Latinoamérica

Microsoft TechNet

Capítulo 3: Arquitectura de la solución de LAN inalámbrica segura

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

En esta página

Introducción

El capítulo anterior mostraba las opciones de seguridad de WLAN y describía las razones por las que se seleccionó la autenticación inalámbrica de 802.1X con el protocolo EAP-TLS para esta solución. Este capítulo ofrece una descripción de la arquitectura de la solución y, seguidamente, se genera un diseño lógico a partir de los criterios de diseño tomados de una organización de ejemplo. Puede utilizar esta información como base para implementar su solución. El diseño lógico utiliza hardware de red WLAN 802.1X, autenticación de RADIUS y PKI.

Requisitos previos

Le será útil conocer los conceptos de diseño de infraestructuras de TI y estar familiarizado con los componentes clave que forman parte de dicho diseño. Los componentes clave son los siguientes: WLAN y componentes de red, RADIUS, el servicio de directorio Active Directory® y PKI. No se necesita un conocimiento profundo de estos componentes.

Descripción general del capítulo

Los objetivos de este capítulo son los siguientes:

- proporcionar una descripción conceptual del funcionamiento de una solución de WLAN segura basada en los protocolos 802.1X y EAP-TLS, así como de los componentes principales de este tipo de solución.
- definir los criterios de diseño de la solución para el diseño lógico y las fases posteriores del diseño técnico detallado.
- producir un diseño lógico coherente que constituya la base para el diseño detallado en los capítulos siguientes.
- explicar la forma en que puede modificarse la solución para cumplir los requisitos de organizaciones de diferentes tamaños.
- explicar en detalle algunas de las formas en que puede ampliarse el diseño propuesto o utilizarse como base para generar otras soluciones de acceso de red (por ejemplo, redes privadas virtuales y control de acceso a redes por cable) y examinar el modo en que el componente PKI del diseño puede servir de punto de partida para varias aplicaciones de seguridad.

En los capítulos siguientes examinaremos el proceso de diseño detallado para cada uno de los componentes principales del diseño lógico (WLAN, RADIUS y PKI) como preparación para generar y poner la solución en funcionamiento.

Principio de la página

Diseño conceptual

Como se mencionó en el capítulo anterior, hay diversos puntos débiles graves en la seguridad inherentes a las redes inalámbricas. En el mejor de los casos, estos puntos débiles se solucionan parcialmente mediante el uso de la privacidad equivalente por cable (WEP, Wired Equivalent Privacy), como se especifica en el estándar 802.11 del IEEE. La solución propuesta en esta guía se ocupa del problema de cómo mejorar la seguridad de las comunicaciones mediante redes inalámbricas. La solución ideal necesita contar con las características siguientes:

- autenticación sólida de cliente inalámbrico. Esto debe incluir la autenticación mutua del cliente, el punto de acceso (PA) inalámbrico y el servidor RADIUS.
- un proceso de autorización para determinar quién tendrá o no tendrá acceso a la red inalámbrica.
- control de acceso que solamente permita el acceso de red a clientes autorizados.
- cifrado eficaz del tráfico de la red inalámbrica.
- Una administración segura de las claves de cifrado.
- Una resistencia a los ataques de denegación de servicio (DoS).

El estándar del protocolo 802.1X para control de acceso a la red, en combinación con un método de autenticación segura como EAP-TLS, cumple con algunos de estos requisitos. La WEP de alta potencia brinda un cifrado seguro del tráfico de red pero ofrece un nivel de administración de claves deficiente. Los métodos para administrar claves de cifrado WEP inherentes a 802.1X y EAP son mucho más seguros que lo permitido por los estándares básicos de 802.11. El estándar de acceso protegido WiFi (WPA, WiFi Protected Access) es un grupo de normas basadas en el sector que incluye 802.1X y EAP (entre otras mejoras) y un protocolo estandarizado para la administración de claves conocido como Protocolo de integridad de claves temporales (TKIP, Temporal Key Integrity Protocol). El estándar WPA representa un paso considerable hacia la seguridad de WLAN y cuenta con el respaldo de la mayoría de los analistas y proveedores.

Nota: ninguna de las mejoras de WPA se ocupa de los problemas de denegación de servicio inherentes a 802.11 y 802.1X. Estas debilidades no representan un problema tan grave como los otros fallos de WEP, y la mayoría de los ataques de denegación de servicio demostrados causan únicamente una disrupción temporal en la red. Sin embargo, la amenaza de los ataques de denegación de servicio continúa siendo un tema preocupante para algunas empresas. La solución debería estar disponible tras la publicación del estándar IEEE 802.11i.

Aunque la compatibilidad con WPA ya está bastante extendida, todavía hay muchos dispositivos y sistemas incapaces de acomodar este estándar. Por esta razón, la solución en esta guía está diseñada para funcionar con WPA y WEP dinámica. La mayoría de los proveedores de hardware de red venden productos compatibles con 802.1X con claves WEP dinámicas y WPA. La finalidad de este capítulo ofrece la posibilidad de tratar los dos métodos indistintamente; el uso de uno u otro no influye significativamente en el diseño.

La figura siguiente muestra un diagrama conceptual de la solución (autenticación de 802.1X EAP-TLS).

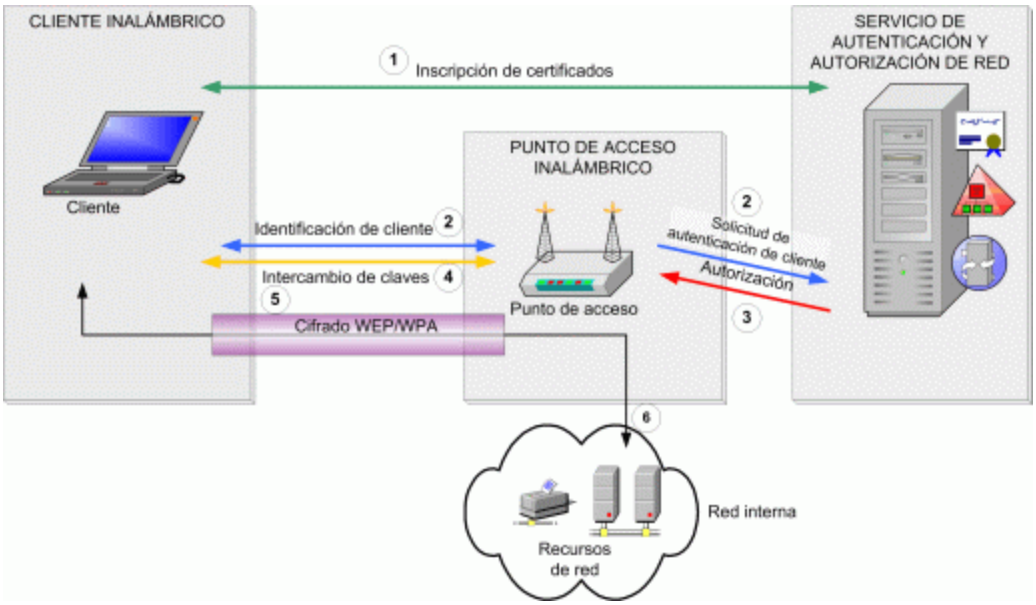

Figura 3.1 Concepto de la solución basado en la autenticación de 802.1X EAP-TLS
Ver imagen a tamaño completo

El diagrama muestra cuatro componentes principales:

- **El cliente inalámbrico**. Se trata de un equipo o dispositivo que ejecuta una aplicación que requiere acceso a los recursos de red. El cliente tiene la capacidad de cifrar su tráfico de red, además de guardar e intercambiar credenciales de manera segura (como claves o contraseñas).
- **El PA inalámbrico**. En términos de redes más generales se conoce como "servicio de acceso a la red" (NAS, Network Access Service) pero en los estándares inalámbricos se hace referencia a este componente como "AP" o "punto de acceso". El punto de acceso inalámbrico implementa funciones de control de acceso para permitir o denegar el acceso a la red y ofrece la capacidad de cifrar el tráfico inalámbrico. También cuenta con los medios para intercambiar claves de cifrado de manera segura con el cliente a fin de asegurar el tráfico de red. Finalmente, puede consultar un servicio de autenticación y autorización para tomar decisiones de autorización.
- **servicio de autenticación (AS, Authentication Service).** Guarda y comprueba las credenciales de los usuarios válidos y toma decisiones de autorización basándose en una directiva de acceso. También puede recopilar información contable y de auditoría sobre el acceso de los clientes a la red. El servidor RADIUS es el componente principal de este servicio pero el directorio y la entidad emisora también contribuyen a esta función.
- **La red interna**. Se trata de un área segura de servicios conectados a la red a los que la aplicación cliente inalámbrica debe obtener acceso.

Los números del diagrama ilustran el proceso de acceso a la red, que se describe con más detalle en los pasos siguientes:

1. El cliente inalámbrico debe establecer credenciales con el servicio de autenticación antes de que se establezca el acceso a la red inalámbrica. (Esto podría realizarse con algunos medios fuera de banda como, por ejemplo, mediante un intercambio de disquetes, o bien podría realizarse en una red segura por cable o de otro tipo.)
2. Cuando se encuentra al alcance del punto de acceso inalámbrico, el equipo cliente intenta conectarse a la WLAN activa en el punto de acceso. Para su identificación, la WLAN cuenta con un identificador del conjunto de servicios (SSID, Service Set Identifier). El cliente detecta el SSID de la WLAN y lo usa para determinar la configuración correcta y el tipo de credencial que debe utilizarse para esta WLAN

específica.

El punto de acceso inalámbrico se configura para permitir únicamente conexiones seguras (autenticadas de 802.1X). Cuando el cliente intenta conectarse a él, el punto de acceso envía un desafío al cliente. A continuación, el punto de acceso configura un canal restringido que permite al cliente comunicarse sólo con el servidor RADIUS. Este canal bloquea el acceso al resto de la red. El servidor RADIUS solamente aceptará una conexión de un punto de acceso inalámbrico de confianza o de uno que haya sido configurado como cliente RADIUS en el servicio de autenticación de Internet (IAS, Internet Authentication Service) de Microsoft y que proporcione el secreto compartido para dicho cliente RADIUS.

El cliente intenta realizar la autenticación con el servidor RADIUS a través del canal restringido por medio de 802.1X. Como parte de la negociación EAP-TLS, el cliente establece una sesión de seguridad de la capa de transporte (TLS, Transport Layer Security) con el servidor RADIUS. El uso de una sesión de TLS tiene las finalidades siguientes:

- permite al cliente llevar a cabo la autenticación del servidor RADIUS, lo que significa que el cliente solamente establecerá la sesión con un servidor que cuente con un certificado de confianza.
- permite al cliente suministrar sus credenciales de certificado al servidor RADIUS.
- protege el intercambio de autenticación frente a intrusiones contra paquetes.
- la negociación de la sesión de TLS genera una clave que el cliente y el servidor RADIUS pueden utilizar para establecer claves maestras comunes. Estas claves se usan para derivar las claves utilizadas en el cifrado de tráfico de WLAN.

Durante este intercambio, solamente el cliente y el servidor RADIUS pueden ver el tráfico en el túnel de TLS y no queda nunca expuesto al punto de acceso inalámbrico.

3. El servidor RADIUS valida las credenciales de cliente con el directorio. Si la autenticación del cliente se lleva a cabo de forma satisfactoria, el servidor RADIUS reunirá la información que le permitirá decidir si debe autorizarse el uso de la WLAN al cliente. Utiliza información del directorio (por ejemplo, sobre la pertenencia a grupos) y las restricciones definidas en su directiva de acceso (por ejemplo, los períodos de tiempo en que se permite el acceso a la WLAN) para conceder o denegar el acceso del cliente. Seguidamente, el servidor RADIUS transmite la decisión al punto de acceso.

4. Si se concede acceso al cliente, RADIUS transmitirá la clave maestra del cliente al punto de acceso inalámbrico. Con ello, el cliente y el punto de acceso comparten información de clave común que pueden utilizar para cifrar y descifrar el tráfico de WLAN que se desplaza entre ellos.

   Cuando se utiliza WEP dinámica para cifrar el tráfico, las claves maestras deben cambiarse periódicamente para evitar ataques de recuperación de claves WEP. El servidor RADIUS realiza este proceso de forma regular, lo que obliga al cliente a repetir la autenticación y generar un conjunto de claves nuevo.

   Si se utiliza WPA para proteger la comunicación, la información de la clave maestra se usa para derivar las claves de cifrado de datos, que cambian para cada paquete transmitido. WPA no necesita exigir la repetición frecuente de la autenticación para garantizar la seguridad de las claves.

5. A continuación, el punto de acceso establece la conexión de WLAN del cliente con la LAN interna, lo que ofrece al cliente un acceso sin restricciones a los sistemas de la red interna. Ahora, el tráfico transmitido entre el cliente y el punto de acceso está cifrado.

6. Si el cliente requiere una dirección IP, puede solicitar una concesión del protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol) de un servidor en la LAN. Tras la asignación de la dirección IP, el cliente puede empezar a intercambiar información con los sistemas en el resto de la red de forma normal.

La figura siguiente muestra este proceso en más detalle.

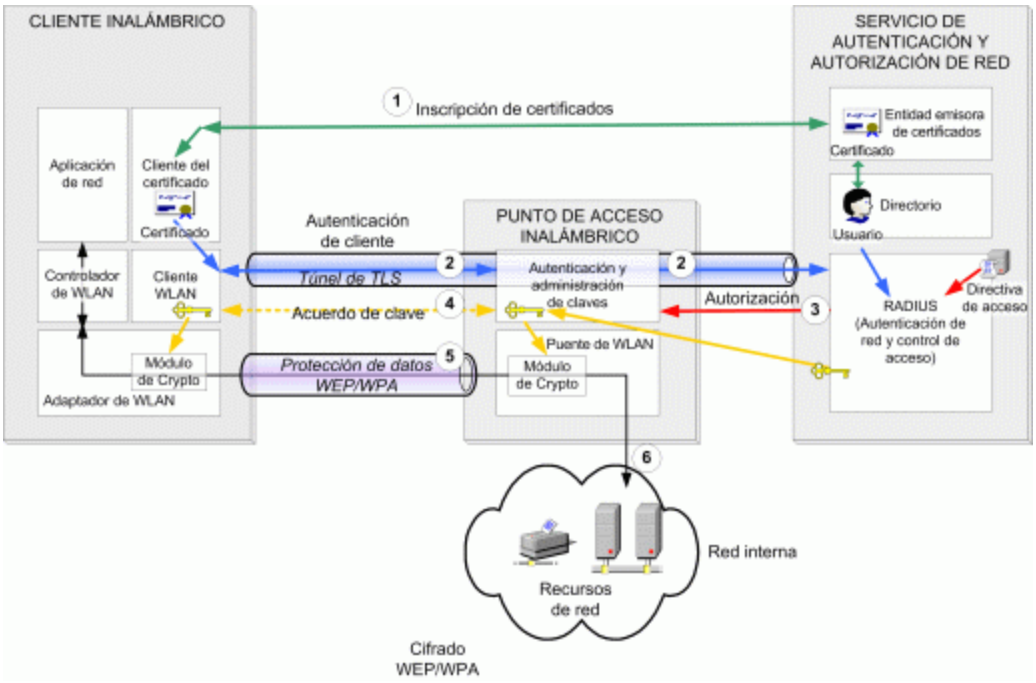

Figura 3.2 Proceso de acceso de 802.1X EAP-TLS
Ver imagen a tamaño completo

El diagrama muestra los componentes individuales de forma más detallada. En secciones posteriores de este capítulo regresaremos a este diagrama con explicaciones sobre diferentes aspectos del mismo. Por el momento, recuerde los subcomponentes del servicio de autenticación: la entidad emisora de certificados (CA), el directorio y el servidor RADIUS. Si bien conceptualmente estos subcomponentes llevan a cabo un conjunto de tareas relativamente simples, para hacerlo de manera segura, escalable, administrable y fiable, necesitan una infraestructura auxiliar muy sofisticada. La mayor parte de las tareas de planeamiento, implementación y administración requeridas para ello se explican con detalle en capítulos posteriores de esta guía.

Principio de la página

Criterios de diseño de soluciones

Una vez descritos los conceptos básicos de la solución, deben analizarse sus principales criterios de diseño. Éstos proporcionarán las pautas con las que el concepto de la solución se transformará en un diseño que pueda implementarse en una situación real.

Los criterios de diseño se han tomado de los requisitos de una organización típica en proceso de implementación de esta solución. Las secciones siguientes describen esta organización y sus principales requisitos técnicos.

Organización de destino

La descripción de la organización en esta sección sólo tiene la finalidad de proporcionar un contexto para los criterios de diseño. Al evaluar la utilidad de esta solución para su organización, procure centrarse en averiguar si los criterios de diseño pueden serle de utilidad, en lugar de intentar descubrir si su organización es exactamente igual a la que describimos aquí.

Es posible que la organización de destino haya implementado una WLAN en algunas ubicaciones para reducir los costos de infraestructura de la red y aumentar la movilidad y productividad del personal. La organización tiene una idea clara de sus necesidades de seguridad y ya ha implementado varias tecnologías para mejorar la seguridad de TI, por ejemplo, la autenticación de dominios, servidores de seguridad de Internet, programas de detección de virus y una solución VPN o de acceso remoto. Probablemente, tendrá planes a largo plazo para utilizar otras aplicaciones de alta seguridad, como el cifrado de archivos y el correo electrónico seguro.

El diseño de red lógico / físico simplificado de esta organización podría ser similar al definido en el diagrama

siguiente:

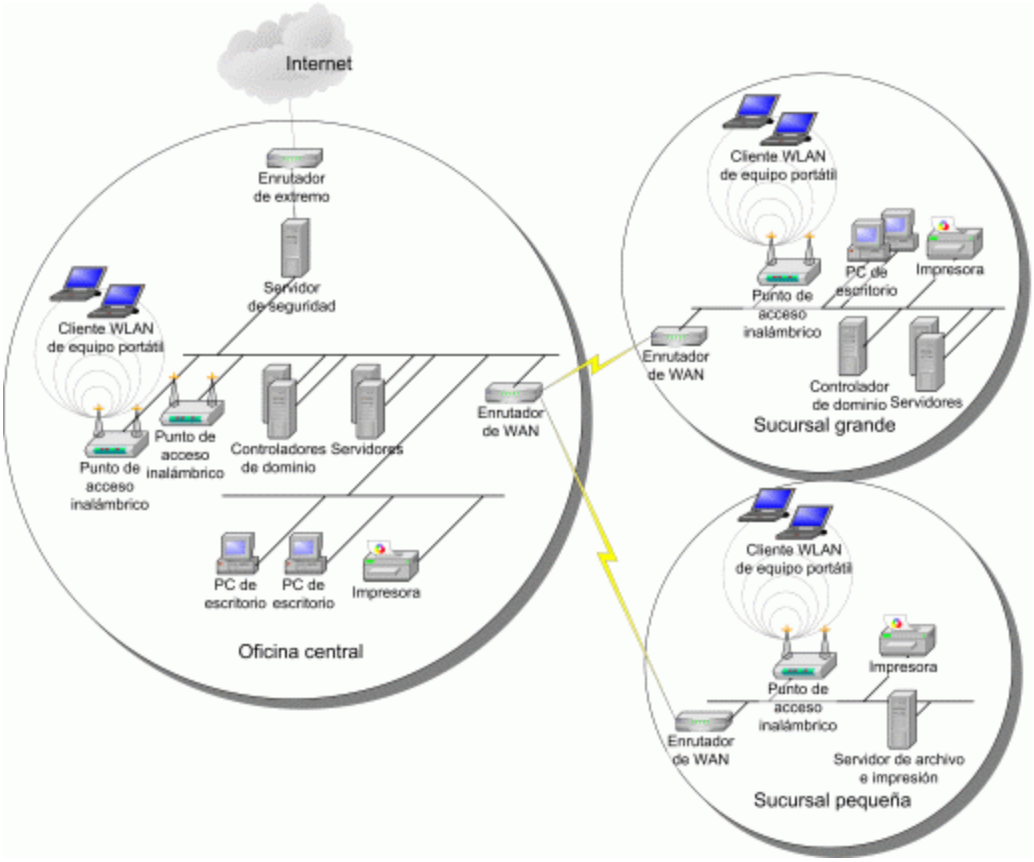

Figura 3.3 Esquema del diseño físico y de red de la organización de destino
Ver imagen a tamaño completo

Aunque la figura solamente incluye una oficina grande y una pequeña remota, en realidad podría haber varias de cada tipo. En virtud de la claridad, sólo se muestran algunos servidores y clientes. Este número reducido de hosts no tiene por qué ser representativo del tamaño de la organización.

Dentro de ciertos límites, el tamaño de la organización de destino tiene un efecto relativamente menor en los criterios de diseño de la solución. En el extremo inferior de la escala, es posible que la oficina central cuente con varios cientos de usuarios que trabajan con sucursales que incluyen a decenas de empleados. En el extremo superior de la escala, es posible que la oficina central tenga varios miles de empleados y las sucursales varios cientos. En ambos extremos de la escala, las organizaciones también suelen contar con oficinas más pequeñas y una cantidad menor de empleados.

Requisitos de la organización

Los requisitos siguientes suelen aplicarse al tipo de organización descrita en este escenario:

- la organización debe mejorar la seguridad de la WLAN para eliminar o reducir considerablemente las amenazas siguientes:
  - Intrusos que intercepten transmisiones de datos en la WLAN.
  - Intrusos que intercepten y modifiquen transmisiones de datos en la WLAN.
  - Intrusos u otros usuarios no autorizados que se conecten a la WLAN e introduzcan virus u otro tipo de código hostil en la red interna.
  - ataques de denegación de servicio a nivel de la red (en lugar de a nivel de radio).

- intrusos que utilizan la WLAN corporativa para obtener acceso a Internet.

- las medidas de seguridad no deben tener un impacto negativo en la capacidad de uso de la red y no deben dar lugar a un incremento significativo de las llamadas al servicio de asistencia.
- Los costos de implementación y administración continua deben ser lo suficientemente bajos como para ser justificables aunque solamente utilicen la solución de WLAN unos pocos usuarios (menos del 10% del personal).
- El diseño debe ser compatible con gran variedad de clientes y dispositivos.

Adicionalmente, suelen existir otros requisitos técnicos de naturaleza general:

- resistencia a errores de componente individual.
- posibilidad de escalabilidad para soportar niveles de uso superiores en el futuro, posiblemente de más del 100% del personal existente. El costo de la provisión de compatibilidad con números de usuarios cada vez mayores debería ser mínimo o, al menos, lo será en proporción a la ampliación requerida.
- posibilidad de reutilización de los componentes, siempre que sea posible. La solución debe reutilizar la infraestructura existente y los proyectos futuros deben poder reutilizar los nuevos componentes introducidos por la solución.
- la infraestructura de administración y supervisión existente debería poder acomodar la nueva solución sin dificultad.
- capacidad de recuperación en caso de errores graves (por ejemplo, mediante la restauración de copias de seguridad en hardware alternativo).
- cumplimiento de los protocolos y formatos de los estándares del sector. Donde no existan normas actuales, la solución debería instaurarse según estándares futuros.
- seguridad sólida (incluyendo una renovación regular) de las credenciales y las claves utilizadas en la solución.
- información de auditoría completa para la inscripción de usuarios y el acceso de clientes a la red.

Criterios de diseño de soluciones

A partir de estos requisitos, pueden determinarse los criterios de compatibilidad con el diseño de la solución en la tabla siguiente.

Tabla 3.1: Criterios de diseño de la solución

Factor de diseño	Criterios
Seguridad	–autenticación sólida de los clientes inalámbricos. –control de acceso que solamente permita el acceso de red a clientes autorizados. –cifrado eficaz del tráfico de red inalámbrica. –administración segura de las claves de cifrado. –resistencia a ataques de denegación de servicio.
Escalabilidad	Diseño básico con escalabilidad ascendente y descendente para abarcar un amplio espectro de tamaños de organización
–Número mínimo/máximo de usuarios admitidos	–de 500 a 15000 (o más) usuarios de WLAN. –de 500 a 15000 (o más) usuarios de certificados.

–Número de sitios admitidos	–múltiples sitios grandes, con controladores de dominio de autenticación locales y servicio de autenticación de Internet (IAS, Internet Authentication Service) de Microsoft, admitidos con resistencia a errores de red de área extensa (WAN, Wide Area Network). –múltiples sitios pequeños admitidos sin resistencia a errores de WAN.
Reutilización de componentes (uso de la infraestructura existente)	Utilización de Active Directory, servicios de red y clientes con Microsoft Windows® XP
Reutilización de componentes (capacidad de uso por parte de aplicaciones futuras)	–compatibilidad con otras aplicaciones de acceso a la red (acceso a red por cable 802.1X y VPN) mediante la infraestructura de autenticación. –compatibilidad con una amplia variedad de aplicaciones, como el sistema de archivos cifrados (EFS, Encrypting File System) y VPN, mediante PKI.
Disponibilidad	Resistencia a errores de componentes individuales o de vínculo de red
Extensibilidad	–extensible para admitir capacidad y normas futuras (por ejemplo, 802.11i, WPA y 802.11a para WLAN). –infraestructura de servicios de Certificate Server extensible para admitir la mayoría de los usos comunes de certificados de claves públicas (correo electrónico seguro, inicio de sesión con tarjeta inteligente, firma de código y Seguridad de servicio Web, entre otros).
Capacidad de administración	Integración con las soluciones de administración corporativa existentes (incluye la supervisión del sistema y del servicio, la creación de copias de seguridad, la administración de la configuración, etc.)
Estructura de la organización de TI	Favorece las TI centralizadas (departamento con un mínimo de cinco empleados y, normalmente, con 20 o 30 empleados de TI)
Cumplimiento de las normas	Cumplimiento de los principales estándares actuales y oferta de una ruta de migración clara a futuras normas importantes

Principio de la página

Diseño lógico de la solución

Esta sección describe el diseño lógico y lógico/físico de la solución. Esto implica la especificación y colocación de los componentes reales, aunque no incluye los detalles de diseño físicos, como la especificación del hardware del servidor.

Revisión del diseño conceptual

Mediante el uso de la figura siguiente (presentada anteriormente en este capítulo), esta sección examina el modo en que los componentes individuales se adaptan y agrupan para formar el diseño global.

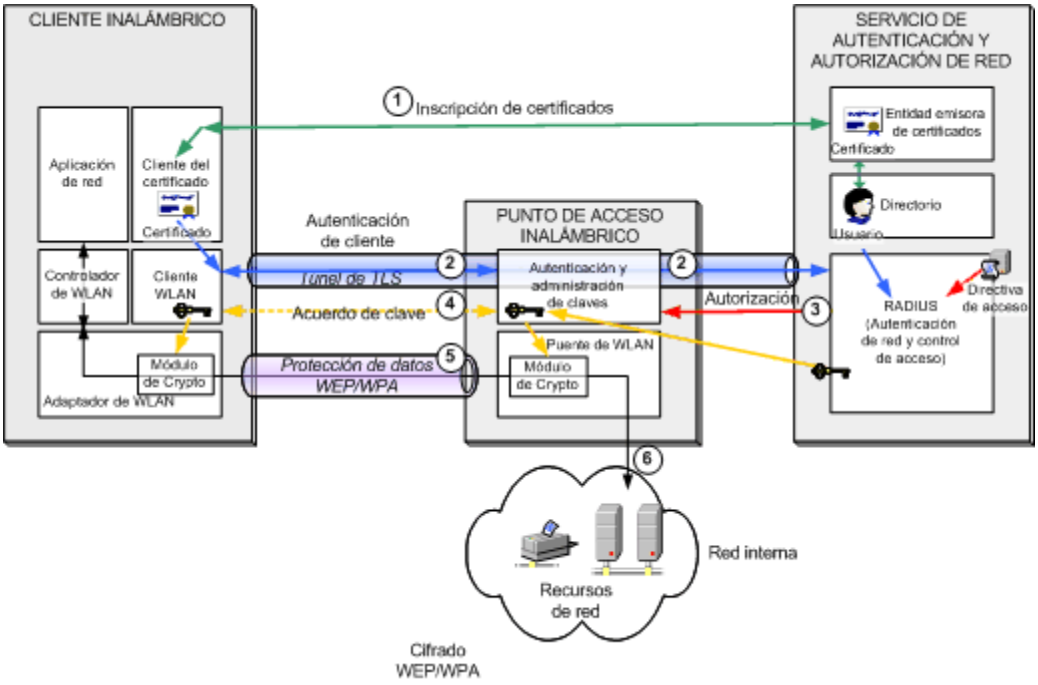

Figura 3.4 Vista conceptual del proceso de acceso a la red
Ver imagen a tamaño completo

Diseño lógico

La figura anterior dividía los componentes lógicos para facilitar la comprensión del proceso de acceso a la WLAN. Sin embargo, una ligera reagrupación de los componentes puede ayudar a simplificar los procesos de implementación y administración.

La agrupación de componentes elegida permite una visualización modular del diseño completo que permite una máxima reutilización de estos componentes. Por ejemplo, sería posible implementar el componente PKI únicamente como medio de autenticación de usuarios de WLAN. Sin embargo, esto podría limitar la reutilización del componente PKI para otras aplicaciones. De manera similar, el componente RADIUS debe diseñarse teniendo en cuenta otras aplicaciones que podrían requerirse en el futuro.

Los servicios de TI del diseño se agruparán en los siguientes grupos lógicos:

- Componentes WLAN: clientes y puntos de acceso inalámbricos
- Componente RADIUS
- Componente PKI: entidades emisoras de certificados
- Componente Servicios de infraestructura

Este último componente incluye un directorio y servicios de red auxiliares. Éstos se componen de servicios de TI que generalmente ya existían en la organización y con los que la solución interactúa de algún modo.

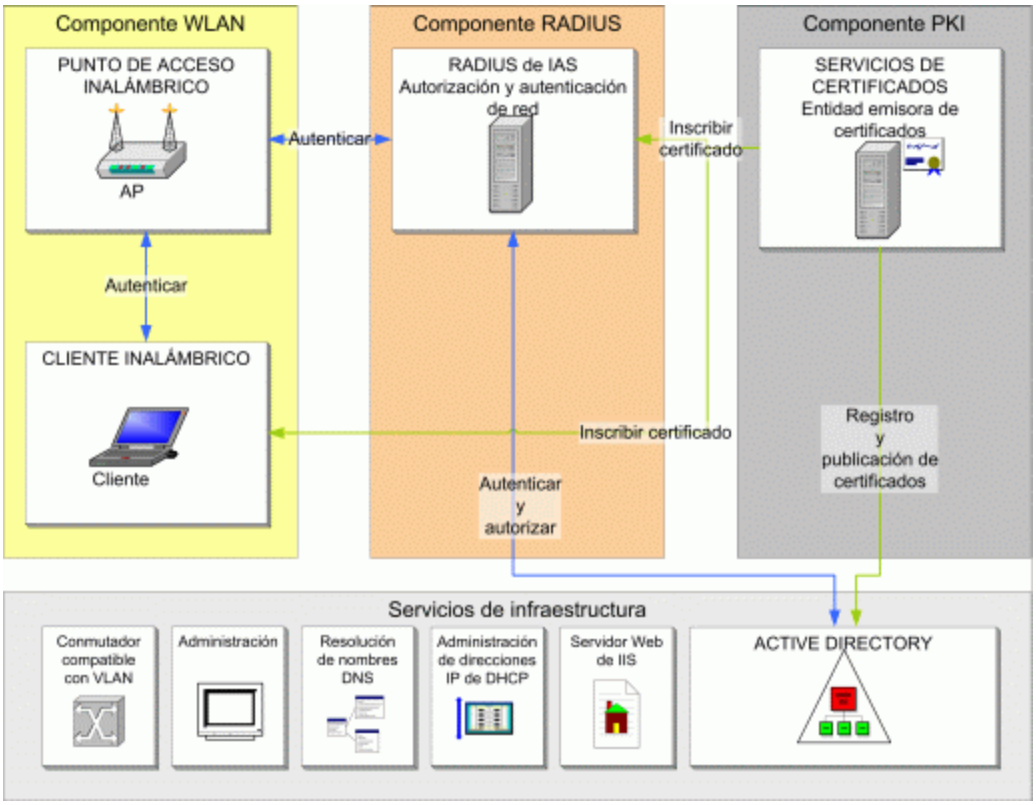

Figura 3.5 Diseño lógico de la solución de WLAN segura
Ver imagen a tamaño completo

Nivel lógico / físico

En el nivel lógico / físico, el diseño muestra cómo se implementarán estos componentes como servidores físicos, cómo se vincularán y cómo se distribuirán entre los diferentes sitios de la organización de destino. Sin embargo, el número de servidores que se muestran en la figura siguiente constituye una generalización. Nos ocuparemos de la definición final de la cantidad y la colocación de los servidores en capítulos de planeamiento posteriores de esta guía.

Oficina central

El diagrama siguiente ilustra la implementación de servidores en la oficina central. Sólo los tres componentes superiores representan los servidores o componentes nuevos que deben adquirirse. Los componentes de servicios de infraestructura generalmente estarán presentes de alguna manera en la mayoría de las organizaciones. Si la organización ya ha implementado un equipo de WLAN con capacidad para 802.1X, es posible que el componente WLAN ya exista.

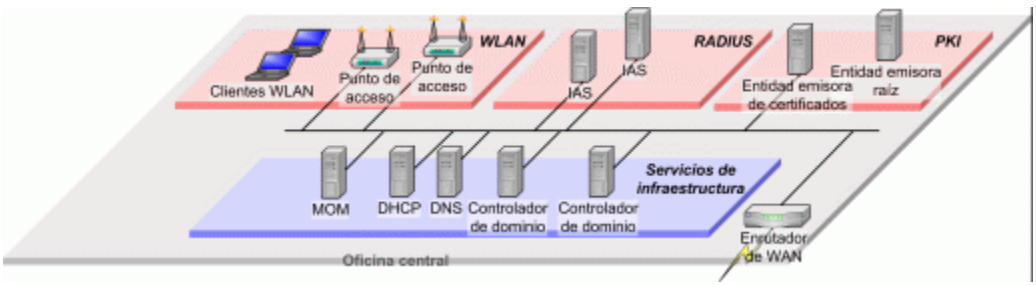

Figura 3.6 Implementación de servidores en la oficina central
Ver imagen a tamaño completo

Sucursal regional grande

El diagrama siguiente ilustra el diseño físico de una oficina más grande, que se distingue de una sucursal

pequeña por contar con un controlador de dominio local del sitio. Se implementa un único servidor IAS en la oficina remota. Aunque se describe como servidor individual, puede ejecutarse como servidor en el controlador de dominio.

Nota: si el vínculo WAN a la oficina central es fiable (es decir, si hay vínculos de red redundantes) y no se congestiona excesivamente, la sucursal grande podrá utilizar los servicios RADIUS de la oficina central en lugar de tener servicios propios. Este tema se analiza con mayor detalle en el capítulo 5, "Diseño de una infraestructura de RADIUS para la seguridad de LAN inalámbricas".

Todos los demás servicios (por ejemplo las entidades emisoras) son suministrados por la oficina central.

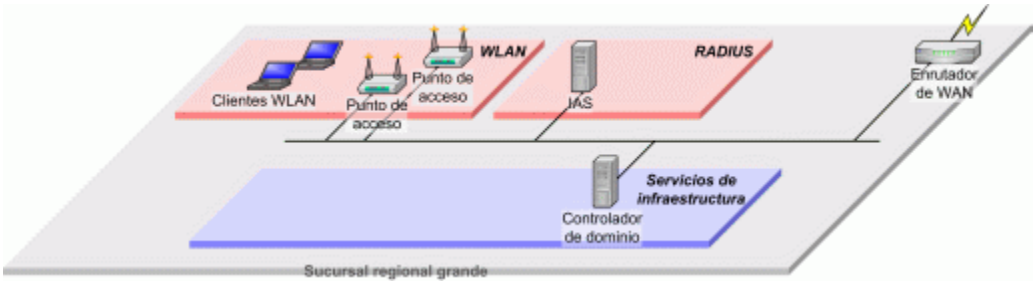

Figura 3.7 Diseño físico para una sucursal grande
Ver imagen a tamaño completo

Sucursal pequeña

Es posible que la sucursal pequeña cuente con cierta infraestructura de TI, como, por ejemplo, un servidor de archivos y una impresora, pero generalmente no dispondrá de una infraestructura de autenticación. Algunas organizaciones consideran que este tipo de oficina no requiere ni justifica el uso de servicios de WLAN. Sin embargo, se trata de una posibilidad atractiva para otras organizaciones que tienen la flexibilidad de utilizar oficinas temporales, ya que se elimina la necesidad de tender y administrar cables de red.

Si se necesitan servicios de WLAN en oficinas pequeñas que carecen de controlador de dominio, los puntos de acceso inalámbricos locales se basarán en la infraestructura de la autenticación de dominio y el servidor IAS de la oficina central. El problema principal de este enfoque radica en que si se produce un error en el vínculo WAN a la oficina central, se pierde toda conectividad con la WLAN. Aunque no existe una solución fácil para este escenario, puede ocuparse de esta vulnerabilidad (a cambio de un precio) mediante la provisión de redundancia de WAN o la implementación de controladores de dominio locales.

Si considera que la resistencia de WAN o la ubicación de controladores de dominio locales en las sucursales de su organización es demasiado cara, puede recurrir a la opción de implementar puntos de acceso inalámbricos aislados mediante el modo de clave previamente compartida de WPA. Ahora todos los puntos de acceso inalámbrico certificados por Wi-Fi son compatibles con WPA. Aunque es mucho más segura que WEP estática, esta opción conlleva una carga de administración adicional.

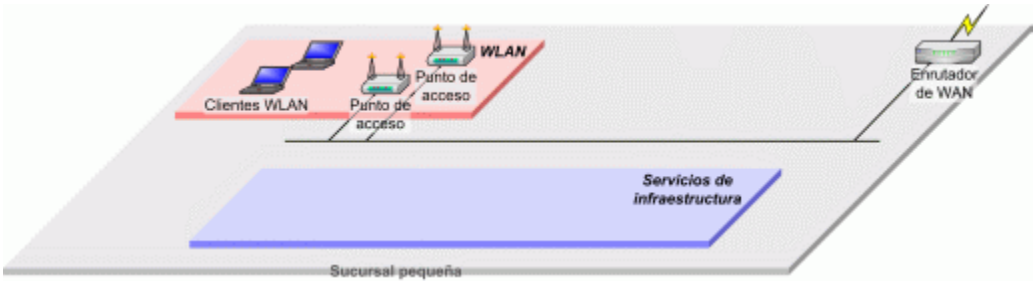

Figura 3.8 Diseño físico para una sucursal pequeña
Ver imagen a tamaño completo

Estrategia de escalabilidad

Uno de los principales criterios del diseño es la garantía de escalabilidad del mismo. La solución debe ser

compatible con una amplia gama de tamaños de implementación a un costo apropiado para cada uno. Por ejemplo, una implementación para 500 usuarios debería costar proporcionalmente menos que una implementación para 5000 usuarios. La complejidad de la implementación y administración también debe ser realista para esta gama de organizaciones.

Organización grande

El diagrama siguiente ilustra cómo puede escalarse el diseño en forma ascendente para abarcar una gran cantidad de usuarios en una oficina central y en oficinas regionales grandes. Probablemente, los servidores IAS también se utilizarán para otras aplicaciones de red, como VPN. Para obtener más información, consulte la sección "*Extensión del diseño*" incluida más adelante en este capítulo. Esta consideración podría influir en la cantidad y estructura precisa de los servidores. Los servidores IAS adicionales se muestran únicamente con fines ilustrativos.

Los servidores adicionales requeridos para la versión escalada de la solución se muestran sombreados.

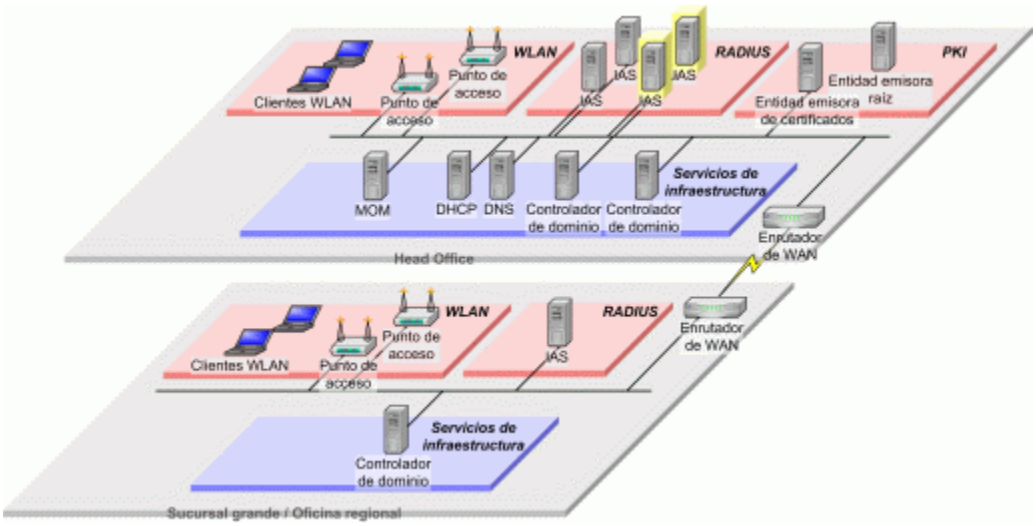

Figura 3.9 Solución escalada para una sucursal grande

Ver imagen a tamaño completo

Organización pequeña

Al otro lado del espectro, la solución puede implementarse con una cantidad modesta de sistemas de hardware y software nuevos. Esto se logra principalmente ejecutando el servicio IAS en controladores de dominio existentes. Se trata de una alternativa ampliamente probada por el grupo de productos IAS en Microsoft y se recomienda para varios escenarios. El siguiente diagrama ilustra esta variante del diseño.

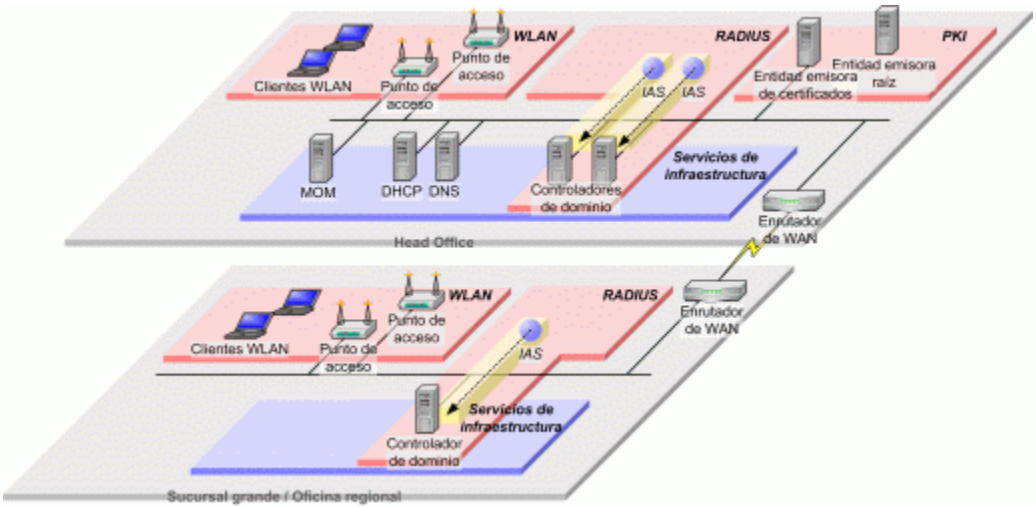

Figura 3.10 Solución escalada para una sucursal pequeña
Ver imagen a tamaño completo

El componente RADIUS aún se muestra aquí separado lógicamente (de modo que coincida con el diseño del diagrama anterior para su correspondiente comparación), pero se implementa realmente como servicio en controladores de dominio ya existentes. Los únicos servidores requeridos en esta versión de la solución son las entidades emisoras que residen en el área de PKI de la solución.

Extensión del diseño

Otro criterio de diseño clave es la reutilización de los componentes en aplicaciones futuras. Tanto el componente RADIUS como el componente PKI pueden reutilizarse para proporcionar servicios de autenticación y otros servicios de seguridad para diversas aplicaciones.

Otros servicios de acceso a la red

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

Autenticación de red por cable 802.1X

La aplicación más sencilla, sin modificación del diseño básico de RADIUS WLAN, es la autenticación por cable 802.1X. A las organizaciones que tienen una infraestructura de red por cable de amplia distribución les puede resultar difícil controlar el uso no autorizado de la red corporativa. Por ejemplo, generalmente 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 designarse como zonas de alta seguridad. Sólo los dispositivos autorizados deben admitirse en estas zonas, excluyendo además, si fuera necesario, a empleados con equipos corporativos.

La figura siguiente muestra cómo se integra en el diseño una solución de acceso a red por cable: el área con bordes en negrita representa los componentes por cable de 802.1X, mientras que las otras áreas de la estructura contienen los servicios relevantes que se mostraron en el diagrama de diseño anterior.

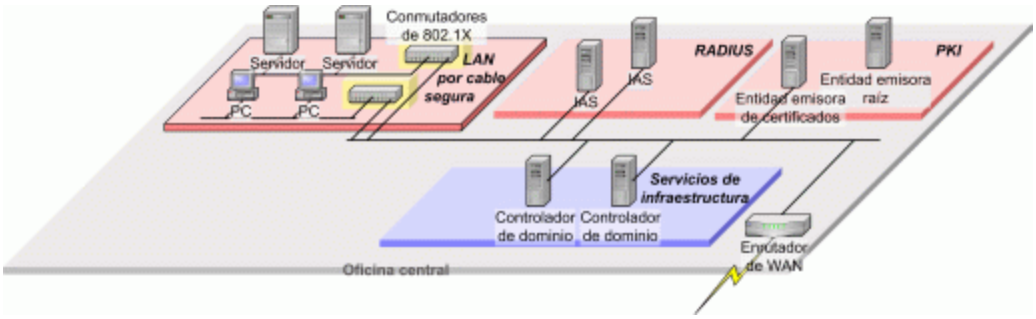

Figura 3.11 Uso de la autenticación por cable 802.1X
Ver imagen a tamaño completo

Las redes que usan conmutadores de 802.1X ofrecen un servicio idéntico al de los puntos de acceso inalámbrico en la solución principal. Es más, pueden utilizar la misma infraestructura de RADIUS para autenticar clientes y autorizar selectivamente el acceso al segmento de red correspondiente. Esto incluye las ventajas obvias de centralizar la administración de cuentas en el directorio corporativo, dejando las directivas de acceso a la red bajo el control del administrador de seguridad de la red.

Autenticación de VPN y acceso telefónico remoto

Otros servicios de acceso a la red que podrían utilizar los componentes RADIUS son la VPN y el acceso telefónico remoto. Es probable que, particularmente en las organizaciones grandes, sea necesario realizar algunas adiciones al diseño original, como la adición de servidores proxy RADIUS. La figura siguiente muestra la apariencia que podría presentar la solución extendida.

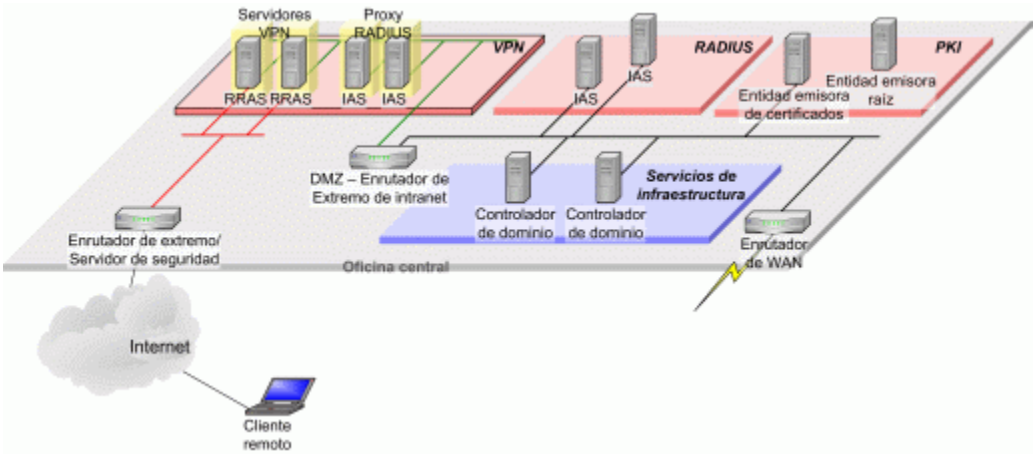

Figura 3.12 Extensión del componente RADIUS para admitir VPN
Ver imagen a tamaño completo

Los servidores VPN de esta solución cumplen la misma función NAS que los PA inalámbricos en el diseño principal: transmiten las solicitudes de autenticación de los clientes a la infraestructura de RADIUS. Si bien las solicitudes de RADIUS pueden pasar directamente a los servidores IAS internos, se considera más seguro utilizar una capa proxy de RADIUS que reenvíe solicitudes a los servidores IAS internos.

Esta solución también brinda ventajas de utilización de la infraestructura existente y centralización de la administración de cuentas, manteniendo el control de la directiva de acceso bajo supervisión del administrador de seguridad de la red. Las mejoras adicionales, como la autenticación obligatoria de usuarios con tarjeta inteligente, realizan un aporte a la seguridad general suministrada por la solución. Microsoft utiliza una configuración muy similar para su propio personal interno, a fin de permitirles conectarse de manera segura a la red corporativa.

El acceso telefónico remoto funciona de manera similar mediante la utilización de la capacidad de servidor de acceso telefónico del servicio de enrutamiento y acceso remoto (RRAS, Routing and Remote Access Service) en lugar de las funciones de VPN.

Otra ventaja de la utilización de RADIUS (específicamente IAS) en este escenario es la capacidad de utilizar directivas de establecimiento de *cuarentenas*. Esta función utiliza el servicio de enrutamiento y acceso remoto en Microsoft Windows Server 2003 y el administrador de conexión (el cliente de acceso remoto mejorado con Windows) para permitir o denegar el acceso según el estado de seguridad del equipo cliente. Con esta configuración, IAS puede verificar que el cliente cumple determinados requisitos cuando se conecta a la red. Por ejemplo, este procedimiento puede comprobar que el cliente cuenta con software antivirus actualizado o que ejecuta una versión de sistema operativo aprobada por la empresa. Si el cliente no satisface alguna de estas comprobaciones, el servidor RADIUS denegará su acceso a la red. De esta forma se puede denegar el acceso incluso a usuarios y equipos autenticados de la forma adecuada si representan una amenaza de seguridad para la red corporativa.

Aplicaciones de PKI

Puesto que los criterios de reutilización y extensibilidad se consideran importantes, el diseño del componente PKI se desarrolló con la idea de que podría utilizarse para diferentes aplicaciones de seguridad en el futuro. Como se analizará en el capítulo siguiente, el diseño de la PKI consiste, por un lado, en una estrategia combinada de minimización de costo y complejidad como parte de una solución inalámbrica segura y, por otro, en el mantenimiento de suficiente flexibilidad para utilizarla como base de otras aplicaciones en el futuro.

El siguiente diagrama ilustra algunas aplicaciones que el componente PKI podría admitir junto con la aplicación inalámbrica segura. Algunas de ellas son aplicaciones relativamente sencillas que pueden utilizar la PKI desarrollada en esta solución con mínimos cambios en el diseño principal. Otras, como el correo electrónico seguro y el inicio de sesión con tarjeta inteligente, son más complejas y requerirán seguramente una consideración y extensión más cuidadosas de la solución PKI.

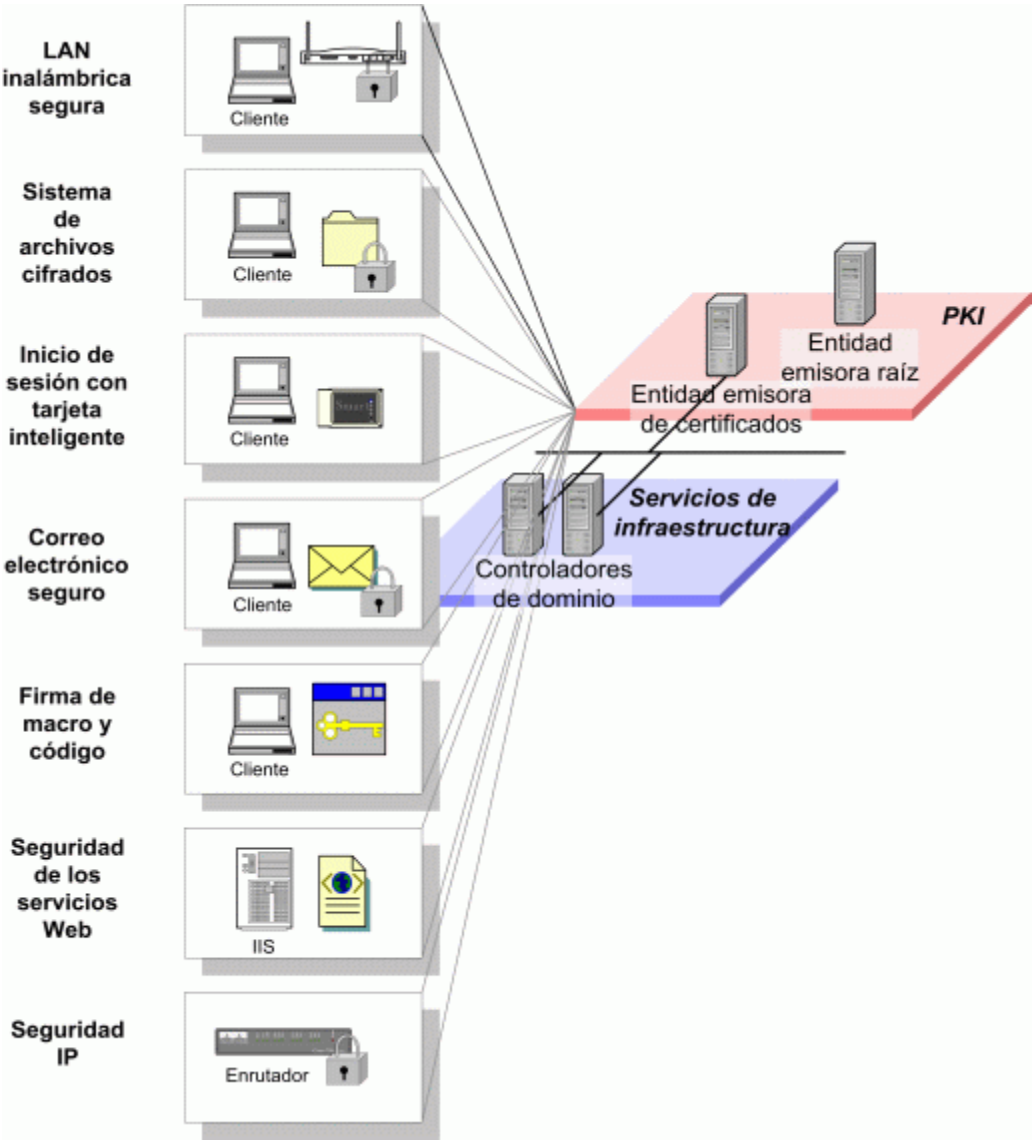

Figura 3.13 Aplicaciones de PKI
Ver imagen a tamaño completo

Principio de la página

Reevaluación de los criterios de diseño

Antes de cerrar el capítulo, resulta conveniente volver a examinar la lista de criterios para ver en qué grado el diseño propuesto cumple los objetivos establecidos anteriormente. Esta evaluación se resume en la lista a continuación. Muchos de estos elementos se tratan de forma exhaustiva en capítulos de diseño posteriores.

- **Seguridad**. El diseño incluye servicios de autenticación, autorización y control de acceso sólidos. El cifrado de alta seguridad (de 128 bits) es una función del hardware de red compatible con la mayoría de los dispositivos disponibles actualmente. Se proporciona una administración segura de las claves de cifrado mediante la combinación del cliente 802.1X de Microsoft, el punto de acceso inalámbrico habilitado para 802.1X y las tarjetas de red inalámbrica y el servidor RADIUS.

  El logro de una resistencia total a ataques de denegación de servicio constituye una tarea compleja; los estándares anteriores a 802.11i presentan vulnerabilidad a diversos ataques de este tipo.

- **Escalabilidad**. El diseño básico se ajusta a una gama de organizaciones con un costo asequible y una

capacidad que oscila entre cientos y varios miles de usuarios. El diseño también es flexible en relación con el diseño geográfico y de red. Las oficinas pequeñas sin controlador de dominio local dependen de la fiabilidad de la WAN o de una solución de seguridad de menor calidad.

- **Reutilización de componentes (uso de la infraestructura existente)**. El diseño utiliza el servicio de directorio de Active Directory y muchos servicios de red existentes, como el protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol) y el sistema de nombres de dominio (DNS, Domain Name System).
- **Reutilización de componentes por parte de aplicaciones futuras.** El diseño de RADIUS, implementado mediante IAS, está listo para utilizarse o puede extenderse fácilmente para admitir otras aplicaciones de acceso a red (como VPN, acceso a red por cable 802.1X y acceso telefónico remoto). De forma similar, la PKI es capaz de admitir aplicaciones sencillas de clave pública, como EFS, y proporciona el entorno para aplicaciones más complejas, como el inicio de sesión con tarjeta inteligente.

  Este elemento también cumple el criterio de diseño de **extensibilidad**.
- **Disponibilidad**. La solución es resistente a errores en componentes individuales o en vínculos de red en la oficina central y en todas las oficinas remotas donde pueda implementarse un servidor RADIUS. Las oficinas pequeñas sin servidor RADIUS local son vulnerables a errores de WAN.
- **Capacidad de administración**. La capacidad de administración de la solución no es evidente en el diseño, pero este criterio se aplica al diseño del marco operativo.
- **Estructura de la organización de TI**. Resulta esencial tener como mínimo una base de especialización con WLAN en el departamento de TI de la organización para implementar y administrar una solución de este tipo.
- **Cumplimiento de estándares.** La solución cumple con las normas industriales y oficiales actuales. Esto resulta de mayor importancia en el área de seguridad de WLAN donde la solución se basa en el protocolo 802.1X, EAP-TLS y WEP dinámica de 128 bits o WPA. Microsoft anunció recientemente la compatibilidad del producto Windows XP con WPA, proporcionando los estándares de seguridad más altos disponibles de WLAN. El diseño será compatible con WPA o WEP dinámica.

Principio de la página

Resumen

Este capítulo describe a nivel conceptual una solución de red de LAN inalámbrica segura basada en el protocolo 802.1X y EAP-TLS. Los componentes clave se explican al nivel de arquitectura. También se describe la organización de destino para esta solución, junto con los criterios de diseño utilizados para crearla.

Seguidamente, los criterios de diseño se utilizan para trasladar la solución conceptual a un diseño de solución lógico. Esto incluye un análisis de las opciones de implementación para escalar a diferentes tamaños y requisitos de organizaciones, extendiendo el diseño básico para proporcionar compatibilidad con otras aplicaciones de seguridad y acceso a la red. Finalmente, los principales criterios de diseño se revisan, comparándolos con las características del diseño propuesto. Esta revisión de criterios sirve de introducción al resto de los capítulos de la guía de planeamiento.

Los tres capítulos siguientes profundizan en el análisis de diseño detallado de cada uno de los principales componentes de arquitectura de la solución: la PKI, la infraestructura de RADIUS y el diseño de seguridad de WLAN.

Principio de la página

Administre su perfil