelante en este capítulo.

Protección de datos de WLAN

Las decisiones sobre el uso de autenticación de 802.1X y el acceso a la red constituyen una sola parte de la solución. El otro componente importante será lo que se utilice para proteger el tráfico en la red inalámbrica.

Los defectos en el cifrado de datos WEP descritos anteriormente quizás no hubieran sido tan graves si la WEP estática hubiese incluido un método para actualizar las claves de cifrado regularmente de forma automática. Las herramientas utilizadas para averiguar la clave de acceso a una WEP estática necesitan recopilar entre uno y diez millones de paquetes cifrados con la misma clave para tener éxito. Las claves de WEP estática suelen permanecer sin variaciones durante semanas o meses, por lo que no es difícil para un atacante recopilar esta cantidad de información. Todos los equipos en una WLAN comparten la misma clave estática, de modo que el atacante puede recopilar transmisiones de datos de todos los equipos en la WLAN para descubrir la clave.

El uso de una solución basada en 802.1X permite la modificación frecuente de las claves de cifrado. Como parte del proceso de autenticación segura de 802.1X, el método EAP genera una clave de cifrado única para cada cliente. El servidor RADIUS exige la generación de claves de cifrado nuevas regularmente para mitigar ataques contra la clave de WEP (descritos anteriormente). Esto le permite utilizar algoritmos de cifrado WEP (presentes en la mayoría de los componentes de hardware de WLAN actuales) de un modo mucho más seguro.

WPA y 802.11i

Aunque WEP con claves de registro dinámicas de 802.1X constituye un sistema seguro en la mayoría de los casos, presenta algunos problemas persistentes, entre ellos:

- WEP utiliza una clave estática independiente para transmisiones globales como paquetes de difusión. Al contrario que ocurre con las claves por usuario, la clave global no se renueva de forma regular. Es poco probable que se transmitan datos confidenciales mediante paquetes de difusión pero el uso de una clave estática para transmisiones globales proporciona a usuarios malintencionados la posibilidad de descubrir información sobre la red como, por ejemplo, direcciones IP y nombres de usuarios y equipos.
- Los marcos de red protegidos por WEP cuentan con un nivel de protección de integridad muy bajo. El uso de técnicas de cifrado permite a posibles atacantes modificar la información en la WLAN y actualizar el valor de comprobación de integridad del marco sin que el receptor pueda detectar el cambio.
- Al tiempo que aumenta la velocidad de transmisión de WLAN y mejoran las técnicas de cifrado y la capacidad informática, las claves de WEP deben renovarse con mayor frecuencia. Es posible que esto suponga una carga inaceptable en los servidores RADIUS.

Para solucionar estos problemas, el IEEE está trabajando en un nuevo estándar de seguridad de WLAN llamado 802.11i y conocido también como "red de seguridad sólida" (RSN, Robust Security Network). La Wi-Fi Alliance, un consorcio formado por los principales proveedores de Wi-Fi, ha tomado una versión adelantada de 802.11i y la ha publicado en el estándar de seguridad de acceso protegido Wi-Fi (WPA, Wi – Fi Protected Access). WPA incluye un amplio subconjunto de características de 802.11i. La publicación de WPA ha permitido a la Wi-Fi Alliance exigir el uso del estándar WPA con todos los componentes que presentan el logotipo de Wi-Fi. Ahora, los proveedores de hardware de red Wi-Fi pueden ofrecer una opción estándar de alta seguridad previa a la publicación de 802.11i. WPA reúne un conjunto de características de seguridad ampliamente aceptadas como los métodos más seguros disponibles en la actualidad para proteger las WLAN.

WPA incluye dos modos de uso: uno que utiliza 802.1X y autenticación de RADIUS (simplemente conocido como

WPA) y un esquema más sencillo para entornos de SOHO que utiliza una clave previamente compartida (conocido como WPA PSK). WPA proporciona una combinación óptima de cifrado sólido y el mecanismo de autorización y autenticación seguro del protocolo 802.1X. La protección de datos que ofrece elimina las vulnerabilidades conocida de WEP por medio de:

- una clave de cifrado única para cada paquete.
- un vector de inicialización mucho más largo, con 128 bits adicionales de material de generación de claves, lo que duplica el espacio de claves.
- un valor de comprobación de integridad de mensaje firmado imposible de alterar o imitar.
- un contador de marcos cifrado incorporado para impedir ataques de reproducción.

Sin embargo, WPA utiliza algoritmos de cifrado similares a los utilizados por WEP, de modo que es posible implementar este estándar en hardware existente por medio de una simple actualización de firmware.

El modo PSK de WPA permite a organizaciones pequeñas y a usuarios de oficinas domésticas utilizar WLAN de claves compartidas sin las vulnerabilidades de WEP estática. La viabilidad de esta opción depende de la elección de una clave previamente compartida que sea lo suficientemente segura como para evitar simples ataques destinados a averiguar la contraseña. Al igual que WEP dinámica y WPA basado en RADIUS, las claves de cifrado individuales se generan para cada cliente inalámbrico. La clave previamente compartida se utiliza como credencial de autenticación; si el usuario posee la clave, recibe autorización para usar la WLAN y una clave de cifrado única para proteger los datos.

El estándar RSN 802.11i llevará las WLAN a un nivel de seguridad aún superior que incluirá protección mejorada contra ataques de denegación de servicio (DoS). La publicación del nuevo estándar se esperaba para mediados de 2004.

Métodos de autenticación de EAP

EAP es compatible con varios métodos de autenticación que pueden utilizar protocolos de autenticación diferentes, como la versión 5 de Kerberos, el protocolo de seguridad de la capa de transporte (TLS, Transport Layer Security) y el protocolo de Microsoft de autenticación por desafío mutuo (MS-CHAP, Microsoft Challenge Handshake Authentication). Adicionalmente pueden utilizar distintos tipos de credenciales, como contraseñas, certificados, tokens de contraseñas de uso único y biométrica. Aunque en teoría es posible utilizar cualquier método de EAP con el protocolo 802.1X, no todos son apropiados para el uso con WLAN. Especialmente, el método seleccionado debe ser adecuado para su uso en entornos desprotegidos y contar con la capacidad de generar claves de cifrado.

Los métodos de EAP principales que se utilizan con WLAN son: EAP-TLS, EAP protegido (PEAP, Protected EAP), TLS de túnel (TTLS, Tunneled TLS) y EAP ligero (LEAP, Lightweight EAP). PEAP y EAP-TLS son compatibles con Microsoft.

EAP-TLS

EAP-TLS es un estándar del IETF (RFC 2716) y probablemente sea el método de autenticación más utilizado hoy día, tanto en clientes inalámbricos como en servidores RADIUS. Usa certificados de claves públicas para autenticar los clientes inalámbricos y los servidores RADIUS mediante el establecimiento de una sesión TLS cifrada entre ellos.

PEAP

PEAP es un método de autenticación en dos fases. La primera establece una sesión de TLS con el servidor y permite que el cliente lleve a cabo la autenticación del mismo mediante el certificado digital del servidor. La segunda fase requiere un segundo método de EAP de túnel dentro de la sesión PEAP para llevar a cabo la autenticación del cliente con el servidor RADIUS. Esto ofrece a PEAP la posibilidad de utilizar métodos de autenticación de clientes diferentes, como contraseñas con la versión 2 del protocolo MS-CHAP (MS – CHAP v2) y certificados que usan EAP-TLS de túnel dentro de PEAP. Los métodos de EAP como MS-CHAP v2 no son lo suficientemente seguros como para usarse sin protección PEAP, pues quedarían susceptibles a ataques de diccionario sin conexión. La compatibilidad con PEAP está muy extendida en el sector; Microsoft Windows XP

SP1 y Pocket PC 2003 presentan compatibilidad incorporada para PEAP.

TTLS

TTLS es un protocolo de dos fases similar a PEAP que utiliza sesiones TLS para proteger la autenticación de clientes de túnel. Además de métodos EAP de túnel, TTLS también puede presentarse en la forma de versiones de protocolos de autenticación ajenos a EAP, como CHAP y MS-CHAP, entre otros. Microsoft y Cisco no son compatibles con TTLS, aunque otros proveedores disponen de clientes TTLS para plataformas diferentes.

LEAP

LEAP es un método de EAP desarrollado por Cisco que utiliza contraseñas para autenticar clientes. A pesar de su popularidad, LEAP solamente funciona con hardware y software de Cisco y algunos otros proveedores. Adicionalmente, LEAP cuenta con varias vulnerabilidades de seguridad, como la propensión a ataques de diccionario sin conexión (que permiten a los atacantes averiguar las contraseñas de los usuarios) y ataques de intermediario. En un entorno de dominio, LEAP únicamente puede llevar a cabo la autenticación del *usuario*, no del *equipo*, con la WLAN. Sin el proceso de autenticación de equipos, las directivas de grupo no se ejecutarán correctamente, pueden fallar los ajustes de instalación de software, los perfiles móviles y las secuencias de comandos de inicio de sesión, y los usuarios no podrán cambiar las contraseñas caducadas.

Hay varias soluciones de seguridad de WLAN que usan el protocolo 802.1X con otros métodos de EAP. Algunos de estos métodos, como EAP-MD5, presentan puntos débiles importantes de seguridad cuando se usan en un entorno de WLAN. Por este motivo no deben utilizarse. Existen otros métodos compatibles con el uso de token de contraseñas de uso único y otros protocolos de autenticación, como el protocolo Kerberos. Sin embargo, estos métodos no han conseguido todavía causar un impacto sustancial en el mercado de WLAN.

Ventajas de 802.1X con protección de datos de WLAN

En resumen, las ventajas principales derivadas del uso de una solución basada en el protocolo 802.1X para WLAN son las siguientes:

- **Alto nivel de seguridad:** el protocolo proporciona un esquema de autenticación muy seguro, ya que puede utilizar certificados de cliente o nombres y contraseñas de usuario.
- **Cifrado más seguro:** permite el cifrado seguro de los datos de la red.
- **Transparencia:** proporciona transparencia en la autenticación y conexión con la WLAN.
- **Autenticación de usuarios y equipos:** permite el uso de métodos de autenticación independientes para los usuarios y los equipos del entorno. La autenticación de equipos independiente permite la administración de los equipos en el entorno aunque no se encuentren en uso por parte de los usuarios.
- **Rentabilidad:** el hardware de red es muy barato.
- **Alto rendimiento:** el cifrado se lleva a cabo en el hardware de WLAN en lugar de en la CPU del equipo cliente, de modo que el cifrado WLAN no influye de ningún modo en el rendimiento de este último.

Deben tenerse en cuenta algunas advertencias referentes al uso de una solución basada en el protocolo 802.1X.

- Aunque este protocolo cuenta ya con una aceptación prácticamente internacional, el uso de métodos de EAP diferentes significa que el aspecto de interoperabilidad no puede garantizarse siempre.
- WPA se encuentra aún en una fase temprana de adopción y quizás no esté disponible en los componentes de hardware más antiguos.
- La siguiente generación del estándar RSN (802.11i) aún no está ratificada y su uso requerirá la implementación de actualizaciones de hardware y software (el hardware de red suele requerir una actualización de firmware).

Sin embargo, estas cuestiones son de poca importancia, sobre todo al compararlas con las ventajas derivadas del uso del protocolo 802.1X y, en particular, con la gravedad de los problemas planteados por el uso de enfoques alternativos (que se describen más adelante en este capítulo).

Resistencia de la solución 802.1X frente a las amenazas de seguridad
Una tabla incluida anteriormente en este capítulo ofrecía una descripción de las principales amenazas de seguridad para WLAN. La tabla siguiente evalúa las posibles amenazas contra una solución basada en el protocolo 802.1X y protección de datos de WLAN.

Tabla 2.2: Amenazas contra la seguridad evaluadas 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 no se puede descubrir las claves y el acceso a los datos de ninguna forma conocida (siempre y cuando la actualización de claves se lleve a cabo con frecuencia). WPA ofrece mayor seguridad, ya que las claves de cifrado son diferentes para cada paquete. La clave global (que protege el tráfico de difusión) cambia para cada paquete.
Interceptación y modificación de datos transmitidos	Puesto que entre el cliente inalámbrico y el punto de acceso inalámbrico se utiliza el cifrado mediante claves dinámicas, ningún usuario malintencionado puede interceptar los datos y modificarlos. La autenticación mutua entre el cliente, el servidor RADIUS y el AP 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 falsos desde el interior.
Denegación de servicio (DoS)	Pueden evitarse los ataques de exceso de datos, entre otros ataques de denegación de servicio, mediante el control de acceso a la WLAN con el protocolo 802.1X. No existe ningún modo de defensa contra ataques DoS de 802.11 de bajo nivel en WEP dinámica ni WPA. El estándar 802.11i se ocupará de esta cuestión. Sin embargo, este estándar tampoco será inmune a trastornos de la capa física (nivel de radio) de las redes. Estas vulnerabilidades son características de las WLAN 802.11 actuales y comunes en el resto de las opciones mencionadas anteriormente en este capítulo.
Carga libre (robo de recursos)	El requisito de autenticación segura impide el uso no autorizado de la red.
Amenazas accidentales	El requisito de autenticación segura impide la conexión accidental a la WLAN.
WLAN falsas	Si bien la solución no se ocupa directamente de los puntos de acceso inalámbricos falsos, la implementación de una solución inalámbrica segura como ésta elimina prácticamente los motivos para establecer una WLAN falsa. Sin embargo, debería considerar la creación y publicación de una directiva clara que prohíba el uso de WLAN no autorizadas. Puede forzar su implementación mediante herramientas de software que

	exploran la red en busca de direcciones de hardware de punto de acceso inalámbrico y equipos de detección de WLAN de mano.

Otros enfoques a la seguridad de WLAN

En la sección anterior nos ocupamos en detalle de la autenticación de 802.1X con protección de datos de WLAN. Esta sección ofrece una descripción de las otras cuatro alternativas a la seguridad de WLAN mencionadas anteriormente en este capítulo (al principio de la sección Protección real de la WLAN).

Los cuatro enfoques alternativos eran los siguientes:

- no implementar tecnología WLAN.
- continuar usando la seguridad de WEP estática 802.11.
- utilizar una red privada virtual para proteger los datos en la WLAN.
- utilizar IPsec para proteger el tráfico de la WLAN.

Las diferencias clave entre estos enfoques y la solución basada en el protocolo 802.1X quedan resumidas en la tabla siguiente (aunque la opción “No WLAN” no se incluye porque no puede compararse directamente con el resto). Estas opciones se describen con mayor detalle en secciones posteriores de este mismo capítulo.

Tabla 2.3: Comparación de los enfoques de seguridad de WLAN

Característica	WLAN 802.1X	WEP estática	VPN	IPsec
Autenticación segura (1)	Sí	No	Sí, pero no en el caso de VPN que utilizan autenticación de clave compartida.	Sí, siempre y cuando se use la autenticación de certificados o de Kerberos.
Cifrado de datos seguro	Sí	No	Sí	Sí
Transparencia en conexión y reconexión a WLAN	Sí	Sí	No	Sí
Autenticación de usuarios	Sí	No	Sí	Sí
Autenticación de equipos (2)	Sí	Sí	No	Sí
Tráfico de difusión y multidifusión protegido	Sí	Sí	Sí	No
Se requieren dispositivos de red adicionales	Servidores RADIUS	No	Servidores VPN, servidores RADIUS	No
Garantiza el acceso a la WLAN	Sí	Sí	No	No

(1) Muchas implementaciones de VPN que usan el modo de túnel IPsec utilizan un esquema de autenticación de clave compartida poco seguro conocido como *XAuth*.

(2) La autenticación de equipos permite que éstos permanezcan conectados a la WLAN y la red corporativa incluso en el caso de que no haya usuarios utilizándolos. Esta capacidad resulta necesaria para que las características de dominio de Windows siguientes funcionen correctamente:

- perfiles de usuarios móviles.
- configuración de la directiva de grupo de equipos (especialmente, secuencias de comando de inicio y software implementado).
- secuencias de comando de inicio de sesión de usuario y software implementado mediante la directiva de grupo.

Alternativa 1: no implementar tecnología WLAN.
Quizás la forma más obvia de evitar por completo los riesgos de seguridad con WLAN sea sencillamente no implementar este sistema. Sin embargo, además de no poder beneficiarse de las ventajas derivadas del uso de WLAN (descritas anteriormente en este capítulo), encontrará que esta estrategia no le proporcionará un entorno completamente libre de dificultades. Las organizaciones que optan por esta alternativa acaban por pagar lo que el grupo META llama el “precio de la demora”, que es mucho más que el simple costo de la oportunidad perdida. El grupo META llevó a cabo un estudio sobre el crecimiento del uso no administrado de LAN por cable hace una década. En la mayoría de los casos, los departamentos de TI centrales se vieron obligados a tomar el control de la implementación de LAN de forma reactiva. El costo asociado a la reestructuración de la multitud de las LAN de departamentos independientes y, a menudo, incompatibles era enorme. Si desea obtener más información sobre la restricción de riesgos de seguridad con LAN inalámbricas y la protección de información corporativa, 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 12 de diciembre de 2002.

Ésta es una amenaza constante con las WLAN, sobre todo en organizaciones grandes donde, a menudo, es difícil ver físicamente lo que sucede en cada ubicación. La implementación "de raíz" no administrada de WLAN (facilitada por el bajísimo costo de los componentes) constituye, potencialmente, el peor de los escenarios, ya que expone a la organización a todas las amenazas de seguridad descritas anteriormente y, además, sin que el grupo central de TI sea consciente de ello o pueda tomar medidas para hacer frente a los riesgos.

Esto indica que si su estrategia es la de no adoptar la tecnología WLAN, debe ponerla en práctica de forma activa y no pasiva. Debe respaldar esta decisión con una directiva muy clara y asegurarse de que todos los empleados la conocen y están al tanto también de las consecuencias que pueden derivarse de su incumplimiento. Quizás debiera considerar el uso de sistemas de exploración y monitores de paquetes de red para detectar el uso no autorizado de componentes inalámbricos.

Alternativa 2: uso de seguridad básica mediante 802.11 (WEP estática).
Esta alternativa utiliza una clave compartida para controlar el acceso a la red y la misma clave sirve para cifrar el tráfico inalámbrico. Este modelo simple de autorización suele complementarse con el filtrado de puertos basado en direcciones de hardware de tarjeta de WLAN, aunque este proceso no forma parte de la seguridad 802.11. El mayor atractivo de este enfoque es su sencillez. Si bien ofrece una seguridad mayor que las WLAN desprotegidas, este sistema conlleva serios inconvenientes de administración y seguridad, sobre todo para empresas de gran tamaño.

Entre los inconvenientes derivados del uso de WEP estática se incluyen los siguientes:

- Las claves de WEP estática se pueden averiguar en cuestión de horas en una red muy ocupada por medio de un equipo que cuente con un adaptador de WLAN y herramientas de piratería como Airsnort o WEPCrack.
- El punto más débil de WEP estática es que no existe ningún mecanismo para asignar ni actualizar la clave de cifrado de red dinámicamente. Sin 802.1X y EAP para implementar la actualización frecuente de la clave, el algoritmo de cifrado que utiliza la WEP estática queda vulnerable a ataques de recuperación de claves.
- Es posible cambiar las claves estáticas pero el proceso de modificación en los clientes inalámbricos y puntos de acceso es, por lo general, manual y laborioso. Además, las claves deben actualizarse simultáneamente en

los clientes y los puntos de acceso para conservar la conectividad de los clientes. En la práctica, esto es tan difícil de conseguir que las claves suelen dejarse sin cambiar permanentemente.

- La clave estática necesita compartirse entre todos los usuarios de la WLAN y todos los puntos de acceso inalámbricos. Ya de por sí, esta situación crea una vulnerabilidad, ya que un secreto compartido por multitud de personas y dispositivos no suele ser secreto durante mucho tiempo.

La WEP estática proporciona a las WLAN un mecanismo de control de acceso muy limitado basado en el conocimiento de la clave de WEP. Si se descubre el nombre de la red (lo que es muy fácil) y la clave de WEP, es posible conectarse a la red.

Un modo de mejorar esta situación es la configuración de los puntos de acceso inalámbricos de forma que sólo admitan un conjunto predefinido de direcciones de adaptadores de red cliente. Esto recibe el nombre de filtrado de direcciones de control de acceso a medios (MAC, Media Access Control). La capa MAC hace referencia al firmware de nivel bajo del adaptador de red.

El filtrado de direcciones de adaptadores de red para controlar el acceso tiene los problemas siguientes:

- la capacidad de administración deja mucho que desear. El mantenimiento de una lista de direcciones de hardware para algo más que un número reducido de clientes es una tarea compleja. Además, la distribución y la sincronización de esta lista en todos los puntos de acceso constituye un desafío considerable.
- la escalabilidad tampoco es buena. Los puntos de acceso pueden tener un límite finito del tamaño de la tabla de filtros, 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 suplantar 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 previamente compartidas solamente resultan prácticas para números reducidos de usuarios y puntos de acceso debido a la dificultad asociada a la administración de actualizaciones de claves en ubicaciones múltiples. Los problemas de cifrado con WEP dan a su utilidad un carácter dudoso incluso en entornos pequeños.

Por su parte, el modo de clave previamente compartida de WPA proporciona a organizaciones pequeñas un nivel de seguridad alto a cambio de una carga en la infraestructura muy baja. Existe una amplia gama de componentes de hardware compatibles con WPA PSK y es posible configurar clientes WLAN manualmente. Todas estas razones hacen que WPA PSK sea la configuración preferida para entornos de SOHO.

Alternativa 3: uso de redes privadas virtuales.
Probablemente, las VPN constituyen la forma más popular de cifrado de red; son muchos los usuarios que confían en las tecnologías probadas y de confianza de VPN para proteger la confidencialidad de los datos transmitidos por Internet. Cuando se descubrieron las vulnerabilidades de WEP estática, VPN se presentó rápidamente como el mejor modo de proteger los datos en una WLAN. Este enfoque recibió el apoyo de analistas, como Gartner Group, y, como era de esperar, los proveedores de soluciones VPN promocionaron su uso con entusiasmo.

VPN constituye una solución excelente para el desplazamiento seguro en una red hostil como Internet (aunque la calidad de las implementaciones VPN puede variar considerablemente). Sin embargo, no es necesariamente la mejor solución para asegurar WLAN internas. Para este tipo de entorno, una VPN no ofrece prácticamente ningún grado de seguridad adicional en comparación con las soluciones 802.1X. Adicionalmente, incrementa la complejidad y los costos significativamente, reduce la capacidad de uso y anula el funcionamiento de características importantes.

Nota: estas limitaciones no se aplican al uso de VPN para proteger el tráfico en puntos de conexión públicos de LAN inalámbrica. La protección de los datos de red de usuarios que se conectan a redes remotas hostiles constituye un uso legítimo de VPN. En este tipo de escenario, los usuarios aceptan que la conectividad segura sea más rigurosa y menos funcional que una conexión de LAN, algo que no esperan que ocurra en las oficinas

de la empresa.

Las ventajas asociadas con el uso de VPN para proteger WLAN incluyen las siguientes:

- la mayoría de las organizaciones ya cuentan con una implementación de VPN, de modo que los usuarios y el personal de TI ya están familiarizados con la solución.
- la protección de datos VPN suele utilizar cifrado de software que permite la modificación y actualización de los algoritmos de forma mucho más sencilla que con cifrado basado en hardware.
- quizás pueda usar hardware de costo algo más reducido, ya que la protección VPN es independiente del hardware de WLAN (aunque el precio elevado de hardware de red compatible con 802.1X ya ha desaparecido prácticamente).

Los inconvenientes del uso de VPN en lugar de seguridad de WLAN nativa incluyen:

- VPN no ofrece transparencia de usuario. Normalmente, los clientes VPN requieren que el usuario inicie la conexión con el servidor VPN de forma manual. Por lo tanto, la conexión nunca será tan transparente como una conexión de LAN por cable. Es probable que los clientes VPN ajenos a Microsoft necesiten especificar credenciales de inicio de sesión al intentar conectar a la red, además del inicio de sesión de dominio o red estándar. Los clientes tendrán que volver a conectarse a la red en caso de que la VPN los desconecte como consecuencia de una señal de WLAN de baja calidad o si el usuario se desplaza entre puntos de acceso.
- el inicio de la conexión de VPN debe llevarlo a cabo el usuario, por lo que los equipos inactivos no estarán conectados a la red privada virtual (y, consecuentemente, a la LAN corporativa). Por lo tanto, no puede realizarse la administración ni la supervisión remota de los equipos a menos que haya usuarios conectados. Esto podría impedir la aplicación de algunos aspectos de la configuración de objetos de directiva de grupo (GPO, Group Policy Object) de equipos como, por ejemplo, secuencias de comandos de inicio de sesión y software asignado a equipos.
- es posible que los perfiles móviles, las secuencias de comandos de inicio de sesión y el software implementado mediante GPO no funcione como debería. A menos que el usuario decida iniciar la sesión por medio de la conexión VPN desde el inicio de sesión de Windows, el equipo no se conectará a la LAN corporativa hasta que el usuario haya iniciado la sesión y la conexión VPN. Hasta entonces, fallará cualquier intento de acceso a la red segura. Quizás resulte imposible llevar a cabo un inicio de sesión completo en una conexión VPN con clientes VPN ajenos a Microsoft.
- la reanudación de la actividad tras la suspensión o hibernación no reestablece la conexión VPN de forma automática; el usuario tendrá que hacerlo manualmente.
- aunque la información en el túnel de VPN está protegida, la VPN no ofrece protección alguna a la WLAN. Un intruso puede conectarse a la WLAN y sondear o atacar cualquier dispositivo conectado a ella.
- los servidores VPN pueden convertirse en limitaciones. Todo acceso de clientes WLAN a la LAN corporativa se realiza a través del servidor VPN. Normalmente, los dispositivos de VPN dan servicio a muchos clientes remotos de baja velocidad. Por lo tanto, la mayoría de las puertas de enlace de VPN no pueden soportar decenas o cientos de clientes ejecutándose a la velocidad máxima de LAN.
- seguramente, el costo del hardware adicional y la administración constante de dispositivos VPN será muy superior al costo de una solución de WLAN nativa. Por lo general, cada sitio necesita su propio servidor VPN además de puntos de acceso de WLAN.
- las sesiones de VPN son más propensas a la desconexión cuando los clientes se desplazan entre puntos de acceso. Normalmente, las aplicaciones toleran una desconexión momentánea durante el cambio de puntos de acceso inalámbricos; sin embargo, incluso una breve interrupción de la conexión VPN requerirá que el usuario vuelva a establecerla de forma manual.
- el costo de licencias de software cliente y servidor VPN, además del costo de la implementación del software, podría suponer un problema para soluciones VPN ajenas a Microsoft. Es posible que se produzcan problemas referentes a la compatibilidad de software cliente VPN, ya que los clientes ajenos a Microsoft suelen sustituir

características básicas de Windows.

- muchos analistas y proveedores dan por hecho que el nivel de seguridad de VPN es siempre superior al nivel de seguridad de WLAN. Quizás esto sea cierto en lo que respecta a WEP estática pero no lo es necesariamente para las soluciones 802.1X basadas en EAP descritas en este capítulo. Particularmente, los métodos de autenticación de VPN son a menudo mucho *menos* seguros y, en el mejor de los casos, no ofrecen una seguridad considerablemente mayor. 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 v2). Muchas implementaciones de VPN, especialmente las basadas en el modo de túnel IPsec, usan la autenticación de clave previamente compartida (una contraseña de grupo). Se ha demostrado que este sistema conlleva vulnerabilidades de seguridad graves; irónicamente, comparte algunas de ellas con WEP estática.
- las VPN no ofrecen ningún tipo de seguridad a la WLAN. Aunque la información en los túneles de VPN está protegida, cualquiera puede conectarse a la WLAN e intentar atacar clientes inalámbricos legítimos y otros dispositivos en la WLAN.

VPN resulta ideal para proteger el tráfico en redes hostiles, tanto si el usuario está utilizando una conexión de banda ancha desde casa como si se trata de un punto de conexión público inalámbrico. Sin embargo, VPN no se diseñó para proteger tráfico de red en redes internas. En esta función, VPN resulta demasiado torpe para la mayoría de las organizaciones, la funcionalidad es demasiado restrictiva para el usuario y su mantenimiento demasiado costoso y complejo para el departamento de TI.

En casos excepcionales, cuando se necesita un nivel de seguridad superior para un tipo específico de tráfico o conexión, esta seguridad adicional puede proporcionarla un túnel de VPN o un modo de transporte IPsec, *además* de la protección de WLAN nativa. Éste supone un uso mucho más razonable de los recursos de red.

Alternativa 4: uso de seguridad de IP

IPsec permite a dos usuarios de red autenticarse mutuamente de forma segura y autenticar o cifrar paquetes de red individuales. Puede usar IPsec para colocar una red sobre la otra en modo de túnel de forma segura o simplemente para proteger paquetes IP transmitidos entre dos equipos.

El modo de túnel IPsec suele utilizarse en conexiones VPN de sitio a sitio o de acceso de cliente. Constituye una forma de VPN que funciona mediante la encapsulación de un paquete IP completo dentro de un paquete IPsec protegido. Al igual que ocurre con otras soluciones VPN, esto añade una carga a la comunicación que no se necesita realmente para la comunicación entre sistemas en la misma red. Las ventajas y los inconvenientes del modo de túnel IPsec se trataron en la descripción de VPN en la sección anterior.

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

Algunas de las ventajas de la protección por medio del modo de transporte IPsec son:

- la transparencia para los usuarios. Al contrario que ocurre con VPN, no se requiere ningún procedimiento de inicio de sesión especial.
- la protección de IPsec es independiente del hardware de WLAN. Solamente requiere una WLAN abierta, sin autenticar. Una vez más, al contrario que ocurre con VPN, no se necesitan servidores o dispositivos adicionales, ya que la negociación de la seguridad se lleva a cabo directamente entre los equipos a cada extremo de la comunicación.
- el uso de algoritmos de cifrado no está restringido por el hardware de WLAN.

Los inconvenientes del uso de IPsec en lugar de seguridad de WLAN nativa incluyen:

- IPSec utiliza sólo la autenticación de nivel de equipo y no hay forma de implementar a la vez un esquema de autenticación basado en el usuario. En muchas organizaciones, esto no constituirá necesariamente un problema pero si algún usuario *no autorizado* consigue iniciar la sesión en un equipo *autorizado*, podrá acceder también a otros equipos protegidos por IPsec en la red.

Nota: algunas implementaciones de IPSec en plataformas ajenas a Windows utilizan sólo la autenticación de usuario. Sin embargo, al igual que sucede con la solución de VPN, el equipo no estará conectado a la red a menos que el usuario haya iniciado la sesión, lo que impide que se lleven a cabo determinadas operaciones administrativas y desactiva la funcionalidad de la configuración del usuario.

- la administración de directivas de IPSec puede ser muy complicada en grandes organizaciones. Los intentos de forzar la protección general del tráfico de IP podrían interferir con otros usos más especializados de IPSec, donde la protección de extremo a extremo es realmente necesaria.
- la seguridad completa exige el cifrado de todo el tráfico de extremo a extremo pero algunos dispositivos pueden ser incompatibles con IPSec, con lo que el tráfico se transmitirá a estos dispositivos sin cifrar. IPsec no proporcionará ningún tipo de protección a estos dispositivos, de modo que estarán expuestos a cualquiera que se conecte a la WLAN.
- la protección de IPSec se manifiesta al nivel de la red en lugar de producirse en la capa de MAC, por lo que no es totalmente transparente para dispositivos de red, como los servidores de seguridad. Algunas implementaciones de IPsec no funcionarán en un dispositivo de traducción de direcciones de red (NAT, Network Address Translation).
- IPsec de extremo a extremo no puede proteger tráfico de difusión o multidifusión, ya que IPsec se basa en dos partes que se autentican e intercambian claves mutuamente.
- aunque la información en los paquetes IPsec está protegida, la WLAN no lo está. Un intruso puede conectarse a la WLAN y sondear o atacar cualquier dispositivo conectado a ella o escuchar tráfico que no está protegido por IPsec.
- el cifrado y descifrado de tráfico de red IPsec incrementa la carga en las CPU de los equipos. A su vez, esto puede sobrecargar los servidores de uso intensivo. Esta carga de procesamiento puede desviarse a tarjetas de red especiales pero no suelen venir integradas en los servidores.

Al igual que VPN, IPsec constituye una solución excelente para muchos escenarios de seguridad pero no se ocupa de la seguridad de WLAN tan satisfactoriamente como la protección de WLAN nativa.

Principio de la página

Selección de las opciones de WLAN adecuadas

Si partimos de la explicación en la sección anterior, la solución de WLAN 802.1X es la mejor de todas las alternativas disponibles sin lugar a dudas. Sin embargo, tal y como se mencionó en la sección La seguridad de WLAN, tras tomar la decisión de utilizar una solución 802.1X, tendrá que elegir entre varias opciones para que su funcionamiento sea correcto.

las dos opciones principales son las siguientes:

- el uso de contraseñas o certificados para la autenticación de usuarios y equipos.
- el uso de protección de datos de WLAN WPA o WEP dinámica.

Estas dos opciones son independientes una de la otra.

Como ya mencionamos anteriormente en este capítulo, Microsoft cuenta con dos guías de soluciones de seguridad de WLAN: una de ellas utiliza autenticación de contraseñas y la otra, de certificados. Ambas soluciones funcionan con WPA o WEP dinámica.

Selección de la solución de seguridad de WLAN adecuada

El diagrama de flujo siguiente muestra un resumen de las opciones entre las dos guías de soluciones de seguridad de WLAN.

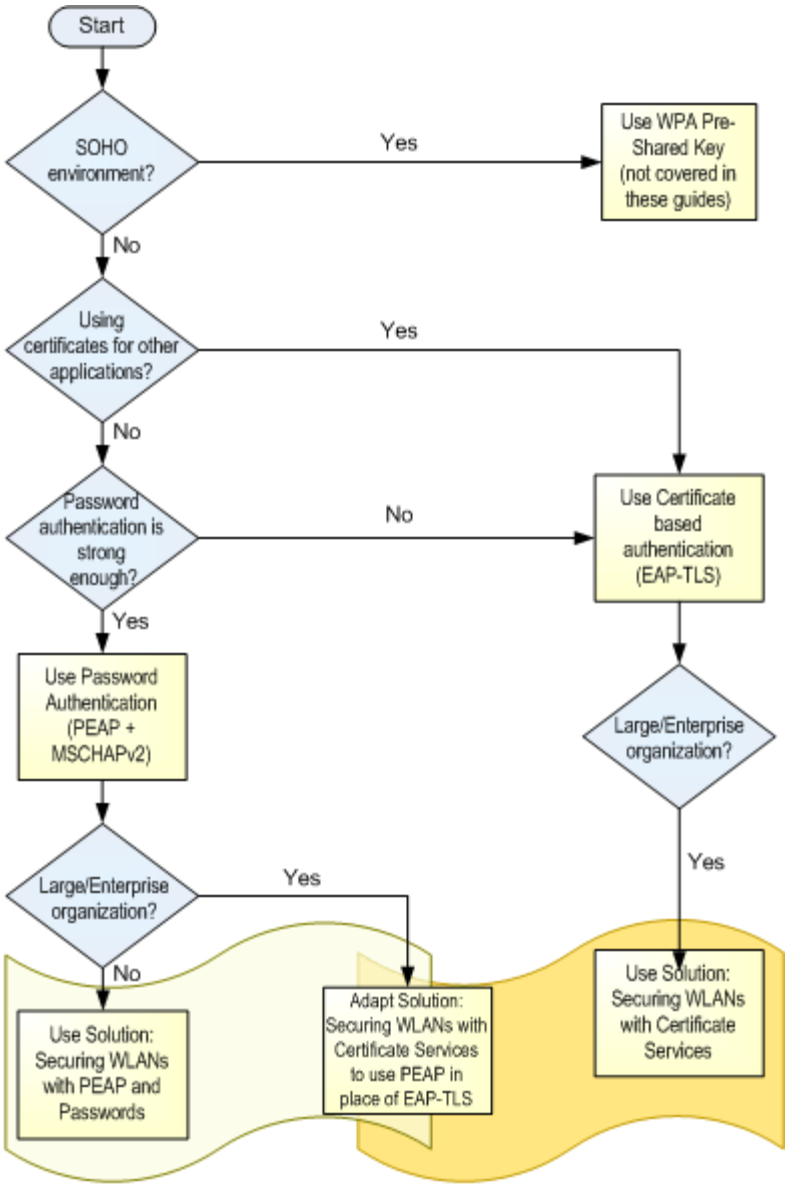

Figura 2.2 Árbol de decisiones para las soluciones de seguridad de WLAN

El resultado de este árbol de decisiones dependerá del tamaño de la organización, así como de sus requisitos de seguridad específicos. La mayoría de las organizaciones pueden utilizar cualquiera de las soluciones de WLAN de Microsoft sin necesidad de modificaciones. Por ejemplo, gran parte de las empresas pequeñas y medianas elegirán la solución más simple de autenticación de contraseñas descrita en la guía de la solución *Seguridad en LAN inalámbricas con PEAP y contraseñas*. Las organizaciones más grandes suelen decantarse por el uso de la guía de la solución *Seguridad en LAN inalámbricas con Servicios de Certificate Server*, basada en certificados digitales.

Aunque cada solución se desarrolló pensando en estos usuarios, ambas permiten aprovechar un alto grado de flexibilidad. *Seguridad en LAN inalámbricas con PEAP y contraseñas* puede implementarse en organizaciones que tienen decenas o miles de usuarios. La solución *Seguridad en LAN inalámbricas con Servicios de Certificate Server* se aplica a empresas de cientos a decenas de miles de usuarios (las organizaciones con menos de quinientos usuarios no suelen disponer de recursos de TI suficientes para implementar y mantener las entidades emisoras de certificados).

Un caso común que escapa a las dos guías es el de organizaciones grandes que implementan una solución de

WLAN basada en contraseñas. Aunque los detalles técnicos en la solución *Seguridad en LAN inalámbricas con PEAP y contraseñas* pueden aplicarse tanto a empresas pequeñas como grandes, omitimos gran parte del diseño, planeamiento y detalle operativo requerido en las organizaciones más grandes en virtud de la sencillez. Afortunadamente, la semejanza de la arquitectura y los componentes técnicos utilizados en ambas soluciones permiten mezclar partes de ambas soluciones sin mucha dificultad. La solución *Seguridad en LAN inalámbricas con PEAP y contraseñas* incluye un apéndice con información orientativa sobre las partes de cada solución relevantes para organizaciones grandes que desean implementar una solución de WLAN basada en contraseñas.

Selección de WPA o WEP dinámica

En combinación con la autenticación segura y la actualización de claves dinámicas que ofrecen 802.1X y EAP, la protección de datos de WEP proporciona un nivel de seguridad que resulta más que apropiado para la mayoría de las organizaciones. Sin embargo, el estándar WPA mejora esta situación y proporciona niveles de seguridad aún mayores.

Las diferencias entre el uso de WPA y una WEP dinámica en cualquiera de las soluciones son mínimas y la migración de un entorno de WEP dinámica a un entorno de WPA es muy simple. Los cambios principales que conlleva la migración son los siguientes:

- si el hardware no es compatible con WPAit, deberá obtener e implementar actualizaciones de firmware para su hardware de red (puntos de acceso y adaptadores de red inalámbricos). Las actualizaciones de firmware para los adaptadores suelen incluirse en las actualizaciones de controladores de red.
- deberá activar WPA en los puntos de acceso inalámbricos.
- deberá cambiar la configuración de clientes WLAN para el uso de WPA en lugar de seguridad de WEP.
- debería incrementar los tiempos de espera para el cierre de la sesión en la directiva de acceso remoto del servicio de autenticación de Internet (IAS, Internet Authentication Service), que se utiliza para exigir la actualización de claves WEP y reducir la carga en el servidor IAS.

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

De ser posible, WPA debería ser su primera elección. Sin embargo, compruebe que las cuestiones siguientes no crearán problemas a la hora de usar WPA:

- es posible que el hardware de la red no sea compatible con WPA (esto no suele ocurrir con dispositivos nuevos pero quizás tenga instalada una amplia base de componentes de hardware anteriores a WPA).
- la compatibilidad con la configuración controlada por GPO se hará disponible en la próxima actualización de Windows Server 2003. Otras versiones no disponen de la compatibilidad y, en equipos con Windows XP, tendrá que llevar a cabo la configuración de WPA manualmente.
- quizás no todos los clientes en su entorno sean compatibles con WPA; por ejemplo, Windows 2000 (y las versiones anteriores) y Pocket PC no ofrecen compatibilidad integrada para WPA.

Si decide que aún no está preparado para implementar WPA, debería utilizar una solución de WEP dinámica y considerar la migración a WPA en cuanto las circunstancias lo permitan.

Principio de la página

Resumen

Este capítulo proporciona información que puede utilizar para definir una estrategia de seguridad de LAN inalámbrica para su organización. La primera parte del capítulo se ocupaba de las ventajas comerciales derivadas del uso de redes inalámbricas, así como de las amenazas de seguridad a que deben hacer frente las LAN con un nivel bajo de protección. En la sección central del capítulo examinábamos los recursos utilizados por la seguridad de LAN inalámbrica basada en el protocolo 802.1X, EAP y la protección de datos segura para mitigar estas amenazas. También consideramos los méritos relativos de alternativas como VPN, IPsec y WEP estática. La última parte del capítulo incluía información orientativa sobre cómo determinar cuál de las opciones

de seguridad de WLAN es la mejor para su organización y cuál de las dos soluciones de seguridad de WLAN de Microsoft es la más apropiada.

Principio de la página

Referencias

A continuación encontrará referencias a información complementaria importante y materiales de apoyo relevantes a este capítulo.

- La solución de Microsoft *Seguridad en LAN inalámbricas con PEAP y contraseñas* está disponible en http://go.microsoft.com/fwlink/?LinkId=23459.
- Si desea información técnica detallada sobre IEEE 802.11 y tecnologías relacionadas, consulte la sección "802.11 Wireless Technical Reference" de la guía de referencia técnica de Windows Server 2003 disponible en http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs /techref/w2k3tr_wir_intro.mspx.
- Para obtener más información sobre 802.11, consulte la página Web sobre 802.11 del boletín de estándares del IEEE 802.11 en http://www.ieee802.org/11/.
- Si desea información adicional sobre el control de acceso de red basado en el puerto 802.1X, consulte la página 802.1x - Port Based Network Access Control en www.ieee802.org/1/pages/802.1x.html.
- Para obtener más información sobre el estándar EAP, consulte el RFC 2284, en http://www.ietf.org/rfc/rfc2284.txt?number=2284.
- Si desea consultar más información acerca del estándar WPA de la Wi-Fi Alliance, vea la descripción general de la Wi-Fi Alliance en www.wi-fialliance.org/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf.
- Para obtener más información sobre redes inalámbricas, consulte la página Wi-Fi del sitio Web de Microsoft Windows Server System en http://www.microsoft.com/wifi.
- Si desea consultar una descripción detallada de PEAP y los resultados de su comparación con LEAP (además de EAP-TLS y EAP-MD5), vea el artículo "The Advantages of Protected Extensible Authentication Protocol (PEAP): A Standard Approach to User Authentication for IEEE 802.11 Wireless Network" en http://www.microsoft.com/windowsserver2003/techinfo/overview/peap.mspx.
- Para información sobre la restricción de riesgos de seguridad con LAN inalámbricas y la protección de información corporativa, consulte el artículo del grupo META "How Do I Limit My Exposure Against the Wireless LAN Security Threat? The New Realities of Protecting Corporate Information", en www.metagroup.com/cgi-bin/inetcgi/jsp/displayArticle.do?oid=35725.

Principio de la página