Latinoamérica

Microsoft TechNet

Seguridad en LAN inalámbricas con PEAP y contraseñas

Capítulo 2: Planeamiento de la implementación de seguridad en LAN inalámbricas

Actualizado: abril 3, aaaa

Ver todos los temas de guía de seguridad

En esta página

Información general

El objetivo de este capítulo, que trata las pautas generales de diseño de la solución de red de área local inalámbrica (WLAN) segura, reside en describir minuciosamente el diseño de la solución y las razones para hacerlo de tal forma. Asimismo, proporciona toda la información precisa para adaptar el diseño a las necesidades particulares de la organización.

El capítulo comienza con una descripción del funcionamiento de 802.1X y del protocolo de autenticación extensible (PEAP) para proteger el acceso a la red. A continuación, se especifica la organización de destino de la solución, al tiempo que se explican algunos de los requisitos clave.

A mediados del capítulo se describe el diseño de la solución de WLAN, y así, aspectos como el diseño de la red; la situación del servidor del servicio de autenticación de Internet (IAS); la selección del hardware y del software; la obtención de certificados y la configuración del cliente. Del mismo modo, se indica cómo migrar de una WLAN sin protección a 802.1X y PEAP.

Las secciones que ponen fin al capítulo se centran en las variaciones que pueden darse en el diseño básico de la solución. El aspecto más importante de estas variaciones de diseño (que se trata en profundidad) es la forma en que la solución se escala para que pueda usarse en organizaciones más grandes. Otras opciones de diseño que se contemplan son:

- Reutilización de la infraestructura de IAS para la seguridad de LAN con cable.
- Utilización de IAS para la autenticación de acceso remoto.
- Implementación de WLAN en entornos SOHO.

Principio de la 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

Requisitos previos del capítulo

Parte del planeamiento de la implementación de la WLAN segura consiste en garantizar que la organización posea las habilidades necesarias y que, asimismo, se implique a las personas adecuadas para que tomen las decisiones pertinentes relativas a la implementación.

Si desea sacar el máximo partido del capítulo, sería conveniente que se familiarizara con los siguientes temas:

- Conceptos relacionados con la red, en concreto LAN inalámbricas.
- Microsoft® 2000 Windows® o Windows Server™ 2003.
- Conceptos del servicio de directorio Microsoft Active Directory®, incluidos los dominios y bosques de Active Directory, las herramientas de administración, el uso de la directiva de grupo y la manipulación de usuarios, grupos y otros objetos de Active Directory.
- Conceptos de Servicios de Certificate Server e infraestructura de claves públicas.
- Conceptos generales de seguridad como la autenticación, la autorización y el cifrado.
- Características de seguridad de Windows como usuarios, grupos, auditorías y listas de control de acceso.
- Aplicación de la configuración de seguridad mediante la directiva de grupo.

  Nota: si bien esta solución puede implementarse sin poseer un amplio conocimiento técnico, sería conveniente tener una certificación Microsoft Certified Systems Engineer (MSCE) o bien, conocimiento y experiencia equivalentes.

Principio de la página

Modo de funcionamiento de la seguridad de LAN inalámbrica

En el documento de introducción ("Elección de una estrategia para la seguridad en LAN inalámbricas") se han tratado con detenimiento algunos de los métodos para proteger las WLAN, con especial atención al uso de la autenticación segura para WLAN a través de 802.1X y del cifrado del tráfico de red mediante la privacidad equivalente por cable (WEP) dinámica o el acceso protegido Wi-Fi (WPA). A continuación se señalan los puntos clave relacionados con este tema:

- El esquema de seguridad de WLAN 802.11 original (conocido como WEP), contiene graves deficiencias de seguridad que posibilitan que un atacante descubra la clave de red para poder adentrarse en ella. Este esquema también se conoce como "WEP estática", debido a que emplea un acceso a red fijo y una clave de cifrado que todos los miembros de la WLAN comparten.
- El uso de IEEE 802.1X proporciona un mecanismo de control de acceso seguro para la WLAN que ha de asociarse al mismo tiempo con un método de protocolo de autenticación extensible (EAP). La elección de este método de EAP define el tipo de credenciales que pueden usarse a la hora de autenticar usuarios y equipos en la WLAN.
- Microsoft admite y recomienda el uso, por un lado, de PEAP con MS-CHAP v2 en el caso de la autenticación de contraseñas y, por otro, de EAP-TLS para la autenticación de certificados.
- PEAP constituye un medio de protección de otro método de EAP (como pueda ser MS-CHAP v2) en el canal de seguridad. De este modo, PEAP se convierte en un elemento esencial para evitar ataques a métodos de EAP basados en contraseñas.
- Una buena protección de datos del tráfico de WLAN puede conseguirse por medio tanto de una WEP dinámica como de una WPA. Las claves de cifrado maestras para la protección de datos se generan como parte del proceso de autenticación 802.1X (aunque la WEP dinámica y WPA emplean estas claves de manera distinta).
- La distinción entre WEP estática y WEP dinámica es crucial, ya que ésta última emplea los mismos algoritmos de cifrado que la WEP estática, si bien actualiza las claves de cifrado de forma constante para acabar con ataques conocidos a la WEP estática. La WEP dinámica sólo hace referencia al mecanismo de protección de

los datos de la red, en tanto que la autenticación de red se controla de forma separada mediante 802.1X.

Funcionamiento de 802.1X con PEAP y contraseñas

Microsoft admite el uso de PEAP con MS-CHAP v2 para la autenticación de la WLAN basada en contraseñas. La figura 2.2 ilustra el modo en que 802.1X con PEAP y MS-CHAP v2 funciona.

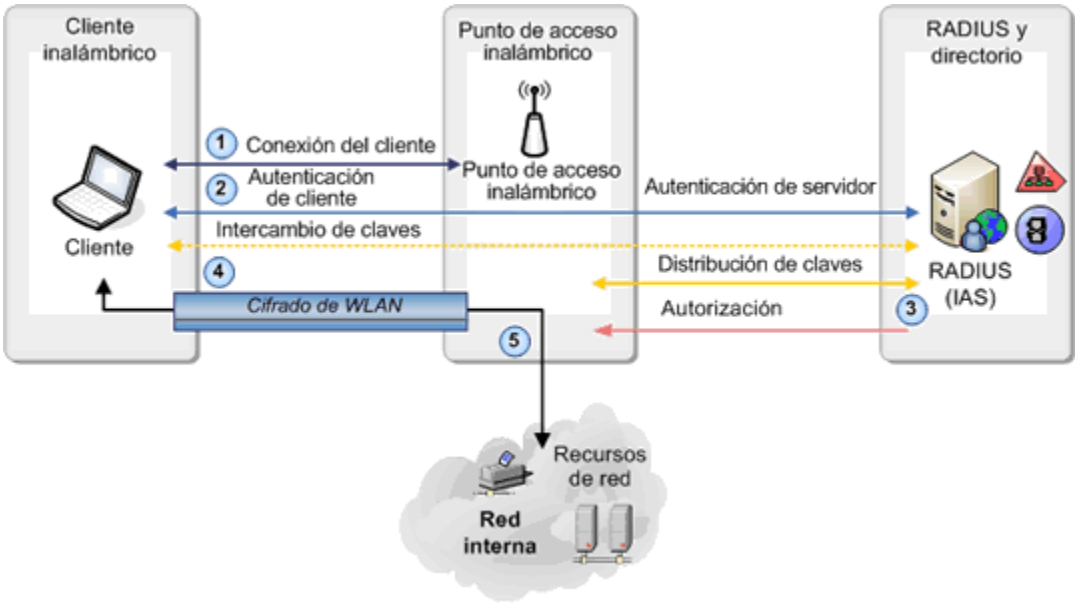

Figura 2.1. Autenticación 802.1X y PEAP para la LAN inalámbrica
Vista de imagen a pantalla completa

La figura muestra los siguientes cuatro componentes principales:

- **Cliente inalámbrico:** se trata de un equipo o dispositivo que ejecuta una aplicación que requiere acceso a los recursos de red. El propietario de las credenciales que se usan para autenticar al cliente en la red puede ser tanto un usuario como un equipo. El cliente debe tener un adaptador de red WLAN que sea compatible con 802.1X y la WEP dinámica o con el cifrado de WPA. Este cliente, además, es conocido como estación (STA) en una gran cantidad de documentos sobre estándares de red.

  Antes de que el cliente pueda tener acceso a la WLAN, deberá ponerse de acuerdo con el servicio de autenticación (el servidor RADIUS y el directorio) en una serie de credenciales mediante una operación fuera de banda. En tal caso, las cuentas de dominio del usuario y del equipo se crean antes de que se produzca la conexión a WLAN. El cliente sabe la contraseña que le corresponde, mientras que el controlador de dominio (el directorio) puede comprobarla. Asimismo, el cliente ha de preconfigurarse con los valores de configuración de WLAN adecuados, que engloban el nombre WLAN y el método de autenticación que ha de utilizarse.

  Nota: en un sentido riguroso, sólo es preciso acordar (ya sea el usuario o el equipo) una serie de credenciales fuera de banda. Así, puede conectarse a la WLAN utilizando las credenciales de usuario para, a continuación, unir el equipo al dominio; no obstante, en esta solución se da por hecho que las cuentas de usuario y de equipo existían previamente al acceso a la WLAN.

- **Punto de acceso inalámbrico:** el punto de acceso inalámbrico tiene como función el control del acceso a la WLAN y, al mismo tiempo, la unión de la conexión del cliente a la LAN interna. Debe ser compatible con 802.1X y la WEP dinámica o con el cifrado de WPA. En términos de conexión a red estándar, los puntos de acceso cumplen la función del Servicio de acceso a la red (NAS).

  Asimismo, el punto de acceso inalámbrico y el servidor RADIUS comparten un secreto que les permite identificarse mutuamente sin riesgo alguno.

- **El servidor RADIUS y el directorio:** el servidor RADIUS utiliza el directorio para comprobar las

credenciales de los clientes WLAN, al tiempo que toma decisiones relativas a la autorización en función de una directiva de acceso a red. También puede recopilar información de responsabilidad y de auditoría sobre el acceso de los clientes a la red. Esto se conoce como servicio de autenticación (AS) en términos de estándares de red.

- **La red interna:** se trata de una red segura a la que la aplicación cliente inalámbrica debe obtener acceso.

Los siguientes pasos indican el modo en que el cliente realiza una solicitud y recibe permiso para tener acceso a la WLAN (y, en consecuencia, a la red interna). La numeración de estos pasos se corresponde con los números de la figura 2.1.

1. Cuando el equipo cliente se encuentra dentro del alcance del punto de acceso inalámbrico, intenta conectarse a la WLAN que se encuentre activa en este punto y que el Identificador del conjunto de servicios (SSID) haya identificado. El SSID es el nombre de la WLAN que el cliente utiliza para identificar la configuración correcta y el tipo de credencial para esta WLAN en particular.

2. El punto de acceso inalámbrico se configura con el propósito de permitir sólo conexiones seguras (autenticadas mediante 802.1X). Así, cuando el cliente intente conectarse al punto, éste le desafiará. A continuación, el punto de acceso configura un canal restringido que permite al cliente comunicarse únicamente con el servidor RADIUS (se bloquea el acceso al resto de la red). Por su parte, el servidor RADIUS sólo admitirá una conexión proveniente de un punto de acceso inalámbrico de confianza; es decir, una conexión que se haya configurado como un cliente RADIUS en el servidor IAS y que, por lo tanto, proporcione el secreto compartido para tal cliente RADIUS.

   El cliente intenta autenticarse en el servidor RADIUS a través del canal restringido por medio de 802.1X. Dentro de la negociación PEAP, el cliente establece una sesión de seguridad de la capa de transporte (TLS) con el servidor RADIUS. Una sesión TLS se utiliza como parte de los servidores PEAP con fines diversos:

   - Permite que el cliente autentique el servidor RADIUS; esto significa que el cliente sólo establecerá la sesión con un servidor que cuente con un certificado en el que confíe el cliente.
   - Protege el protocolo de autenticación MS-CHAP v2 frente al rastreo de paquetes.
   - La negociación de la sesión TLS genera una clave que el cliente y el servidor RADIUS pueden utilizar a fin de establecer claves maestras comunes (que, a su vez, se usan para generar aquellas claves que van a emplearse para cifrar el tráfico de WLAN).

   Bajo la protección del canal de PEAP, el cliente se autentica en el servidor RADIUS utilizando el protocolo EAP MS-CHAP v2. En el transcurso de este intercambio, el tráfico dentro del túnel de TLS nunca se expone al punto de acceso inalámbrico: sólo el cliente y el servidor RADIUS pueden verlo.

3. El servidor RADIUS comprueba las credenciales del cliente en relación con el directorio. Si el cliente se autentica correctamente, el servidor RADIUS recabará información con la que decidirá si autoriza al cliente a usar la WLAN. De esta forma, concede o deniega el acceso al cliente de acuerdo con la información del directorio (como la pertenencia a grupos) y también con las restricciones que se definen en la directiva de acceso correspondiente (por ejemplo, las horas del día en que es posible tener acceso a la WLAN). El servidor RADIUS transfiere la responsabilidad de decidir sobre el acceso al punto de acceso.

   Así, si el cliente obtiene acceso, el servidor RADIUS transmitirá la clave maestra del cliente al punto de acceso inalámbrico. Por su parte, el cliente y el punto de acceso comparten ahora material de claves comunes que pueden utilizar para cifrar y descifrar el tráfico de WLAN que fluye entre ellos.

   Cuando se utiliza una WEP dinámica para cifrar el tráfico, las claves maestras se utilizan directamente como clave de cifrado. Estas claves han de modificarse cada cierto tiempo para frustrar ataques de recuperación de claves WEP. El servidor RADIUS lleva esto a cabo obligando al cliente de forma periódica a volver a autenticarse y generar un conjunto de claves nuevo.

   En caso de que la comunicación se proteja mediante WPA, el material de clave maestra se usará para

crear claves de cifrado de datos, que se modifican para cada paquete que se transmita. Con WPA no es necesario forzar la reautenticación para garantizar la seguridad de la clave.

4. A continuación, el punto de acceso une la conexión de la WLAN del cliente a la LAN interna, lo que posibilita que el cliente se comunique con total libertad con los sistemas de la red interna. Así, ahora el tráfico que fluye entre el cliente y el punto de acceso está cifrado.

5. En caso de que el cliente necesitara una dirección IP, podría solicitar el alquiler de un protocolo de configuración dinámica de host (DHCP) de un servidor de la LAN. Una vez se haya asignado la dirección IP, el cliente podrá empezar a comunicarse con normalidad con los restantes sistemas de la red.

Autenticación del equipo y del usuario en la WLAN

El proceso que se acaba de describir señala el modo en que un cliente (sea usuario o equipo) se conecta con éxito a la WLAN. Windows XP autentica tanto al usuario como al equipo de manera independiente. Cuando un equipo se inicia por primera vez, utiliza una cuenta de dominio y una contraseña para autenticarse en la WLAN. La autorización del equipo a la WLAN tiene lugar exactamente tal y como se ha especificado en la sección anterior. Aun cuando ningún usuario haya iniciado sesión, el equipo se podrá administrar si se conecta a la WLAN a través de sus propias credenciales. Por ejemplo, se podrá aplicar una configuración de directiva de grupo en el equipo, así como distribuir software y revisiones.

Cuando un usuario inicia sesión en el equipo, este proceso de autenticación y autorización se repite, pero, en este caso, con el nombre de usuario y la contraseña del usuario. La sesión de un usuario sustituye la sesión de WLAN del equipo, de modo que no hay dos sesiones activas al mismo tiempo. Además, esto evita que un usuario no autorizado utilice un equipo autorizado para obtener acceso a la WLAN.

Nota: Windows XP permite anular este comportamiento y especificar que sólo sirvan las credenciales del equipo o de un usuario. Estas configuraciones no son recomendables: la primera, porque permite que los usuarios se conecten a la WLAN sin autorización y la segunda, porque impide que el equipo pueda conectarse a la WLAN si no lo hace antes un usuario (lo que interferiría en varias de las funciones de administración de los equipos).

Principio de la página

Perfil de la organización de destino

El diseño de esta solución está pensado para pequeñas empresas de entre 100 y 200 personas. Si bien la organización es ficticia, las características y requisitos son producto de una intensa investigación en el mundo real. Estos requisitos del mundo real han servido para modelar el estilo y el alcance de la guía, así como las preferencias de diseño.

Es importante comprender que esta solución no está limitada exclusivamente a organizaciones de este tamaño, dado que la sencillez del diseño y la escalabilidad de los componentes utilizados hacen de ella una solución de WLAN basada en PEAP adecuada para organizaciones mucho más pequeñas y mucho más grandes (con miles de usuarios). Si comprende las características de la organización de destino, sabrá con mayor seguridad las características del diseño y, en consecuencia, podrá adaptarlas a la organización.

El uso de esta solución en organizaciones de mayor envergadura se detalla en la sección "Escalabilidad para organizaciones más grandes" de este capítulo. En cuanto a aquellas organizaciones realmente pequeñas, todos los componentes pueden instalarse en un único servidor.

Diseño de la organización

La siguiente figura muestra el diseño físico y de tecnología de la información (TI) de la organización.

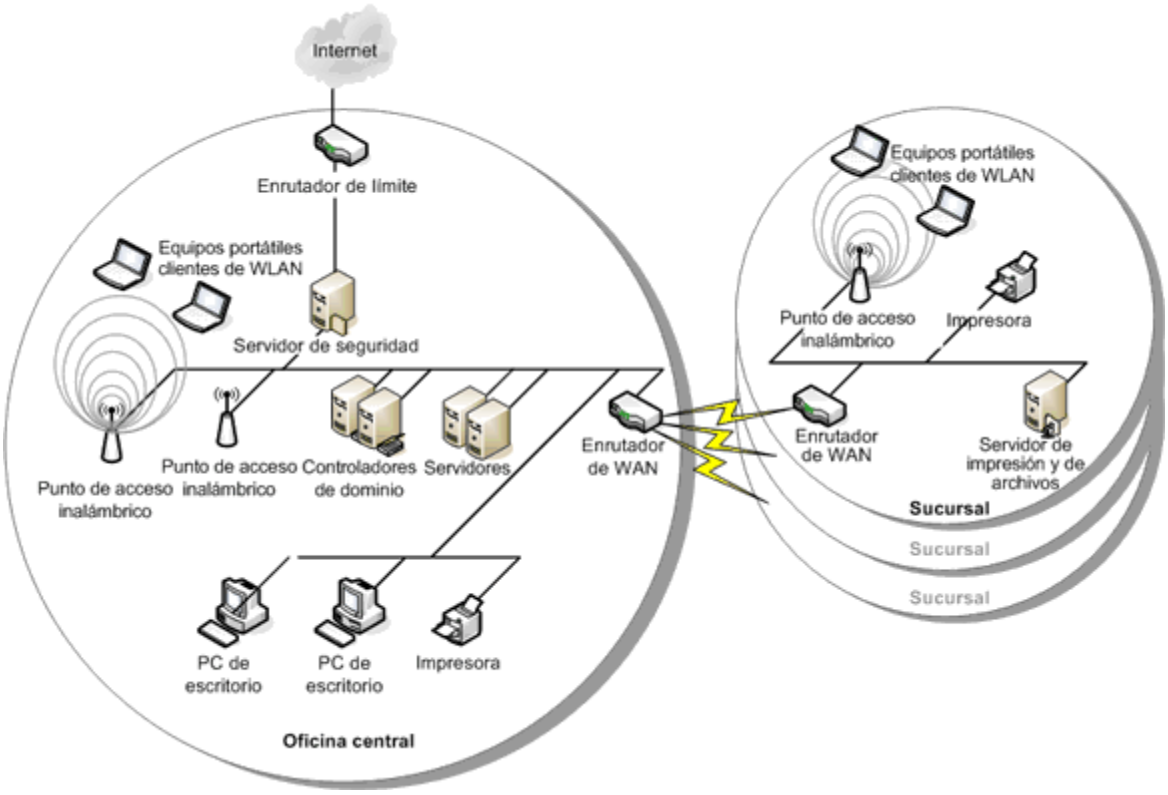

Figura 2.2. Diseño físico y de TI de la organización de destino
Vista de imagen a pantalla completa

Hay una gran oficina central donde se encuentran la mayoría de los sistemas de TI y gran parte de los usuarios. Todos los controladores de dominio de Active Directory se hallan aquí. La conexión a Internet en esta oficina se realiza a través de un servidor de seguridad. Existe un número de clientes WLAN y puntos de acceso inalámbrico conectados a la red interna.

También hay una o varias oficinas remotas con muy pocos servicios de TI locales aparte de la conexión de red con la oficina central. El número de clientes (todos inalámbricos, posiblemente) es pequeño en esta oficina, que con frecuencia recibe visitantes de la oficina central que disponen de sus propios clientes WLAN para que puedan volver a conectarse a sus aplicaciones y datos en la oficina central.

La conectividad de la red de área extensa (WAN) entre oficinas se suministra bien mediante líneas privadas (así, una T1 a 1,5 Mbps), bien mediante conexiones DSL y un vínculo entre enrutadores de una red privada virtual (VPN) a través de Internet. Normalmente, la conexión WAN es proclive a dar errores.

Nota: por lo general, cuando la conexión WAN entre oficinas se obtiene de una conexión VPN a través de Internet, cada oficina tiene un servidor de seguridad que la protege de las amenazas de Internet. En relación con la WLAN, el tema de la presencia de un servidor de seguridad no procede, de manera que se ha omitido en aras de una mayor claridad.

Entorno de TI

Active Directory, que en esta organización consiste en un solo bosque de dominios con al menos dos controladores de dominio, autentica usuarios en el dominio y proporciona servicios de directorio y autenticación a varias aplicaciones, como Microsoft Exchange Server y Outlook® para el correo electrónico. Los controladores de dominio han pasado recientemente de Windows 2000 Server a Windows Server 2003, versión Standard Edition. Para algunas aplicaciones heredadas, estos controladores de dominio ejecutan también otro tipo de servicios, como el Sistema de nombres de dominio (DNS), DHCP y el Servicio de nombres de Internet de Windows (WINS).

Los sistemas de TI son en su mayoría tecnologías Microsoft, con Windows XP en los equipos cliente y Windows

Server 2003 en los sistemas servidor. Asimismo, existe un determinado número de servidores que ejecutan Windows 2000, algo que la compañía planea mejorar en tanto la prueba y la compatibilidad de las aplicaciones lo permitan. La organización empieza a invertir en sistemas móviles como Windows XP, Tablet Edition y Pocket PC 2003, en especial para el personal de ventas, de distribución y de almacén.

Entre las aplicaciones de servidor clave se incluyen Microsoft Exchange Server, SQL Server (que ejecuta varias aplicaciones de línea de negocios), Servicios de Internet Information Server (IIS) y Windows SharePoint™ Team Services.

Las aplicaciones se implementan en equipos cliente por medio de la directiva de grupo de Active Directory. En cuanto a las revisiones del sistema operativo, se implementan por medio de Microsoft Software Update Service (SUS) y el servicio Windows AutoUpdate.

El seguimiento del sistema se realiza directamente en los sistemas servidor mediante la revisión diaria de los registros de sucesos, los registros de rendimiento y los registros de aplicaciones. Las alertas importantes relativas al software y al hardware se envían al administrador de TI por medio de correos electrónicos y alertas en las consolas del sistema.

La organización cuenta con dos personas responsables de TI a tiempo completo que se encargan del planeamiento de TI, la entrega de servicios y la asistencia diaria. Tanto el administrador de TI como el ingeniero asistente de TI poseen las certificaciones MCSE más recientes y años de experiencia en este ámbito.

Principio de la página

Criterios de diseño

La organización descrita en la sección anterior generalmente cumplirá con los siguientes tipos de criterios para una solución de WLAN. Estos criterios se han ampliado a fin de cubrir una amplia categoría de organizaciones. En el diseño presentado en el resto del capítulo se usan estos criterios de forma explícita.

Tabla 2.1. Criterios de diseño de la solución de WLAN

Factor de diseño	Criterios
Requisitos de seguridad	-Una autenticación y autorización sólidas de los clientes inalámbricos. -Un control de acceso sólido que permita el acceso de red a clientes autorizados y lo deniegue a clientes no autorizados. -Un cifrado eficaz (128 bits) del tráfico de red inalámbrica. -Una administración segura de las claves de cifrado.
Escalabilidad: número mínimo/máximo de usuarios admitidos	De 25 a 5000 usuarios de WLAN (o más) Consulte la tabla 2.2 para obtener información sobre las cargas de autenticación para distintos tamaños de WLAN.
Escalabilidad: número de sitios admitidos	**Básico:** un solo sitio de dimensiones considerables con controladores de dominio y servicios de TI locales; uno o más sitios pequeños sin controladores de dominio. El mínimo de usuarios que se precisa es 25. **Superior:** un solo sitio central con varios controladores de dominio; oficinas grandes con un solo controlador de dominio y/o conectividad WAN resistente a la oficina central; varias oficinas pequeñas sin controlador de dominio, con una WAN probablemente poco resistente. El número máximo de usuarios permitido es 5000. Para el uso en organizaciones grandes, consulte el apéndice A, "Uso

	de PEAP en la empresa".
Requisitos de disponibilidad	Las oficinas de mayores dimensiones que utilicen varios puntos de acceso inalámbrico, IAS o controladores de dominio (inalámbricos) contarán con una WLAN resistente a un error de componente individual. Por el contrario, las WLAN de las oficinas pequeñas son vulnerables y con tendencia a producir errores, a menos que se instale una conectividad redundante.
Compatibilidad con plataformas	**Plataformas del servidor:** Windows Server 2003, versión Standard Edition o Enterprise Edition (para la instalación de IAS y de la entidad emisora de certificados). Standard Edition admite un máximo de 50 puntos de acceso inalámbrico (clientes RADIUS) por servidor. **Plataformas cliente:** Windows XP Professional o Tablet Edition; Pocket PC 2003.
Extensibilidad (reutilización de los componentes de la solución para otras aplicaciones)	La misma infraestructura de autenticación puede admitir otras aplicaciones de acceso de red (VPN de acceso remoto, acceso a red por cable 802.1X y autenticación del servidor de seguridad).
Requisitos de la organización de TI	La instalación y la administración de la solución debe estar en manos de un experto de TI que posea la certificación MSCE más reciente o conocimiento equiparable, así como de 2 a 3 años de experiencia en el sector de TI.
Requisitos de capacidad de administración	La solución necesitará un mínimo de administración para mantener un funcionamiento sin problemas. Las alertas se envían por correo electrónico o a través del registro de sucesos de Windows (o bien se modifican para desencadenar otros tipos de alerta). El componente IAS se puede supervisar mediante la solución de supervisión de Windows (a través de registros de sucesos y contadores de rendimiento), mediante el registro de RADIUS y mediante el sistema de administración Protocolo simple de administración de redes (SNMP).
Cumplimiento de las normas	La solución admite las siguientes normas: -Normas de red (a, b o g) IEEE 802.11. -Autenticación IEEE 802.1X con PEAP y MS-CHAP v2, que puede usarse con otros métodos de EAP como el EAP-TLS basado en certificados y PEAP-EAP-TLS. -WEP con clave dinámica y protección WPA para WLAN. Capacidades y normas futuras (por ejemplo, 802.11i). -Compatibilidad con RADIUS para RFC 2865 y 2866.

La siguiente tabla recoge una indicación de los requisitos de autenticación WLAN para diversos tamaños de organización. La columna "Nuevas autenticaciones por segundo" forma parte de la carga fija; en ella, se supone una media de cuatro autenticaciones nuevas por día y usuario, dado que los usuarios se desplazan por los

puntos de acceso inalámbrico. La columna "Nuevas autenticaciones por segundo en hora máxima" señala el tipo de carga que se espera cuando todos los usuarios se autentican en un período de 30 minutos (por ejemplo, al inicio del día). La columna "Reautenticaciones por segundo" contempla el número de reautenticaciones regulares que obligan a una renovación de las claves WEP dinámicas.

Tabla 2.2. Requisitos de autenticación de WLAN

Número de usuarios de WLAN	Nuevas autenticaciones por segundo	Nuevas autenticaciones por segundo en hora máxima	Reautenticaciones por segundo
100	> 0,1	0,1	0,1
1000	0,1	0,6	1,1
10000	1,4	5,6	11,1

Más adelante en este capítulo se hace referencia a estas cifras, en concreto, al tratar el tema de las dimensiones del servidor IAS.

Principio de la página

Arquitectura de WLAN

Esta sección se centra en la arquitectura de la solución.

Diseño de la red

La siguiente figura ilustra el diseño de red básico para la oficina central.

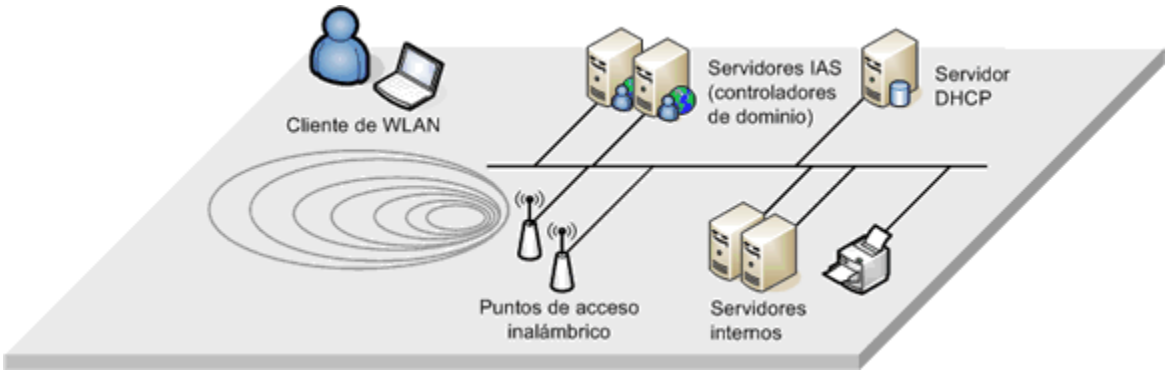

Figura 2.3. Diseño de la red para la oficina central
Vista de imagen a pantalla completa

La figura muestra clientes inalámbricos, dos o más puntos de acceso inalámbrico, dos servidores IAS que se ejecutan en controladores de dominio de Active Directory, un servidor DHCP y otros servidores, clientes y dispositivos conectados a la red. A excepción de los clientes WLAN, todos los elementos se conectan a una sola LAN mediante uno o varios conmutadores de nivel 2. En este sitio se usa una única subred para toda la red interna. Existen conexiones enrutadas (que no aparecen en la figura) a través del servidor de seguridad a Internet y otras oficinas.

Es más probable que las organizaciones de mayores dimensiones tengan un entorno enrutado dentro de un único sitio. Esto no supone diferencia alguna para la infraestructura de autenticación, si bien puede influir en la manera en que los puntos de acceso inalámbrico se conectan con el resto de la red. Para que sea más sencillo que los usuarios se desplacen por los distintos puntos de acceso de un sitio, lo más normal es que se coloquen todos los puntos de acceso inalámbrico y todos los clientes WLAN en la misma subred de IP. Así, los usuarios

podrán moverse por puntos de acceso inalámbrico manteniendo la misma dirección IP. Tratar este tema en mayor profundidad no se corresponde con los objetivos de esta guía. Encontrará más detalles al respecto en el capítulo sobre la implementación de una LAN inalámbrica del *Kit de distribución de Microsoft Windows Server 2003*.

En el diseño de la red, se debe garantizar los siguientes elementos:

- Los puntos de acceso inalámbrico tienen conectividad con los servidores IAS tanto principales como secundarios. Así, en caso de que los puntos de acceso se encuentren en una VLAN/subred distinta de la de los servidores IAS, el tráfico deberá poder enrutarse entre tales subredes.
- Los clientes WLAN deben tener conectividad a los servidores DHCP. Si los servidores no se hallaran en la misma subred, será necesario tener agentes de retransmisión DHCP/BOOTP para reenviar solicitudes DHCP del cliente a un DHCP que posea un ámbito definido para esa subred. Sobra decir que los clientes necesitarán conectividad a los servicios de red normales, como los controladores de dominio, servidores de archivos, etc.

Selección del hardware de la red inalámbrica

Debe garantizar que los puntos de acceso inalámbrico y los adaptadores de red inalámbricos sean compatibles con los siguientes elementos:

- Cifrado de WEP de 128 bits (si se usa una WEP dinámica), cifrado de TKIP (RC4) o cifrado de AES (se usa WPA).
- Autenticación 802.1X.
- Actualización de la clave dinámica (sólo cifrado de WEP).
- Compatibilidad con WPA (aun cuando se use una WEP dinámica, debería tener un compromiso firme por parte del proveedor para que suministre actualizaciones de firmware con las que poder admitir WPA).

Debe tener suficientes puntos de acceso inalámbrico para proporcionar cobertura para clientes WLAN a través de ubicaciones físicas con las que ha de ser compatible. Asimismo, debe planear la colocación de esos puntos de acceso inalámbrico para que, en caso de que se produzca un error en uno de ellos, exista una cobertura de copia de seguridad adecuada en todas las ubicaciones. El tema de la colocación de los puntos de acceso inalámbrico se trata en mayor profundidad en el capítulo sobre la implementación de una LAN inalámbrica del *Kit de distribución de Microsoft Windows Server 2003*, que se incluye igualmente en la sección "Referencias" al final de este capítulo. También es aconsejable que lea el artículo "Recommendations for IEEE 802.11 Access Points", al que se hace referencia al final de este capítulo.

Colocación del servidor IAS

El objetivo de la colocación del servidor IAS reside en obtener un servicio de WLAN resistente con costes de implementación y administración moderados. Un servicio de WLAN que ofrece resistencia a un error de componente individual presenta las siguientes características:

- Todas las áreas físicas que precisen cobertura de WLAN deben tener un mínimo de dos puntos de acceso inalámbrico dentro de su alcance.
- Cada punto de acceso inalámbrico debe poder comunicarse con un servidor IAS de copia de seguridad en caso de que el principal no funcione o que la conexión de red a este servidor no pueda establecerse.
- Los servicios de los que tanto IAS como los clientes WLAN dependen (por ejemplo, Active Directory, DHCP y DNS) deben ofrecer la misma resistencia.

La segunda característica es la más importante a la hora de planear la colocación del servidor IAS. En esta solución, IAS se encuentra en controladores de dominio ya existentes, con lo que se obtiene la mejor configuración de rendimiento con un coste de implementación y administración relativamente bajo. Como recomendación general para cualquier organización (sea del tamaño que sea), IAS se debe implementar en todos los sitios que tengan un controlador de dominio (si bien no tiene por qué instalarse en cada uno de estos controladores).

La siguiente figura recoge la colocación de servidores IAS en la organización. En este caso, IAS se implementa

en dos controladores de dominio en la oficina central. La entidad emisora de certificados de la red (consulte la sección "Obtención de certificados para servidores IAS" más adelante en este capítulo) también se instala en uno de estos controladores de dominio. Todos los puntos de acceso inalámbrico en la oficina central se configuran con el fin de utilizar estos servidores IAS.

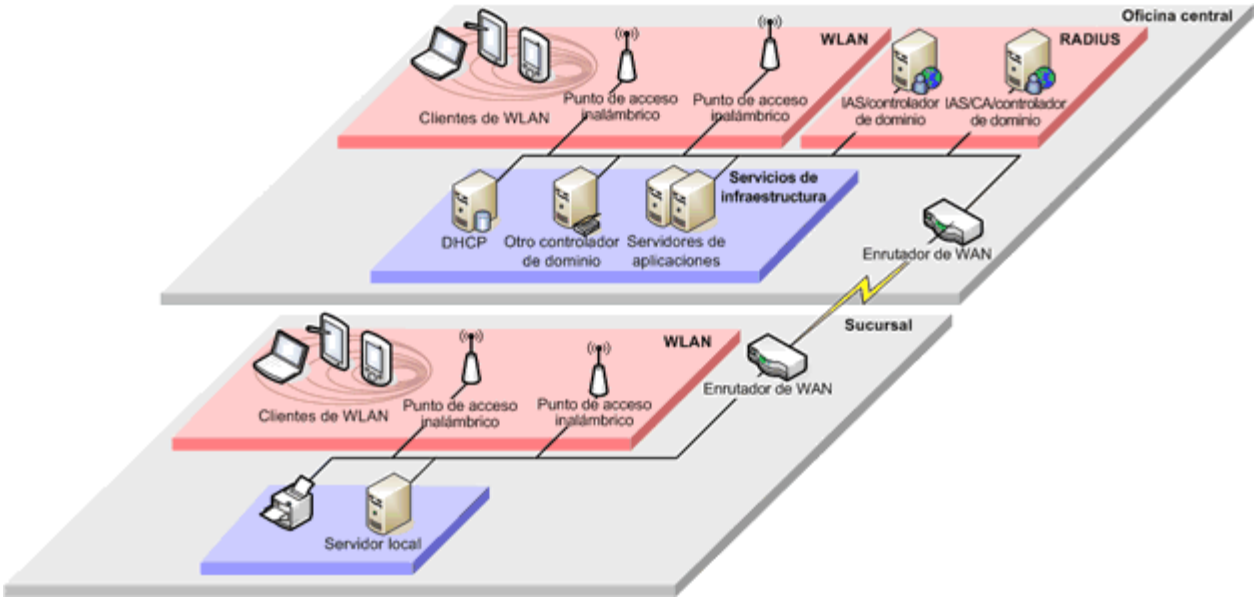

Figura 2.4. Infraestructura de la oficina central y de la sucursal
Vista de imagen a pantalla completa

La organización tiene una pequeña sucursal sin controlador de dominio local. Los puntos de acceso inalámbrico en este sitio emplean los dos servidores IAS de la oficina central para todas las solicitudes de autenticación; es decir, los usuarios no podrán autenticarse en la WLAN si se produce un error en la conexión WAN de la oficina central. Esto constituye un riesgo que muchas organizaciones no pueden permitirse.

Para resolver esto, debería instalar una conectividad WAN redundante, o bien instalar un IAS y un controlador de dominio locales. Si bien puede considerarse como un coste inaceptable para este tipo de oficina, un error en WAN podría provocar igualmente que muchos otros servicios de red no funcionaran adecuadamente (por ejemplo, los servidores de archivos locales) sin acceso a un controlador de dominio. En consecuencia, si soluciona esto, la confiabilidad tanto de estos servicios como de la WLAN local mejorará considerablemente. La implementación de controladores de dominio en sucursales se detalla en la sección "Escalabilidad para organizaciones más grandes" más adelante en este capítulo.

En relación con oficinas pequeñas donde la conectividad WAN es muy poco confiable y donde la implementación de un controlador de dominio no es viable, puede optar por implementar una WLAN independiente. Para obtener más información, lea la sección "Entornos SOHO" más adelante en este capítulo.

Asignación de puntos de acceso a servidores RADIUS

Debe asignar todos los puntos de acceso inalámbrico a servidores IAS. Cada punto de acceso inalámbrico necesita un servidor RADIUS principal y uno secundario, ya que, así, podrá usar el servidor RADIUS secundario en caso de que no pueda ponerse en contacto con el principal o éste no funcione. Esta disposición se muestra en la siguiente figura.

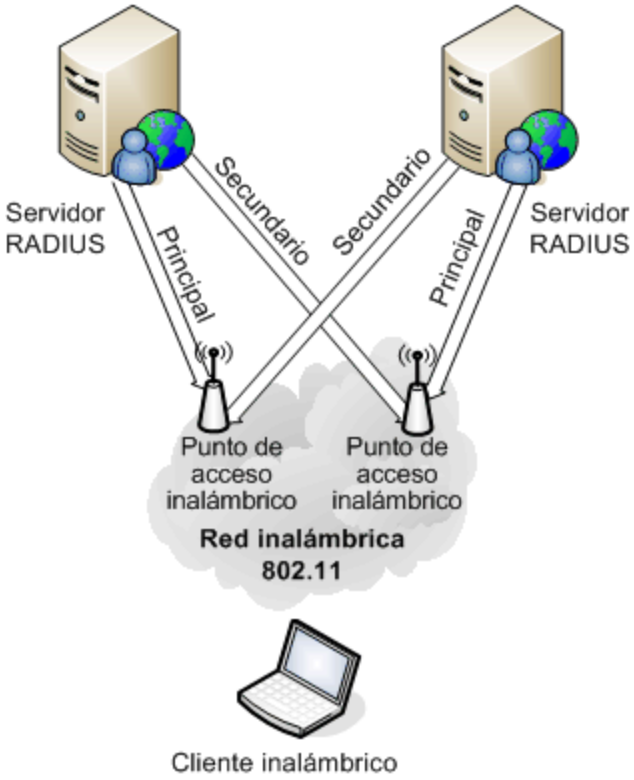

Figura 2.5. Equilibrio del punto de acceso entre los servidores IAS principal y secundario

La figura muestra el modo en que cada uno de los puntos de acceso inalámbrico se configura con un servidor RADIUS principal y uno secundario distintos. Esto permite el equilibrio de carga entre ambos servidores. Los puntos de acceso inalámbrico en sitios que carecen de un servidor IAS local seguirán la misma pauta, pero usando los servidores IAS de la oficina central como servidores RADIUS principal y secundario.

En el caso de los puntos de acceso inalámbrico en sitios que sólo tienen un servidor IAS local, éste siempre ha de ser el principal, mientras que el de la oficina central (u otra ubicación pertinente donde exista conectividad a un servidor IAS confiable) será el secundario. Esta configuración se ilustra en la figura siguiente.

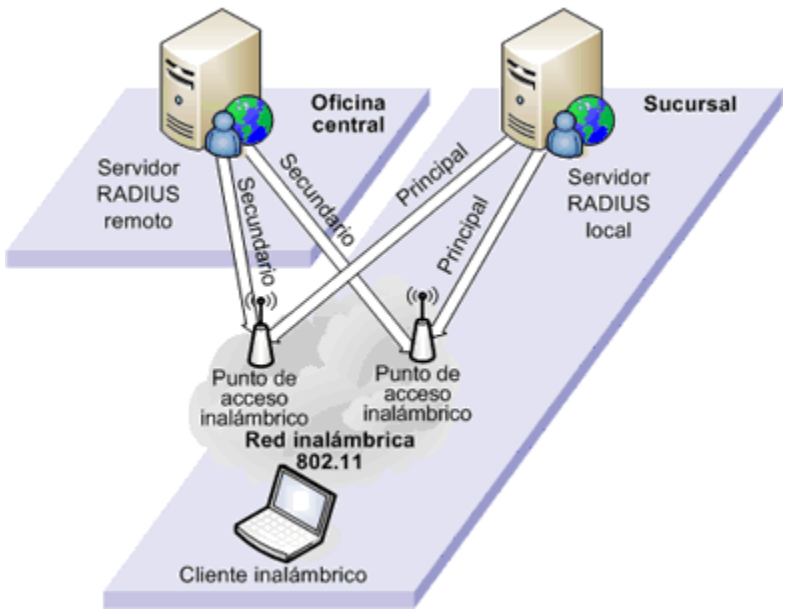

Figura 2.6. Configuración de los puntos de acceso para usar servidores IAS locales y remotos
Vista de imagen a pantalla completa

Si posee una gran cantidad de puntos de acceso, debería documentar minuciosamente la asignación de éstos a servidores IAS. De este modo, podrá usar este registro para garantizar que cada punto de acceso tiene asignado un servidor principal y otro secundario y, asimismo, que la carga desde estos puntos presenta un equilibrio uniforme entre los servidores disponibles.

Nota: si el servidor IAS no está disponible, todos los puntos de acceso inalámbrico realizarán una conmutación por error hacia el servidor IAS secundario. No obstante, la mayoría de los puntos de acceso no volverán a usar el principal automáticamente una vez éste vuelva a estar disponible (sólo lo harán en caso de que se produzca un error posterior en el secundario). Esto no supone un problema de importancia cuando los dos servidores IAS se hallan en la misma ubicación, sino que, simplemente, la carga entre los servidores no será uniforme. Ahora bien, si el servidor IAS secundario es remoto, es posible que un error en el servidor principal provoque que todos los puntos de acceso se autentiquen en el servidor secundario a través de un vínculo WAN que no sea óptimo.

En caso de que los puntos de acceso no vuelvan de manera automática al servidor principal designado, es probable que necesite restablecer manualmente los puntos de acceso para que, así, comiencen a usar el servidor IAS local una vez se haya recuperado tras un error. Las condiciones de red transitorias también pueden ser motivo de conmutación por error de los puntos de acceso hacia los servidores RADIUS secundarios, de manera que puede que sea necesario comprobar de forma ocasional los sucesos de solicitud de autenticación en los registros de aplicación de servidores IAS con el fin de detectar cualquier punto de acceso que esté utilizando el IAS inapropiado.

Co-ubicación de IAS con controladores de dominio

En esta solución, IAS se instala en los controladores de dominio existentes. De esta forma, los costes de implementación se mantienen bajos y se consigue una mejora del rendimiento a través del uso de IAS en un servidor miembro independiente. Esta mejora se produce porque el IAS puede comunicarse con Active Directory en el mismo equipo sin que tenga lugar retraso alguno en la red.

No olvide que hay una serie de salvedades relativas a la instalación de IAS en controladores de dominio. Bien es cierto que no tienen por qué condicionar a muchas organizaciones, pero puede que sea interesante tenerlas en consideración antes de proceder:

- No podrá tener una configuración única para todos los controladores de dominio, a menos que opte por instalar IAS en todos ellos.
- No podrá imponer la separación entre la administración de IAS y la administración del dominio. La instalación de IAS en los controladores de dominio significa que los administradores de IAS deben ser miembros también del grupo de administradores de dominio incrustado.
- Una gran carga de las funciones de los controladores de dominio podría afectar de forma negativa al rendimiento de IAS y viceversa. Así, puede que quiera depositarlas en servidores independientes para ejercer un mayor control sobre el rendimiento individual y el funcionamiento de estos servicios.

Requisitos del software y del hardware de IAS

En una organización de destino de entre 100 y 200 usuarios, es bastante improbable que la carga de IAS en los servidores sea motivo de problema en tanto se use la especificación de hardware recomendada para Windows Server 2003. No obstante, en el caso de organizaciones de mayor tamaño, este aspecto ha de tenerse en cuenta si IAS se ejecuta en los controladores de dominio existentes.

La carga en IAS podrá verse afectada por los siguientes aspectos:

- Número de usuarios y dispositivos que requieren autenticación de RADIUS.
- Elección de las opciones de autenticación tales como el tipo de EAP y la frecuencia de reautenticación.

- Si el registro de RADIUS está habilitado.

Puede hacer uso de las cifras que recoge la tabla 2.2 de la sección anterior, "Criterios de diseño", para calcular el número de autenticaciones por segundo que pueden preverse de una población determinada. Debería tenerse en cuenta la carga de estado fija cuando los usuarios se autentican de manera habitual y, al mismo tiempo, la carga del "peor caso" en horas punta. Si se extrapolan las cifras de esta tabla, 200 usuarios generan una carga de estado fija inferior a una autenticación completa cada 50 segundos, así como una reautenticación rápida cada 10 segundos. Se trata de cifras tan insignificantes, que la única relevante es el tiempo que se tarda en autenticar a todos los usuarios tras una interrupción de la actividad, cuando todos los usuarios necesitan volver a conectarse a la WLAN de inmediato. Este momento constituye una hora punta bastante más acusada que el primer inicio de sesión del día, que tiende a prolongarse unos 30 minutos o más.

Las opciones de autenticación tienen un gran efecto en la carga del servidor IAS. Los protocolos como PEAP realizan una operación de clave pública con gran actividad de la CPU durante el primer inicio de sesión, si bien emplean información de sesiones en caché para reautenticaciones posteriores (lo que se conoce como "reconexión rápida"). Si utiliza una WEP dinámica, los clientes se reautenticarán cada 15-60 minutos para generar nuevas claves de cifrado. Sin embargo, en el caso de WPA, deberá forzar la reautenticación con mucha menos frecuencia, normalmente cada 8 horas.

La siguiente tabla refleja el número aproximado de autenticaciones que se producen por segundo en un IAS en un servidor Intel Pentium 4 a 2 GHz que ejecuta Windows Server 2003 con Active Directory en un servidor independiente.

Nota: la información contenida en la tabla, producto de una serie de pruebas que Microsoft Solutions for Security ha realizado, se ofrece sin garantía alguna y sólo se debe utilizar como orientación a la hora de planear la capacidad y no para realizar comparaciones de rendimiento.

Tabla 2.3. Autenticaciones por segundo

Tipo de autenticación	Nuevas autenticaciones	Autenticaciones de reconexión rápida
Autenticaciones PEAP por segundo	36	166
Tiempo de autenticación de 200 usuarios	6 segundos	2 segundos
Tiempo de autenticación de 1000 usuarios	30 segundos	7 segundos

Estas cifras se han calculado con el registro de RADIUS habilitado y con Active Directory ejecutándose en un servidor independiente. Ambos factores reducen el rendimiento de IAS, de manera que esta estimación podría considerarse pesimista.

Tal y como ponen de manifiesto estas cifras, este tipo de servidor permitirá que 200 usuarios de la WLAN se autentiquen en la red en 6 segundos y 1000 usuarios, en 30.

Uso de Windows Server Standard o Enterprise Edition

En esta solución se usa Windows Server 2003, versión Standard Edition, para todos los servidores IAS; así, los costes de las licencias de los servidores se mantienen bajos y, además, podrá realizar implementaciones en servidores ya existentes, sean éstos Standard o Enterprise Edition.

IAS en la versión Standard Edition de Windows Server 2003 está limitada para que cada servidor admita sólo 50 clientes RADIUS y dos grupos de enrutamiento de servidores RADIUS.

Nota: un cliente RADIUS no es lo mismo que un cliente WLAN. Un cliente RADIUS hace referencia a puntos de acceso inalámbrico y también a otros servidores de acceso a la red (como servidores VPN y servidores de seguridad) que emplean los servicios de autenticación de RADIUS.

Un máximo de 50 puntos de acceso por servidor es más que suficiente para las organizaciones de destino de entre 1 y 200 usuarios. En el caso de organizaciones de dimensiones mayores, este límite podría ser

especialmente relevante para las oficinas más grandes o cuando muchas oficinas satélite se conectan a uno o dos servidores IAS de concentrador.

En el supuesto de que haya 15 usuarios por punto de acceso inalámbrico, quiere decir que un solo servidor IAS en Windows Server 2003, versión Standard Edition, podría admitir hasta aproximadamente 750 usuarios. En esta estimación se tiene presente el número total de puntos de acceso que van a usar un servidor como un servidor RADIUS principal o secundario; en consecuencia, dos servidores admiten 50 puntos de acceso y no 100. En caso de que alguno de los servidores IAS deban admitir más de 50 puntos de acceso, necesitará la versión Enterprise Edition de Windows Server 2003. Obviamente, se pueden combinar ambas ediciones o hacerlas coincidir utilizando Windows Server 2003, Enterprise Edition para oficinas más grandes y oficinas con concentrador y Windows Server 2003, Standard Edition para oficinas más pequeñas.

Configuración de IAS

La configuración de IAS puede dividirse en cuatro categorías principales:

- Configuración del servidor IAS
- Configuración del registro de RADIUS
- Directivas de acceso remoto
- Directivas de solicitud de conexión

Estas categorías se describen detalladamente en las siguientes subsecciones. Estas configuraciones se pueden realizar en un solo servidor IAS y copiarlas en el resto, dado que son comunes a todos los servidores IAS que se usan en esta solución. Esta técnica se aplica en el capítulo 5, "Creación de la infraestructura de seguridad de LAN inalámbricas", con el fin de garantizar que la configuración de IAS sea coherente en todos los servidores de la organización.

Asimismo, cada servidor IAS tendrá uno o varios puntos de acceso inalámbrico configurados como clientes RADIUS. El tema de los clientes RADIUS se trata en la sección anterior "Asignación de puntos de acceso a servidores RADIUS". El grupo de clientes RADIUS es generalmente distinto en cada servidor y, por lo tanto, no se replican entre servidores de la misma forma que el resto de configuraciones.

Configuración del servidor IAS

En esta categoría se incluyen los siguientes elementos:

- Registro de las solicitudes de autenticación en el registro de sucesos de Windows. En esta solución se habilita el registro tanto de los sucesos correctos como de los erróneos.

  Nota: el registro de solicitudes se detalla en la sección "Registro de RADIUS" más adelante en este capítulo.

- Puertos de Protocolo de datagramas de usuarios (UDP) que el servidor IAS escucha para las solicitudes de autenticación y de responsabilidad de RADIUS. En esta solución se utilizan los puertos de RADIUS 1812 y 1813 para la autenticación y la contabilidad respectivamente.

Directivas de RADIUS

Las directivas de servidor IAS controlan la autenticación y la autorización de las cuentas en la red. Existen dos tipos de directivas:

- Directiva de acceso remoto.
- Directiva de solicitud de conexión.

La directiva de acceso remoto controla si se autoriza una conexión en la red y el modo en que se hace. Este tipo de directiva contiene un grupo de condiciones de filtro que determinan si la directiva es apropiada para una solicitud de conexión concreta. Algunos ejemplos de condiciones de filtro son: especificación del grupo de seguridad de Windows al que un cliente debe pertenecer; especificación del tipo de conexión (inalámbrica, VPN, etc.) del cliente que realiza la solicitud, y especificación del momento del día en que el cliente intenta conectarse. Cada directiva de acceso remoto posee una acción de directiva, que se establece en *permitir* o *denegar* una solicitud de conexión. Las solicitudes de conexión que coincidan con el filtro de condición de la

directiva de acceso remoto obtendrán permiso de acceso o no en función de la configuración de esta acción de directiva.

Asimismo, una directiva de acceso remoto contiene una serie de parámetros que se aplican a una conexión permitida, conocidos como perfil de directiva de acceso remoto. Estos parámetros incluyen los métodos de autenticación que se consideran aceptables para esta conexión, el modo en que una dirección IP se asigna al cliente y la cantidad de tiempo durante la que el cliente puede permanecer conectado antes de que la reautenticación sea necesaria. Pueden existir muchas directivas de acceso remoto en un IAS. Así, cada solicitud de conexión se evalúa en relación con éstas (por orden de prioridad), hasta que una directiva coincidente permita o deniegue la solicitud.

La directiva de acceso remoto en esta solución se configura tal y como se muestra en la tabla siguiente:

Tabla 2.4. Configuración de directivas de acceso remoto

Elemento de configuración	**Configuración**
Nombre de directiva	Permitir acceso a LAN inalámbrica
Tipo de directiva	Permitir
Condiciones de directiva de acceso remoto	
Coincidencias de tipo de puerto NAS	IEEE 802.11 inalámbrico Otros dispositivos inalámbricos
Coincidencias del grupo de Windows	Acceso a LAN inalámbrica
Perfil de directiva de acceso remoto	
Restricciones de marcado: tiempo de espera del cliente	60 minutos (WEP dinámica) 8 horas (WPA)
Asignación de dirección IP	La configuración del servidor determina la asignación de la IP
Filtrado IP	Ninguno
Autenticación	Todo deshabilitado aparte de EAP
Autenticación: tipo de EAP empleado	EAP protegido (PEAP)
Autenticación: tipo de PEAP empleado	EAP MS-CHAP v2
Autenticación: reconexión rápida	Habilitado
Atributos RADIUS	Ignorar propiedades de acceso telefónico del usuario = "True" Acción terminación = "RADIUS-Request"

El filtro de condiciones coincide con todos los clientes inalámbricos y con todos los miembros del grupo de dominio de acceso a LAN inalámbrica. La tabla no contempla aquellos parámetros que no sean relevantes para el acceso a WLAN, como puedan ser Multilink o el cifrado punto a punto de Microsoft (MPPE). Para obtener más detalles sobre el uso de los grupos de seguridad con la directiva de acceso remoto, consulte la sección "Modelo de administración de usuario y equipo de WLAN" más adelante en este capítulo.

La configuración Restricciones de marcado: tiempo de espera del cliente puede incidir en la seguridad y en la confiabilidad de la solución. Los motivos por los que han de usarse valores distintos a los recogidos en la tabla se exponen en la sección "Opciones de seguridad para la WEP dinámica" más adelante en este capítulo.

El atributo RADIUS "Ignorar-propiedades-de-acceso-telefónico-del-usuario" se utiliza para omitir el control de los permisos de acceso a la red por usuario. Consulte la sección "Modelo de administración de usuario y equipo de WLAN" para obtener una explicación del control del acceso por usuario y por grupo.

Una directiva de solicitud de conexión controla si la solicitud se procesa en un servidor RADIUS concreto o si se envía a otro distinto (conocido como proxy RADIUS). Normalmente, un proxy RADIUS se utiliza cuando un servidor RADIUS no posee la información necesaria para procesar la solicitud por sí mismo y, por lo tanto, debe reenviarlo a un servidor RADIUS autoritativo (por ejemplo, a un servidor en otro bosque de Active Directory). Los servidores proxy RADIUS no se utilizan en esta solución y no competen a esta guía.

Para obtener más información sobre las directivas de solicitud de acceso remoto y de solicitud de conexión, así como sobre el uso de los servidores proxy RADIUS, consulte la sección "Referencias" al final de este capítulo.

Registro de RADIUS

Puede configurar los servidores IAS para registrar dos tipos de información opcional:

- Sucesos de autenticación aceptados y rechazados.
- Información de autenticación y cuentas de RADIUS.

Los sucesos de autenticación aceptados y rechazados generados a partir de dispositivos y usuarios de WLAN se pueden registrar en el registro de sucesos del sistema Windows Server 2003 del servidor IAS. La información que el registro de sucesos de autenticación contiene es muy útil para la solución de problemas de autenticación, aunque también se puede utilizar con fines de alerta y auditoría de seguridad.

Puede considerar deshabilitar los sucesos aceptados una vez que el sistema se haya estabilizado, si bien, en un principio, el registro de sucesos aceptados y rechazados debe dejarse habilitado. El motivo reside en que, pese a que los sucesos de acceso a WLAN aceptados inunden el registro de sucesos del sistema, puede que sean necesarios para fines de auditoría.

Si utiliza una herramienta de supervisión y alerta como Microsoft Operations Manager (MOM), debería considerar la idea de agregar una regla para avisar de los sucesos de error en la autenticación de IAS en el registro de sucesos del sistema. Otra opción consiste en usar una herramienta de consulta del registro de sucesos como eventquery.vbs para comprobar el registro de sucesos en busca de errores de autenticación (consulte la entrada "Eventquery.vbs" en la ayuda en línea). Por lo general, los sucesos individuales son de poca importancia, pero una serie de dichos sucesos podría indicar que se ha intentado irrumpir en el sistema.

IAS también ofrece la posibilidad de registrar información de la sesión de autenticación y del acceso a la red en forma de registros de solicitudes de RADIUS. Por lo general, el registro de RADIUS se emplea cuando es preciso cobrar por el uso de la red (por ejemplo, como proveedor de un servicio Internet (ISP), ha de cobrar en función del tiempo de conexión) o bien cuando es necesario contar con información de auditoría de seguridad especializada (aunque en la mayoría de los casos esto ya lo cubren los sucesos de autenticación registrados en el registro de sucesos).

Para obtener más información sobre el registro de RADIUS, consulte la sección "Referencias" al final del capítulo.

Seguridad IAS

Las precauciones de seguridad para IAS deben ser las mismas que se usan para un controlador de dominio. Un control seguro de la red depende de la seguridad de la infraestructura de IAS. Para mejorar la seguridad de IAS, puede implementar una serie de medidas sencillas:

- Utilice contraseñas seguras para los clientes RADIUS (puntos de acceso inalámbrico). La solución incluye secuencias de comandos para generar contraseñas verdaderamente aleatorias que dificulten los ataques de diccionario.
- Habilite el autenticador de mensajes de RADIUS en todos los clientes RADIUS a fin de evitar la imitación de

direcciones IP de los puntos de acceso inalámbrico. En esta solución, esta opción está habilitada.

- Asegúrese de que la configuración de seguridad del servidor es la adecuada. Esto se trata en el capítulo 3, "Preparación del entorno".
- Asegúrese de que se han aplicado las revisiones de seguridad más recientes en el servidor y, asimismo, que se obtienen revisiones actualizadas de forma periódica. Esto también se incluye en el capítulo 3, "Preparación del entorno".
- Asegúrese de que usa una configuración de cuenta de dominio segura. En concreto, debería asegurarse de que se utilizan contraseñas seguras y de que se cambian con regularidad. Igualmente, no olvide habilitar el bloqueo de cuenta de dominio para bloquear los ataques de averiguación de contraseña. No obstante, se recomienda habilitar únicamente el bloqueo de cuentas en caso de que tenga los recursos de soporte con los que desbloquear las cuentas de los usuarios de manera puntual.
- Considere utilizar IPSec para proteger el tráfico de RADIUS y reforzar la autenticación mutua entre los puntos de acceso inalámbrico y los servidores IAS. No obstante, no todos los puntos de acceso inalámbrico son compatibles con IPSec.

Para obtener más información sobre las medidas de seguridad de IAS, consulte la sección "Referencias" al final del capítulo.

Modelo de administración de usuario y equipo de WLAN

El acceso a la WLAN en esta solución se controla por medio de grupos de seguridad de dominio. Bien es cierto que se puede hacer uso de las propiedades de acceso telefónico de los objetos de usuario de dominio para admitir o denegar el acceso a elementos individuales, pero esto supondría una tarea de administración muy pesada para muchos de los usuarios.

La solución emplea un esquema realmente básico para conceder el acceso a WLAN a todos los usuarios y equipos del dominio. Para muchas organizaciones, el control del acceso a través de la pertenencia al dominio es ya lo suficientemente seguro y reduce la carga de administración adicional asociada a la WLAN. En el caso de algunas organizaciones que precisan un control mayor, no obstante, pueden emplearse grupos de seguridad para definir quién tiene permiso para tener acceso a la WLAN.

Tal y como se describe en la sección "Directivas de RADIUS", la directiva de acceso remoto en un IAS utiliza una condición de filtro que concede acceso a WLAN a todos los miembros del grupo de acceso a la LAN inalámbrica. En la tabla siguiente se plasma la pertenencia del grupo de acceso a la LAN inalámbrica.

Tabla 2.5. Grupos de acceso inalámbrico para permitir a todos los usuarios y equipos

Grupo universal de nivel superior (acceso concedido en la directiva de acceso remoto)	Miembros de primer nivel (grupos globales de dominio)	Miembros de segundo nivel (grupos globales de dominio)
Acceso a LAN inalámbrica	Usuarios de LAN inalámbrica	Usuarios de dominio
Acceso a LAN inalámbrica	Equipos de LAN inalámbrica	Equipos de dominio

El grupo de la primera columna, Acceso a LAN inalámbrica, tiene dos miembros enumerados en la segunda columna, esto es, Usuarios de LAN inalámbrica y Equipos de LAN inalámbrica. Estos grupos "de primer nivel" contienen miembros (que aparecen en la tercera columna, "Miembros de segundo nivel"), esto es, los grupos de usuarios de dominio y de equipos de dominio respectivamente. Esta disposición de grupos anidados posibilita que todos los usuarios y equipos del dominio se conecten a WLAN.

Si resulta excesivamente permisivo para la organización que todos los usuarios y equipos tengan acceso a

WLAN, puede eliminar a unos u otros de estos grupos. De ser así, deberá agregar las cuentas o grupos de usuario y de equipo concretas a los grupos de LAN inalámbrica. En la tabla siguiente se refleja el modo de usar la estructura de grupos de acceso a la LAN inalámbrica de la forma descrita.

Tabla 2.6. Grupos de acceso inalámbrico para permitir a usuarios y equipos seleccionados

Grupo universal de nivel superior (acceso concedido en la directiva de acceso remoto)	Miembros de primer nivel (grupos globales de dominio)	Miembros de segundo nivel (grupos globales de dominio)
Acceso a LAN inalámbrica	Usuarios de LAN inalámbrica	Usuario1 Usuario2 Usuario3
Acceso a LAN inalámbrica	Equipos de LAN inalámbrica	Equipo1 Equipo2 Equipo3

Para obtener más información sobre el uso de estos grupos de seguridad en un bosque con varios dominios, consulte la sección "Escalabilidad para organizaciones más grandes" más adelante en este capítulo.

Obtención de certificados para servidores IAS

Los servidores IAS requieren tener certificados para autenticar a los clientes WLAN. Los certificados de servidor son necesarios para crear el túnel cifrado de TLS entre servidores IAS y clientes. TLS sirve para proteger el intercambio de autenticaciones entre el servidor y los clientes.

Nota: TLS constituye un estándar de RFC basado en la versión similar de capa de sockets seguros 3.0 (SSL 3.0). Ambos se emplean habitualmente para proteger el tráfico Web como parte del Protocolo de transferencia de hipertexto seguro (HTTPS).

Entidad emisora de certificados incrustada frente a entidad emisora de certificados comercial

Para obtener estos certificados, puede optar por instalar una entidad emisora por sí mismo o bien adquirir los certificados de un proveedor de certificados comercial. Ambas posibilidades son válidas y decantarse por una u otra no supone una diferencia técnica real para la solución de WLAN.

La tabla que sigue a continuación muestra las ventajas y los inconvenientes principales de usar una entidad emisora de certificados interna en lugar de comprar certificados a un proveedor comercial.

Tabla 2.7. Ventajas e inconvenientes de usar una entidad emisora de certificados propia frente a certificados comerciales

Entidad emisora interna	Entidad emisora comercial
Sin coste por certificado	Coste por certificado
El software de la entidad emisora de certificados debe instalarse y administrarse	No hay software de servidor
Inscripción y renovación automáticas	Proceso de inscripción más complejo, instalación manual de los certificados

El equilibrio del argumento se basa en la complejidad y el coste de la administración de la entidad emisora de certificados propia. Así, si el coste de la configuración de una entidad emisora de certificados local es moderado

y la administración sencilla, normalmente resulta más atrayente que la opción de adquirir certificados externos.

Esta solución emplea una entidad emisora interna y sencilla para proporcionar los certificados. Los términos "entidad emisora de certificados incrustada" y "entidad emisora de certificados de red" se han usado en la presente guía para señalar que se trata de una entidad emisora con un propósito especial; en esencia, esta entidad no es visible para usuarios y administradores, y expide certificados de una sola clase. La funcionalidad limitada de la entidad emisora de certificados en esta solución quiere decir que se puede instalar y usar sin administración o intervención alguna del usuario. Por ejemplo, en esta solución, la entidad emisora de certificados puede expedir un certificado que tenga una duración de 25 años, de manera que no tendrá que renovarlo durante la vigencia de la solución. La inscripción y renovación automáticas de los certificados del servidor IAS indican que no hay que realizar una distribución manual de los certificados.

Compare esto con el uso de certificados externos. Recuerde que debe renovar los certificados de todos los servidores IAS cada año o cada dos años, lo que significa crear manualmente la solicitud de certificado en todos los servidores IAS, enviar la solicitud a la entidad emisora de certificados comercial y, finalmente, obtener el certificado expedido e instalarlo manualmente. Si esto no se lleva a cabo, impedirá que los usuarios se conecten a la WLAN. Para muchas organizaciones, esto supone una carga administrativa mucho más pesada que la entidad emisora de certificados interna básica utilizada en esta solución.

Limitaciones de la entidad emisora de certificados de la solución

Esta solución usa una configuración de entidad emisora de certificados especial para expedir certificados para los servidores IAS. Se ha diseñado con el único propósito de cubrir esta necesidad concreta, de modo que no se trata de una autoridad de certificaciones con fines generales.

Los certificados digitales se emplean en muchas aplicaciones, entre otras, el correo electrónico seguro y la exploración Web, la seguridad IP (IPSec), las redes privadas virtuales (VPN) o el sistema de cifrado de archivos (EFS). Cada una de estas aplicaciones posee sus propios requisitos de seguridad. Su organización tendrá una serie de requisitos de seguridad propios y exclusivos de acuerdo con estas aplicaciones. Por estos motivos, Microsoft recomienda enormemente no usar la entidad emisora de certificados de la solución con cualquier otro propósito.

Si tiene intención de usar esas u otras aplicaciones de certificado, diseñe una infraestructura de certificados de acuerdo a los requisitos correspondientes. Algunos de los aspectos que debe tener en cuenta son:

- La entidad emisora de certificados de la solución es una entidad emisora raíz con firma personal, de manera que no se puede revocar (los certificados expedidos se revocan en caso de compromiso de la entidad emisora).
- Es posible que la legislación industrial o específica de cada país obligue al uso de una jerarquía de varios niveles de entidades emisoras para algunos o todos los tipos de certificado.
- Microsoft no recomienda la instalación de una entidad emisora de certificados en un controlador de dominio en el caso de certificados de alta seguridad.

Para obtener más información sobre el planeamiento detallado que se necesita para diseñar una arquitectura de infraestructura de claves públicas más general, consulte el capítulo 4, "Diseño de la infraestructura de claves públicas", de la solución complementaria, *Solución de Seguridad de LAN inalámbricas — Servicios de Certificate Server de Microsoft Windows Server 2003*.

También se ha de tener en cuenta que existe un número de limitaciones cuando la entidad emisora de certificados se instala en la versión Standard Edition de Windows Server 2003, que, aunque adecuada para la solución, es compatible con una serie limitada de funcionalidades en comparación con la versión Enterprise Edition de Windows Server 2003. Entre las características más destacadas de las que no se puede disponer en la versión Enterprise Edition de Windows Server 2003 se incluyen las siguientes:

- **Inscripción automática de certificados para equipos y usuarios:** el servicio de solicitud de certificados automática (que se usa en Windows 2000 Server y Windows Server 2003, Standard Edition) no permite la inscripción automática de certificados para el usuario, ya que sólo es compatible con la inscripción automática de certificados de equipo.

- **Plantillas de certificado de la versión 2:** muchos de los tipos de certificado utilizados en Windows Server 2003 y en Windows XP emplean las características avanzadas de las plantillas de la versión 2. Sin embargo, una entidad emisora basada en la versión Standard Edition de Windows Server 2003 no puede expedir certificados en plantillas de versión 2.
- **Plantillas de certificado modificables:** las plantillas de la versión 1 no se pueden modificar o crear para generar nuevos tipos de certificado.
- **No es compatible con el almacenamiento de claves**.

Si precisa alguna de estas características, necesitará una entidad emisora de certificados basada en las capacidades más avanzadas de la versión Enterprise Edition de Windows Server 2003. Para obtener una descripción minuciosa de las diferencias existentes entre Enterprise Edition y Standard Edition, consulte el documento "PKI Enhancements in Windows XP Professional and Windows Server 2003", incluido en la sección "Referencias" al final de este capítulo.

Si, por el contrario, actualmente no debe cumplir con requisitos establecidos en relación con otros tipos de certificados, podrá implementar la entidad emisora de certificados descrita en esta solución sin cerrar otras opciones en el futuro. De esta manera, si en una fase posterior identifica otros requisitos relativos a los certificados, podrá implementar una infraestructura de claves públicas más sofisticada. Esto le permitirá ejecutarlos conjuntamente o migrar para emitirlos todos desde la nueva infraestructura.

Clientes WLAN

La solución de WLAN es compatible con varios tipos distintos de clientes WLAN, ya sea de manera explícita o implícita. Asimismo, esta solución es compatible con clientes Windows XP, Professional Edition, Windows XP, Tablet Edition y Pocket PC 2003. Para obtener una orientación específica sobre el modo de configurar y usar estos clientes con la solución, consulte el capítulo 6, "Configuración de clientes de LAN inalámbricas". La guía no contempla el uso de otros tipos de clientes que admitan 802.1X con PEAP-MS-CHAP v2. Si bien algunos de estos tipos funcionarían (Windows 2000 Professional, por poner un ejemplo), la presente guía no contiene instrucciones sobre cómo configurarlos; además, el equipo de Microsoft Solutions for Security no ha realizado pruebas con ellos en esta solución.

Windows XP

Esta solución es plenamente compatible con Windows XP, Professional Edition y Windows XP, Tablet Edition. Todos los clientes Windows XP se deben actualizar con Service Pack 1 o posterior. Asimismo, los equipos deben ser miembros del mismo dominio que los servidores IAS o, al menos, miembros de otro dominio dentro del mismo bosque. La pertenencia a un dominio es necesaria para que los equipos se autentiquen en la WLAN y descarguen la configuración de WLAN especificada en la directiva de grupo.

La autenticación del equipo en la WLAN se emplea cuando ningún usuario ha iniciado sesión en él. De esta forma, el equipo podrá obtener la configuración del objeto de directiva de grupo, ejecutar secuencias de comandos de inicio y descargar revisiones. Esto también es necesario durante las primeras fases de inicio de sesión del usuario, ya que éste no podrá empezar la autenticación en WLAN hasta que se cargue su perfil. En consecuencia, se producirá un error en las secuencias de comandos de inicio de sesión, en otras configuraciones de objeto de la directiva de grupo y en los perfiles de itinerancia si el equipo no tiene una conexión existente con la red antes de que el usuario inicie sesión.

La solución puede usar equipos con Windows XP que no pertenezcan al dominio con las siguientes salvedades:

- Deberá configurar el cliente WLAN manualmente.
- La autenticación del equipo en WLAN no es fácil de obtener.
- Para la autenticación del usuario en WLAN, el usuario deberá escribir sus credenciales de dominio (WLAN) en el cuadro de nombre de usuario y contraseña que aparezca.

Microsoft recomienda encarecidamente habilitar el servidor de seguridad personal en todos aquellos equipos cliente en los que se usen elementos inalámbricos.

Pocket PC 2003

Pocket PC 2003 es compatible con 802.1X y PEAP, si bien es posible que tenga que hacerse con actualizaciones del proveedor del dispositivo y de Microsoft para disfrutar de toda la funcionalidad de WLAN. Se pueden usar también versiones de Pocket PC anteriores a 2003, pero Microsoft no ha proporcionado compatibilidad integrada de 802.1X para versiones más antiguas. Es probable que pueda conseguir compatibilidad específica si se dirige al proveedor del dispositivo Pocket PC en cuestión, o bien si usa el software del cliente WLAN de otro fabricante.

Los sistemas Pocket PC no tienen un concepto de una cuenta de dominio de equipo y siempre se autentican en la WLAN por medio de las credenciales de usuario. Por lo general, un usuario debe escribir el nombre de usuario y la contraseña de dominio cada vez que quiera conectarse a la WLAN. Las credenciales se pueden guardar de manera que el dispositivo se conecte automáticamente, pero no es recomendable, a menos que se tengan unas características de seguridad muy sólidas en el dispositivo de Pocket PC.

Además, los Pocket PC no entienden el concepto de directiva de grupo, por lo que la configuración de WLAN no podrá establecerse de manera automática, sino manual.

Otros clientes 802.1X

Puede que algunos clientes que no son Windows XP ni Pocket PC 2003 funcionen con esta solución, siempre que sean compatibles con 802.1X y PEAP-MS-CHAP v2. Los clientes Windows 2000 son compatibles si se usa Microsoft 802.1X Authentication Client de Windows 2000. Los detalles sobre el modo de obtener Microsoft 802.1X Authentication Client de Windows 2000 se incluyen en las referencias recogidas al final del capítulo. Aquellos clientes de Windows que no sean Windows 2000 (así, Windows NT 4.0, Windows 9*x* y Windows Me) son compatibles con un cliente disponible a través de Microsoft Premier Support. Puede que obtenga un cliente para estas y otras plataformas de proveedores de software de red que no sean de Microsoft.

Consulte el apéndice C, "Versiones de sistemas operativos compatibles".

Compatibilidad con WPA

La solución de WLAN que aquí se describe admite el uso de la protección WPA en lugar de la WEP dinámica. WPA es siempre preferible a WEP, por cuanto ofrece una administración de claves más eficaz, al tiempo que implementa un algoritmo de cifrado de red más seguro. Asimismo, WPA admite el uso del cifrado de AES siempre que el hardware (puntos de acceso inalámbrico y adaptadores de red) proporcione la compatibilidad pertinente.

Si bien WPA proporciona un número de ventajas frente a la clave dinámica, hay una serie de puntualizaciones sobre su uso:

- No se dispondrá de compatibilidad con el objeto de directiva de grupo para configurar WPA en clientes WLAN a menos que se tenga Windows Server 2003 Service Pack 1.
- Es posible que el cliente sólo sea compatible con el sistema Windows XP. Si bien puede que Microsoft proporcione compatibilidad de WPA para Pocket PC 2003, es posible que no exista compatibilidad con Windows 2000 y otros clientes de Microsoft (algunos proveedores que no sean de Microsoft quizá proporcionen compatibilidad de WPA para estos clientes).
- Puede que no sea posible actualizar el equipo de WLAN existente (puntos de acceso inalámbrico y adaptadores de red de los clientes) para que sea compatible con WPA. Asimismo, puede que el coste por adquirir e implementar el nuevo hardware sea muy elevado.

La compatibilidad del objeto de directiva de grupo y de Pocket PC 2003 con WPA tendrá lugar pronto (lo que hará de WPA una alternativa por la que decantarse), pero, hasta entonces, la WEP dinámica en uso conjunto con la autenticación 802.1X seguirá ofreciendo un nivel de protección muy elevado para las WLAN. Ésta es la elección predeterminada para esta solución. Para obtener más información sobre WPA, consulte la sección "Referencias" al final de este capítulo.

Migración desde una WLAN existente

Si ya tiene instalada una red inalámbrica, debe planear una estrategia de migración con antelación para garantizar que los usuarios y el entorno se vean afectados lo mínimo posible.

Muchas organizaciones tienen WLAN basadas en 802.11 que funcionan sin autenticación o cifrado de red, mientras que otras han implementado la WEP estática usando el cifrado de clave compartida combinado

frecuentemente con el filtrado de direcciones de control de acceso de medios.

El proceso de migración de uno de estos escenarios a una WLAN protegida con 802.1X implica la consecución de los siguientes pasos:

1. **Implementación de certificados para servidores IAS:** para obtener detalles sobre el modo de implementar certificados en un servidor IAS, consulte el capítulo 4 de esta guía, "Creación de la entidad emisora de certificados de red".

2. **Configuración de las directivas de acceso remoto a redes inalámbricas en servidores IAS:** los pasos para configurar una directiva de acceso remoto inalámbrico se detallan en el capítulo 5 de esta guía, "Creación de la infraestructura de seguridad en LAN inalámbricas".

3. **Implementación de una configuración de WLAN para los equipos cliente de la nueva WLAN nuevos:** la nueva red habilitada para 802.1X necesita un nuevo Identificador del conjunto de servicios de red. Así, la configuración de red para la nueva WLAN podrá implementarse mediante el objeto de directiva de grupo de Active Directory. La directiva de grupo de WLAN debe implementarse con suficiente antelación a la reconfiguración de los puntos de acceso inalámbrico para garantizar que los equipos móviles con acceso a LAN ocasional reciban la configuración. Esto se trata en el capítulo 6, "Configuración de clientes de LAN inalámbricas".

4. **Configuración de puntos de acceso inalámbrico para que requieran la seguridad 802.1X:** por lo general, la mejor forma de llevar esto a cabo es sitio por sitio (por ejemplo, por edificios o por recintos) y ya sea fuera del horario laboral, o bien con el aviso correspondiente a los usuarios sobre una posible interrupción de la actividad de la WLAN. Deberá crear entradas de clientes RADIUS relacionados con IAS para todos los puntos de acceso inalámbrico del sitio, configurar los puntos de acceso con las direcciones de los servidores IAS para las entradas de RADIUS de los puntos de acceso y, finalmente, cambiar el punto de acceso para permitir únicamente a clientes autenticados con 802.1X. Puede que quiera hacer una copia de seguridad de la configuración de los puntos de acceso inalámbrico antes de iniciar este paso para que, en caso de emergencia, pueda recuperarse de forma sencilla.

Este modo de proceder provoca un trastorno menor en los usuarios, al tiempo que permite la recuperación de un sitio con facilidad en caso de que algo vaya mal. Es inevitable que, durante el cambio, los usuarios tengan que hacer frente a algún tipo de problema, de manera que es aconsejable mantenerlos convenientemente informados sobre la migración y, asimismo, deberá estar preparado para recibir más llamadas de soporte técnico de lo habitual.

Como sucede en todas las estrategias de migración, es esencial realizar un planeamiento y una comprobación precisos. Los pasos que implica la configuración de equipos cliente y puntos de acceso inalámbrico puede ocasionar cambios molestos en el entorno si no se prueba con detenimiento para resolver problemas incipientes.

El planeamiento detallado de la migración desde una WLAN insegura con WEP estática, o bien desde esquemas de seguridad de WLAN de propiedad, no se incluye en esta guía, ya que en principio son similares y siguen la pauta anterior. No obstante, si precisa de más asistencia para el planeamiento de la migración, consulte con su socio de Microsoft o bien póngase en contacto con la subsidiaria de Microsoft local, que, a su vez, le pondrá en contacto con un socio de Microsoft de su zona o con los Servicios de consultoría de Microsoft.

Principio de la página

Escalabilidad para organizaciones más grandes

En esta sección se describen algunas de las consideraciones clave para el uso de esta solución en organizaciones de mayor volumen (una con miles de usuarios, por ejemplo). El uso de PEAP y de la autenticación mediante contraseña en la empresa se explica en el apéndice A, "Uso de PEAP en la empresa".

Colocación del servidor IAS

A medida que aumenta el número de ubicaciones donde se admiten las redes WLAN, necesitará decidir el modo en que los servidores IAS van a atender estos puntos de acceso inalámbrico. Existen dos enfoques

fundamentalmente:

- **Uso de un número reducido de servidores IAS centrales:** emplee un número pequeño de servidores IAS centrales para controlar todo el tráfico de autenticación en la WLAN (dos probablemente sería suficiente). Será necesario garantizar que las conexiones de WLAN entre oficinas remotas y los servidores IAS sean resistentes.
- **Distribución de los servidores IAS en cada oficina:** el límite de tamaño de una oficina donde esto reporta beneficios económicos es más bajo, pero, como regla general, cualquier oficina que sea lo suficientemente grande como para tener controladores de dominio propios puede tener IAS de manera local (normalmente, instalado en el controlador de dominio).

La opción de invertir en la resistencia de la red puede parecer costosa, pero es necesario que la contraste con el coste de administración de los diversos servidores IAS distribuidos. Aun cuando IAS se halle instalado físicamente en el mismo servidor que un controlador de dominio existente, la administración de cada una de las instancias IAS supondrá un gasto. En la práctica, la mayoría de las grandes organizaciones emplearán un híbrido de ambas en alguna de las siguientes formas:

- Centralización de los servidores IAS e inversión en resistencia de la WAN siempre que sea posible.
- Distribución de IAS a oficinas donde no se puede disponer de resistencia de WAN o donde ésta es tremendamente costosa.
- Uso de redes WLAN WPA de clave compartida previamente para oficinas muy pequeñas con escasa conectividad o para oficinas de aquellos empleados que trabajen desde casa.

La estrategia centralizada de IAS aparece reflejada en una sección anterior de este capítulo, "Colocación del servidor IAS". La siguiente figura muestra el uso de un controlador de dominio local y de IAS en una sucursal. Ésta contempla una oficina remota más grande vinculada, mediante WAN, a la oficina central de la figura 2.4. anterior.

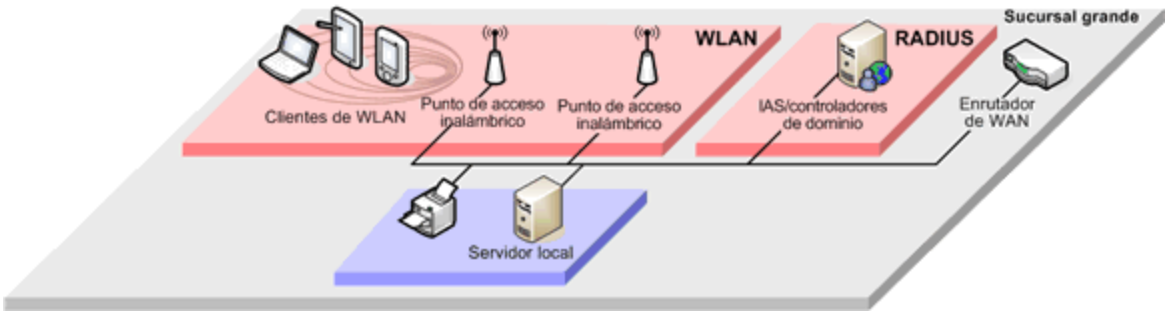

Figura 2.7. Sucursal más grande con controlador de dominio local e IAS
Vista de imagen a pantalla completa

En este sitio, los puntos de acceso se configuran para usar el servidor IAS local como servidor RADIUS principal y uno de los servidores IAS de la oficina central, como servidor RADIUS secundario. Esto quiere decir que los clientes WLAN se pueden autenticar, incluso cuando se produzca un error en el servidor IAS local o en la conectividad WAN.

No obstante, si posee una conectividad WAN resistente (por ejemplo, varios vínculos WAN con proveedores distintos), apenas sacará partido de la implementación de servidores adicionales en las sucursales; de hecho, sólo agregará complejidad y más carga de administración.

Dominios múltiples

El diseño básico de la solución presenta una escala nítida con varios bosques de dominios. A continuación se exponen los puntos clave que se han de tener en cuenta al usar la solución con varios dominios:

- Los servidores IAS deben registrarse en cada dominio que tenga usuarios y equipos que vayan a tener acceso

a la WLAN. Para obtener detalles, consulte el capítulo 5, "Creación de la infraestructura de seguridad en LAN inalámbricas".

- Los objetos de directiva de grupo para la configuración tanto del servidor como de la solicitud de certificados automática se deberán importar a todos los dominios en los que se instalen servidores IAS. Los pasos para llevar esto a cabo se explican en los capítulos 3, "Preparación del entorno" y 4, "Creación de la entidad emisora de certificados de red".
- El objeto de directiva de grupo que controla la configuración de WLAN del equipo cliente debe crearse en cada dominio donde haya equipos cliente que vayan a tener acceso a la WLAN. Para obtener más detalles al respecto, consulte el capítulo 6, "Configuración de clientes de LAN inalámbricas".
- Los grupos de seguridad que IAS utiliza para filtrar las directivas de acceso remoto deben configurarse a fin de admitir varios dominios.

Los tres primeros elementos no precisan más aclaración y, en cuanto a los pasos necesarios para configurarlos para dominios múltiples, se enumeran en capítulos posteriores. El tema del uso de los grupos de seguridad es algo más complejo y, como tal, se detalla en la siguiente sección.

Uso de grupos de seguridad en dominios múltiples

La siguiente tabla refleja el modo en que los grupos de seguridad descritos en la sección "Modelo de administración de usuario y equipo de WLAN" se pueden organizar dentro de un bosque con varios dominios.

Tabla 2.8. Grupos de acceso inalámbrico para permitir a todos los usuarios y equipos

Grupo universal de nivel superior (acceso concedido en la directiva de acceso remoto)	Miembros de primer nivel (grupos globales de dominio)	Miembros de segundo nivel (globales de dominio)
DomRa\Acceso a LAN inalámbrica	DomUsuario1\Usuarios de LAN inalámbrica	DomUsuario1\Usuarios de dominio
DomRa\Acceso a LAN inalámbrica	DomUsuario2\Usuarios de LAN inalámbrica	DomUsuario2\Usuarios de dominio
DomRa\Acceso a LAN inalámbrica	DomUsuario3\Usuarios de LAN inalámbrica	DomUsuario3\Usuario1 DomUsuario3\Usuario2 DomUsuario3\Usuario2
DomRa\Acceso a LAN inalámbrica	DomUsuario1\Equipos de LAN inalámbrica	DomUsuario1\Equipos de dominio
DomRa\Acceso a LAN inalámbrica	DomUsuario2\Equipos de LAN inalámbrica	DomUsuario2\Equipos de dominio
DomRa\Acceso a LAN inalámbrica	DomUsuario3\Equipos de LAN inalámbrica	DomUsuario3\Equipos de recursos humanos DomUsuario3\Equipos de finanzas

Esta tabla refleja la misma disposición de grupos anidados que las tablas de la sección "Modelo de administración de usuario y equipo de WLAN". Los miembros de los grupos recogidos en la primera columna aparecen en la segunda columna y los de los grupos enumerados en la segunda columna, en la tercera.

El ejemplo de la tabla emplea nombres ficticios. Así, DomRa es el nombre del dominio en el que se instalan los servidores IAS, mientras que DomUsuario1 y DomUsuario2 hacen referencia a otros dominios que contienen usuarios y equipos a los que se concede acceso a WLAN.

En el ejemplo, todos los usuarios y equipos de DomUsuario1 y DomUsuario2 obtienen acceso a la WLAN de forma implícita, por cuanto los usuarios y los equipos de dominio de tales dominios pertenecen a los grupos de

usuarios y de equipos de LAN inalámbricas para el mismo dominio. Sin embargo, los usuarios de DomUsuario3 se agregan de manera individual a los grupos de usuarios de la LAN inalámbrica de DomUsuario3. Los equipos obtienen acceso mediante los grupos de seguridad de unidad comercial (por ejemplo, todos los equipos en el departamento de recursos humanos).

Los grupos globales para cada dominio (esto es, para usuarios de LAN inalámbrica y equipos de LAN inalámbrica) se agregan como miembros del grupo universal de acceso a LAN inalámbrica. Todos los miembros de este último grupo obtienen acceso a WLAN en la directiva de acceso remoto de IAS.

Arquitectura de infraestructura de claves públicas

Tal y como se menciona en la sección anterior "Obtención de certificados para servidores IAS", una gran parte de las aplicaciones usan certificados. Es importante resaltar que, si bien es adecuada para esta solución, es posible que una entidad emisora de certificados independiente no cubra las necesidades de organizaciones más grandes por ser más diversas. Así, antes de implementar la entidad emisora descrita en esta guía, sopese con detenimiento el uso de otros certificados que pueda tener en el futuro, así como de otras arquitecturas de infraestructura de claves públicas alternativas que se adecuen de mejor forma a estos escenarios.

Para obtener información detallada sobre el planeamiento de la infraestructura de claves públicas, consulte el capítulo 4, "Diseño de la infraestructura de claves públicas", de la solución complementaria, *Solución de Seguridad de LAN inalámbricas — Servicios de Certificate Server de Microsoft Windows Server 2003*. Aun siendo más sofisticada que la entidad emisora de certificados de esta guía, la infraestructura de claves públicas tratada en esa solución sigue siendo relativamente sencilla (sólo usa dos entidades emisoras de certificados, por ejemplo). No obstante, se ha diseñado para que constituya la base de un intervalo mucho más amplio de necesidades de certificado.

Si decide implementar una infraestructura de claves públicas más sofisticada (como ésta), podrá tomar como referencia las indicaciones del capítulo 4 de esta guía, "Creación de la entidad emisora de certificados de red". De todas formas, no olvide que debe aplicar los siguientes cambios en las instrucciones que ese capítulo contempla:

- Instale la entidad emisora de certificados en su propio servidor y no en un controlador de dominio.
- Utilice la versión Enterprise Edition de Windows Server 2003 a fin de poder disfrutar de una mayor flexibilidad en el futuro.
- En lugar de usar el servicio de solicitud de certificados automática, emplee la inscripción automática de Windows Server 2003. Para obtener instrucciones sobre el modo de usar la inscripción automática, consulte la documentación de producto de Windows Server 2003 Enterprise Edition.
- Use la plantilla de certificado "Servidor RAS e IAS", o bien cree un tipo de certificado de cliente para los certificados del servidor IAS en lugar de usar la plantilla "Equipo".

  Nota: "RAS" en la plantilla de certificados corresponde al inglés *Remote Access Service* (servicio de acceso remoto).

Podrá obtener más indicaciones al respecto en la sección sobre la infraestructura de claves públicas de la documentación de producto de Windows Server 2003, así como en el capítulo 4 ("Diseño de la infraestructura de claves públicas"), el capítulo 7 ("Implementación de la infraestructura de claves públicas") y el capítulo 9 ("Implementación de la seguridad de LAN inalámbricas mediante 802.1X") de la solución complementaria, *Solución de Seguridad de LAN inalámbricas — Servicios de Certificate Server de Microsoft Windows Server 2003*.

Principio de la página

Variaciones en la arquitectura de la solución

En esta sección se tratan las variaciones que pueden producirse en el diseño básico. Las siguientes subsecciones se centran en las alternativas de configuración de seguridad de la solución, como usar los servidores IAS para la autenticación de acceso remoto y con cable, crear WLAN de invitado para visitantes e implementar WLAN en

entornos muy pequeños, como oficinas en casa.

Opciones de seguridad para la WEP dinámica

La sección anterior, "Funcionamiento de 802.1X con PEAP y contraseñas", trata del uso del cifrado de la WEP dinámica en esta solución. La seguridad de la WEP dinámica se basa en su capacidad para renovar las claves de cifrado de manera periódica y, de este modo, frustrar ataques conocidos en el protocolo de WEP. IAS garantiza que las claves de cada uno de los clientes inalámbricos se van a renovar en un intervalo establecido mediante el tiempo de espera de la sesión del cliente, que obliga al cliente a volver a autenticarse en la WLAN.

La reducción del valor del tiempo de espera de sesión aumenta la seguridad, pero, al mismo tiempo, puede mermar la confiabilidad y el rendimiento. Un tiempo de espera de 60 minutos proporciona la seguridad apropiada en la mayoría de las circunstancias y, por supuesto, también para las redes 802.11b de 11 Mbps. Por lo general, los clientes inalámbricos nunca van a transferir datos suficientes en 60 minutos como para permitir que un atacante obtenga la clave WEP.

Las últimas investigaciones arrojan que las claves WEP estáticas pueden obtenerse mediante la captura de entre 1 y 5 millones de paquetes de red cifrados con la misma clave. Esto se recoge en el documento técnico "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP" de Adam Stubblefield, John Ioannidis y Aviel D. Rubin de AT&T Labs, consulte las referencias al final de este capítulo.

Nota: la cifra de 1 millón de paquetes se ha obtenido de la comprobación de WLAN de WEP usando claves relativamente débiles (una "frase fácil de memorizar") y, por lo tanto, no se puede aplicar directamente a las WLAN de WEP dinámica. Al contrario de lo que sucede con las WLAN de WEP estática, la WEP dinámica emplea claves de cifrado aleatorio seguras y resta gran parte de la eficacia de las optimizaciones de clave que los autores utilizan. De todas formas, acostúmbrese a equivocarse como hábito de seguridad y a usar la cifra de 1 millón de paquetes para evaluar la amenaza sobre la seguridad en las WLAN de WEP dinámica.

Un millón de paquetes normalmente equivalen a alrededor de 500 MB de datos (suponiendo que el tamaño medio de un paquete sea de 500 bytes). A fin de que los datos cifrados estén protegidos, el tiempo de espera de sesión habrá de establecerse de manera que obligue a renovar la clave del cliente antes de que se envíe una cantidad de datos superior a la indicada.

En cuanto al uso típico de la red por parte del cliente (como correo electrónico, explorar el Web o compartir archivos), la media de velocidad de transferencia de archivos es de 160 Kbps o inferior. A esta velocidad, y suponiendo que el tamaño de un paquete es de 500 bytes, un atacante tardaría aproximadamente 7 horas en acumular la información suficiente como para dar con la clave de cifrado actual del cliente.

Nota: en el entorno de un laboratorio, se invertiría mucho menos de 7 horas en transferir 500 Mb (unos 10 minutos en una red WLAN a 11 Mbps o menos de 3 minutos en una WLAN a 54 Mbps). Sin embargo, aquí se da por hecho que un solo cliente disfruta de uso exclusivo de la WLAN y transfiere paquetes UDP o autorizados en una dirección, situación que difícilmente se produciría en una WLAN del mundo real.

Un tiempo de espera de sesión de 60 minutos es más que suficiente para la mayoría de las organizaciones. Esto indica que un cliente transferiría un promedio de 150.000 paquetes antes de que cada clave se actualizara; es decir, un pedido de aproximadamente una magnitud inferior al umbral de 1 millón de paquetes necesario para hacerse con la clave WEP. No obstante, es posible que quiera disfrutar de un valor de tiempo de espera más breve por una o varias de las siguientes razones:

- Si tiene clientes inalámbricos que envían o reciben grandes cantidades de datos a través de la WLAN en períodos de tiempo relativamente cortos, debería establecer un tiempo de espera con una duración menor que el tiempo que tarda un solo cliente en enviar y recibir 75 MB (que corresponde a menos del 20 por ciento de la cantidad de datos necesaria para conseguir la clave WEP, por lo que el margen de seguridad es amplio).
- Si utiliza WLAN 802.11a o WLAN 802.11g de 54 Mbps, resulta más fácil transferir un mayor número de paquetes en un tiempo determinado. En este tipo de WLAN de mayor velocidad, es posible que desee reducir el tiempo de espera de sesión a 15 minutos.
- Si las técnicas para descifrar la clave WEP mejoran de manera muy considerable, la cantidad de datos necesaria para obtener las claves WEP será menor. Así, si surge una nueva técnica analítica de cifrados que

permite obtener claves con tan solo 100.000 paquetes, deberá reducir el tiempo de espera de sesión a fin de evitar que los clientes inalámbricos alcancen este límite antes de que las claves de cifrado se renueven.

- Si tiene necesidades de seguridad de especialista, posiblemente quiera establecer este tiempo por debajo del umbral en el que incluso los ataques teóricos de WEP serían fructíferos (10 minutos o 3 minutos, tal y como se ha señalado en la nota anterior). De todas formas, medite esta decisión teniendo presente las salvedades expuestas más adelante en esta sección. En caso de que los datos sean lo suficientemente confidenciales como para fijar este nivel de precaución, debería considerar seriamente el uso exclusivo de la protección de datos WPA en la WLAN y usar la seguridad IP como ayuda para la protección de los datos cuando fluyen por las LAN con cable.

Existen principalmente dos inconvenientes a la hora de reducir el tiempo de espera de sesión:

- **Peor confiabilidad de la WLAN:** un tiempo de espera de sesión en WLAN de escasa duración podría provocar errores en la reautenticación y la desconexión de la propia red en caso de que la comunicación con un controlador de dominio o un servidor IAS se perdiera de manera temporal.
- **Aumento de la carga en los servidores IAS:** cuanto más breve sea el tiempo de espera, más veces tendrá que volver a autenticarse el usuario con un servidor IAS y un controlador de dominio, de manera que la carga en éstos incrementará. Dado que IAS almacena en caché las sesiones de autenticación del cliente, normalmente este aumento de la carga será significativo sólo en aquellas organizaciones con un gran número de clientes inalámbricos o al utilizar valores de tiempo de espera de sesión de muy poca duración.

Otros servicios de acceso a la red

El diseño de RADIUS utilizado en esta solución puede proporcionar servicios de autenticación, autorización y contabilidad para otros servidores de acceso a la red como la autenticación de red 802.1X con cable y la autenticación de acceso remoto y VPN.

Autenticación de red por cable 802.1X

La autenticación de red por cable 802.1X constituye la aplicación más sencilla que no precisa modificación alguna del diseño básico de RADIUS. Es posible que las organizaciones que tienen una infraestructura de red por cable de amplia distribución encuentren difícil controlar el uso no autorizado de la red corporativa. Por ejemplo, normalmente es difícil impedir que los visitantes conecten equipos portátiles o que los empleados agreguen equipos no autorizados a la red. Algunas secciones de la red, como los centros de datos, pueden tener designadas zonas de alta seguridad, de manera que sólo los dispositivos autorizados deben admitirse en estas redes. Esto supondría la exclusión, si procediera, de empleados con equipos corporativos.

En la siguiente figura se ilustra cómo una solución de acceso a red por cable se integraría con el diseño.

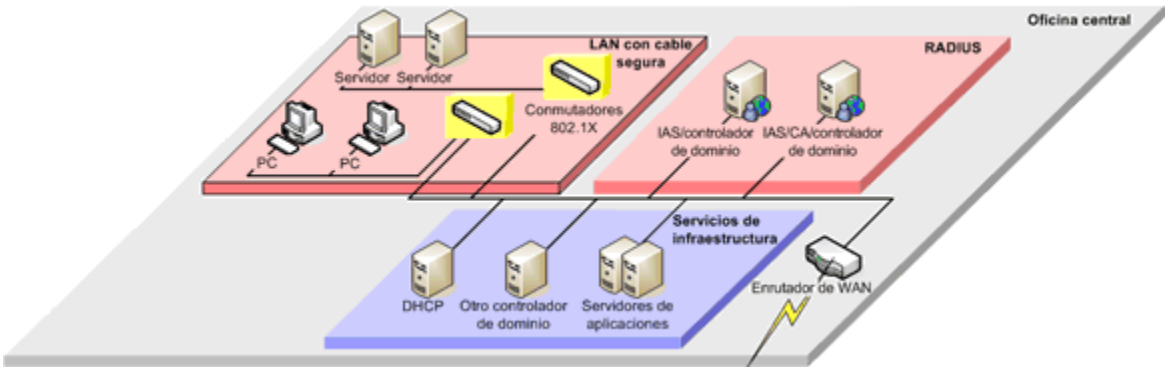

Figura 2.8. Uso de la autenticación por cable 802.1X
Vista de imagen a pantalla completa

El cuadro con los bordes resaltados representa los componentes por cable 802.1X, mientras que los otros contienen los servicios relevantes. Compare esta figura con la figura 2.4. En esta figura sólo se muestra la oficina central.

Los conmutadores de red que admiten 802.1X tienen una función idéntica a los puntos de acceso inalámbrico en la solución principal y pueden utilizar la misma infraestructura de RADIUS para autenticar clientes y autorizar selectivamente el acceso al segmento de red correspondiente. Esto proporciona las ventajas obvias de centralizar la administración de cuentas en el directorio corporativo, pero manteniendo las directivas de acceso a la red bajo el control del administrador de seguridad de la red.

Autenticación de VPN y acceso telefónico remoto

Otro servicio de acceso a la red que podría utilizar los componentes RADIUS es la VPN y el acceso telefónico remoto. Es probable que, particularmente en las organizaciones grandes, sea necesario agregar algunos elementos al diseño original, como servidores proxy RADIUS. La siguiente figura refleja la solución ampliada.

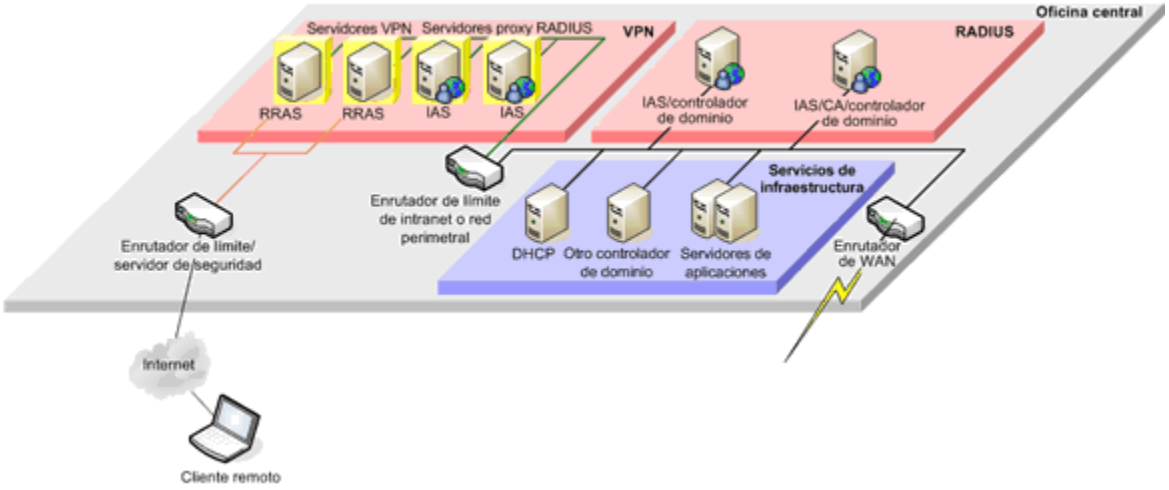

Figura 2.9. Extensión del componente RADIUS para admitir VPN
Vista de imagen a pantalla completa

Los servidores VPN de esta variante cumplen la misma función que los puntos de acceso inalámbrico en el diseño principal: pasar las solicitudes de autenticación de los clientes a la infraestructura de RADIUS. Las solicitudes de RADIUS se pueden pasar directamente a los servidores IAS internos. No obstante, muchas organizaciones optan por agregar un nivel adicional de servidores proxy RADIUS para que proporcione un nivel de seguridad extra y para que las solicitudes se enruten a los servidores IAS internos.

En lo que se refiere a la seguridad de la red con cable, esta solución aporta las mismas ventajas de reutilización de la infraestructura existente y de centralización de la administración de cuentas. Existen otras mejoras, como el uso de la autenticación de usuarios basada en tarjetas inteligentes. La solución de VPN de acceso remoto interna de Microsoft para el propio personal de la empresa utiliza virtualmente la misma VPN y la misma arquitectura de RADIUS con tarjetas inteligentes para la autenticación de usuarios.

El acceso telefónico remoto funciona de manera similar mediante la utilización de la capacidad de servidor de acceso telefónico en lugar de las funciones de VPN del Servicio de enrutamiento y acceso remoto de Windows.

La principal ventaja que el uso de IAS ofrece a VPN y al acceso remoto consiste en la capacidad para utilizar la característica de control de cuarentena para acceso a la red de Windows Server 2003. El control de la cuarentena emplea capacidades de los servidores de enrutamiento y acceso remoto (RAS) y del cliente de acceso remoto mejorado de Windows (Connection Manager) para permitir y denegar el acceso en función del estado de seguridad del equipo cliente. Esto se lleva a cabo realizando comprobaciones en el cliente cuando éste se conecta, y así, para garantizar que dispone de un software antivirus actualizado o que utiliza una versión aprobada del sistema operativo corporativo. En caso de que el cliente no supere estas comprobaciones, el servidor RADIUS le denegará el acceso a la red. Por eso, se puede denegar el acceso a un usuario y un equipo autorizados adecuadamente si representan una amenaza de seguridad para la red de la compañía.

Para obtener más información sobre la característica de cuarentena de Windows Server 2003, consulte las referencias al final de este capítulo.

Inicio de equipos cliente

La mayoría de los equipos con capacidades inalámbricas cuentan también con una interfaz de red con cable, dado que así se facilita en cierta medida que los clientes puedan unirse al dominio y descarguen la configuración de WLAN antes de conectarse a ésta. Sin embargo, no siempre va a producirse esta situación. Ya existen dispositivos de mano que son inalámbricos en su totalidad y, por lo tanto, no tienen adaptadores de red con cable. Esto supone el inconveniente de iniciar un cliente antes de que se conecte a la WLAN, por cuanto no posee la configuración ni las credenciales necesarias para conectarse a ella.

Este problema se agrava si en una organización decide usarse la seguridad 802.1X tanto inalámbrica como con cable, ya que un cliente no puede conectarse a una LAN con cable sin poseer las credenciales y la configuración pertinentes.

Existen dos enfoques fundamentales para iniciar un equipo cliente si no se puede usar una LAN con cable para obtener la configuración y credenciales:

- Uso de una LAN de invitado y de otra conexión autenticada (por ejemplo, una conexión de VPN) para obtener las credenciales y la configuración.
- Configuración manual de los clientes.

Actualmente, Microsoft sólo admite la segunda opción, si bien va a lanzar un servicio de disposición inalámbrica que permitirá el uso de una WLAN "de invitado" con la que iniciar la configuración de la WLAN del equipo cliente. Hasta entonces, la configuración manual constituye un modo sencillo de llevar esto a cabo. Para configurar el equipo cliente y unirlo al dominio, la persona responsable de ello debe pertenecer al grupo Administradores local del equipo.

Para iniciar un equipo mediante la configuración manual:

1. Configure manualmente la WLAN para el SSID de WLAN correspondiente.
2. Conecte la WLAN utilizando credenciales de dominio de usuario válidas. No podrá conectarse mediante la cuenta de equipo hasta que el equipo no se haya unido al dominio.
3. Una el equipo al dominio y, a continuación, reinícielo.
4. Tras ello, el cliente podrá conectarse a la WLAN usando la cuenta de equipo y, por lo tanto, podrá descargar la configuración del objeto de directiva de grupo de la WLAN. Esta configuración simplemente se sobrescribirá sobre la ya establecida manualmente.
5. Llegado este momento, tanto el usuario como el equipo podrán conectarse a la WLAN.

Entorno SOHO

Puede que tenga que implementar las WLAN en ubicaciones donde no es posible (o no resulta práctico) autenticar usuarios por medio de la infraestructura de IAS; así, por ejemplo, en oficinas domésticas de aquellos usuarios que trabajan habitualmente en casa, o bien en oficinas pequeñas con una conectividad a la red corporativa principal baja y poco confiable.

Antes, la única salida a esto consistía en configurar la seguridad de WEP estática y cruzar los dedos para que nadie pusiera demasiado empeño en atacar la WLAN. Por ello, una solución mucho más eficaz consiste en usar WPA en modo de infraestructura de claves públicas. Todos los puntos de acceso inalámbrico con certificado Wi-Fi llevan ahora incorporada la seguridad WPA, si bien es probable que algunos puntos de acceso más antiguos no sean compatibles con ella. Debe asegurarse de que los puntos de acceso son compatibles con WPA de clave previamente compartida por el valor de seguridad adicional que ésta ofrece. Al contrario de lo que sucede con WEP, la clave de autenticación de WPA no puede obtenerse del tráfico cifrado; en consecuencia, resultará mucho más difícil para un atacante irrumpir en la red. Asimismo, deberá garantizar que los usuarios cuentan con los conocimientos necesarios para utilizar claves de WPA seguras y para cambiarlas de manera periódica y, al mismo tiempo, asegurarse de que son conscientes de las implicaciones de seguridad que esto conlleva. Para implementar WPA de clave previamente compartida, necesita un punto de acceso inalámbrico, adaptadores de red inalámbricos y un sistema operativo cliente (como Windows XP) que sea compatible con WPA. No es

necesario tener un servidor RADIUS o cualquier otro tipo de infraestructura de servidores.

Principio de la página

Resumen

Este capítulo ha comenzado con una descripción del modo en que la seguridad en las LAN inalámbricas 802.1X funciona. En aras de centrarse en el diseño, se ha proporcionado una imagen de la organización de destino para la solución, así como los criterios de diseño clave de la organización para la solución de WLAN. A partir de estos elementos, se ha pasado a tratar los aspectos principales del diseño de WLAN escogido. Este diseño ha incluido la red, la colocación del servidor IAS y la configuración de IAS, el uso de certificados y los distintos tipos de clientes inalámbricos. Asimismo, se han expuesto los puntos clave de la migración desde una WLAN existente.

En las dos últimas secciones al final del capítulo se han recogido las variaciones más relevantes que pueden darse en el diseño básico de la solución. Primero, se ha descrito el modo de dotar a la solución de escalabilidad para organizaciones más grandes, junto con instrucciones sobre el modo de afrontar los principales puntos de divergencia de la solución central; Tras ello, se han incluido ilustraciones sobre el modo de usar la misma infraestructura de autenticación básica para admitir otros servicios de red como el acceso remoto, VPN y la seguridad de red con cable, y, por último, se ha detallado el modo de solucionar problemas bastante incómodos de inicio de clientes y de implementación de WLAN en entornos SOHO.

El capítulo siguiente comienza con la implementación de la solución a través de la preparación de la red, Active Directory, y la seguridad de servidores para implementar componentes de WLAN.

Principio de la página

Referencias

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

- Para obtener más detalles sobre la autenticación 802.1X, consulte "IEEE 802.1X Authentication for Wireless Connections" en la siguiente dirección URL:

  http://www.microsoft.com/technet/columns/cableguy/cg0402.mspx

- Para obtener más información sobre el modo en que PEAP funciona con contraseñas, consulte "PEAP with MS-CHAP Version 2 for Secure Password-based Wireless Access" en la siguiente dirección URL:

  http://www.microsoft.com/technet/columns/cableguy/cg0702.mspx

- Para obtener información sobre la autenticación 802.1X, la interacción entre clientes, los puntos de acceso inalámbrico y los servidores RADIUS, así como recomendaciones relativas a las funciones que deberían ser compatibles con los puntos de acceso, consulte "Recommendations for IEEE 802.11 Access Points" en la siguiente dirección URL:

  http://www.microsoft.com/whdc/hwdev/tech/network/802x/AccessPts.mspx

- Para obtener más información sobre el diseño de la LAN inalámbrica, incluidos los servicios DHCP y la distribución de los puntos de distribución, consulte el capítulo sobre la implementación de una LAN inalámbrica del *Kit de distribución de Microsoft Windows Server 2003* en la siguiente dirección URL:

  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/deployguide/DNSBM_WIR_OVERVIEW.mspx

- Para obtener más información sobre la protección de IAS, consulte la documentación de producto de Windows Server 2003 en la siguiente dirección URL:

  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/sag_ias_security.mspx

- Para obtener más información sobre las características de Servicios de Certificate Server disponibles en la

versión Enterprise Edition de Windows Server 2003, consulte el documento "PKI Enhancements in Windows XP Professional and Windows Server 2003" en la siguiente dirección URL:

http://www.microsoft.com/technet/prodtechnol/winxppro/plan/pkienh.mspx

Nota: la redacción de este artículo se realizó antes del lanzamiento de Windows Server 2003, de manera que en él se hace uso de los términos Windows .Net Server, Advanced Server y Standard Server donde debería decirse Windows Server 2003, Enterprise Edition y Standard Edition respectivamente.

- Para obtener más información sobre Microsoft 802.1X Authentication Client para Windows 2000, consulte el artículo de la Knowledge Base "Using 802.1x Authentication on Computers Running Windows 2000" en la siguiente dirección URL:

  http://support.microsoft.com/default.aspx?scid=313664

- Para obtener más información sobre "Wi-Fi Protected Access (WPA) Overview" y la "Introducción a la actualización de seguridad de WPA inalámbrico en Windows XP", consulte las siguientes direcciones respectivamente:

  http://www.microsoft.com/technet/columns/cableguy/cg0303.mspx

  http://support.microsoft.com/default.aspx?scid=kb;es;815485

- Para conocer los asuntos de seguridad relacionados con WEP, consulte los documentos técnicos "Weaknesses in the Key Scheduling Algorithm of RC4" de Scott Fluhrer, Itsik Mantin y Adi Shamir y "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP" de Adam Stubblefield, John Ioannidis y Aviel D. Rubin. Tenga presente que en estos documentos se trata la seguridad de la WEP estática y que, por lo tanto, las conclusiones que en ellos se arrojan no son directamente aplicables a las WLAN de WEP dinámica. Para el primer documento, consulte la siguiente dirección:

  http://www.crypto.com/papers/others/rc4_ksaproc.pdf

- Para el segundo documento, consulte la siguiente dirección:

  http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf

- Para obtener más información sobre la implementación de LAN inalámbricas y VPN de acceso remoto en Microsoft, consulte "Mobility: Empowering People through Wireless Networks" y "Securing Remote Users at Microsoft" en las siguientes direcciones:

  http://www.microsoft.com/technet/itsolutions/msit/security/secwlan.mspx

  http://www.microsoft.com/resources/casestudies/casestudy.asp?casestudyid=13787

- Para obtener más información sobre el control de cuarentena para acceso a la red, consulte los documentos "Network Access Quarantine Control in Windows Server 2003" y "Planning for Network Access Quarantine Control" en las siguientes direcciones:

  http://support.microsoft.com/default.aspx?scid=818747

  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/deployguide/dnsbf_vpn_aosh.mspx

- Para obtener más información sobre el uso de WPA para proteger las WLAN en entornos SOHO, consulte "WPA Wireless Security for Home Networks" en la siguiente dirección URL:

  http://www.microsoft.com/WindowsXP/expertzone/columns/bowman/03july28.asp

(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