Capítulo 6: Diseño de seguridad para LAN inalámbrica mediante 802.1X

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | • | **Seguridad en LAN inalámbricas con Servicios de Certificate Server** |  |  |  | | --- | --- | | • | [Contenido de la solución](http://www.microsoft.com/latam/technet/articulos/wireless/solseptn.mspx) | | • | [Guía de planeamiento](http://www.microsoft.com/latam/technet/articulos/wireless/pgseptn.mspx) |  |  |  | | --- | --- | | • | [Guía de generación](http://www.microsoft.com/latam/technet/articulos/wireless/bgseptn.mspx) |  |  |  | | --- | --- | | • | [Guía de operaciones](http://www.microsoft.com/latam/technet/articulos/wireless/ogseptn.mspx) |  |  |  | | --- | --- | | • | [Guía de prueba](http://www.microsoft.com/latam/technet/articulos/wireless/tgseptn.mspx) |  |  |  | | --- | --- | | • | [Apéndices](http://www.microsoft.com/latam/technet/articulos/wireless/apseptn.mspx) | |

**En esta página**

|  |  |
| --- | --- |
| [Introducción](http://www.microsoft.com/latam/technet/articulos/wireless/pgch06.mspx#E1C) | [Introducción](http://www.microsoft.com/latam/technet/articulos/wireless/pgch06.mspx#E1C) |
| [Uso de 802.1X y cifrado para proteger redes WLAN](http://www.microsoft.com/latam/technet/articulos/wireless/pgch06.mspx#EQF) | [Uso de 802.1X y cifrado para proteger redes WLAN](http://www.microsoft.com/latam/technet/articulos/wireless/pgch06.mspx#EQF) |
| [Decisión entre certificados o contraseñas](http://www.microsoft.com/latam/technet/articulos/wireless/pgch06.mspx#E5F) | [Decisión entre certificados o contraseñas](http://www.microsoft.com/latam/technet/articulos/wireless/pgch06.mspx#E5F) |
| [Requisitos previos de la solución](http://www.microsoft.com/latam/technet/articulos/wireless/pgch06.mspx#EZAAC) | [Requisitos previos de la solución](http://www.microsoft.com/latam/technet/articulos/wireless/pgch06.mspx#EZAAC) |
| [Consideración de las opciones de seguridad de WLAN](http://www.microsoft.com/latam/technet/articulos/wireless/pgch06.mspx#ENBAC) | [Consideración de las opciones de seguridad de WLAN](http://www.microsoft.com/latam/technet/articulos/wireless/pgch06.mspx#ENBAC) |
| [Determinación de la configuración de software necesaria para redes WAN 802.1X](http://www.microsoft.com/latam/technet/articulos/wireless/pgch06.mspx#EGPAC) | [Determinación de la configuración de software necesaria para redes WAN 802.1X](http://www.microsoft.com/latam/technet/articulos/wireless/pgch06.mspx#EGPAC) |
| [Consideraciones adicionales](http://www.microsoft.com/latam/technet/articulos/wireless/pgch06.mspx#EXOAE) | [Consideraciones adicionales](http://www.microsoft.com/latam/technet/articulos/wireless/pgch06.mspx#EXOAE) |
| [Resumen](http://www.microsoft.com/latam/technet/articulos/wireless/pgch06.mspx#EDPAE) | [Resumen](http://www.microsoft.com/latam/technet/articulos/wireless/pgch06.mspx#EDPAE) |

**Introducción**

Este capítulo describe la arquitectura y el diseño de los componentes de red inalámbrica segura basados en el protocolo 802.1X para la solución de LAN inalámbrica (WLAN). El capítulo presenta las decisiones de diseño relacionadas con la seguridad en los componentes de red inalámbrica y las razones de dichas decisiones.

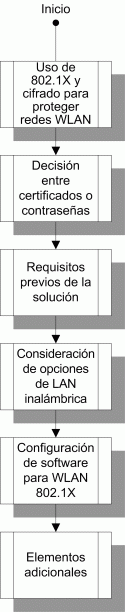
Un objetivo importante de este capítulo consiste en determinar si el diseño es adecuado para su organización. Cuando hay decisiones de diseño alternativas disponibles, se ofrece una relación de otras opciones relevantes junto a la opción utilizada en esta solución. Por esta razón, algunos temas ofrecen consideraciones más detalladas que le ayudarán a comprender las implicaciones de los pasos específicos y evitarán que tenga que consultar otros documentos.

**Requisitos previos**

Antes de continuar con este capítulo, le será de utilidad familiarizarse con los conceptos de WLAN basada en 802.11, el control de acceso a red basado en 802.1X, el servicio de usuario de acceso telefónico de autenticación remota (RADIUS, Remote Authentication Dial-In User Service), el servicio de autenticación de Internet (IAS, Internet Authentication Service) de Microsoft® y las opciones de implementación de WLAN con Microsoft Windows® XP Professional. Las referencias incluidas en la sección "Información adicional" al final de este capítulo le ayudarán a familiarizarse con estos temas. El *kit de recursos* de *Microsoft Windows Server™ 2003* y el *kit de implementación de Microsoft Windows Server™ 2003*contienen información particularmente útil.

**Descripción general del capítulo**

El diagrama de flujo siguiente ilustra la estructura del capítulo.



**Figura 6.1 Planeamiento de la seguridad de WLAN mediante 802.1X**

Este capítulo se ocupa de seis pasos principales:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1. | **Uso de 802.1X y cifrado para proteger redes WLAN** Las WLAN presentan dos vulnerabilidades que podría aprovechar cualquiera que disponga de un adaptador WLAN compatible. Este capítulo se ocupa de explicar estas vulnerabilidades mediante las recomendaciones siguientes:   |  |  | | --- | --- | | • | Garantice el acceso seguro a la red por medio de la configuración de los puntos de acceso inalámbricos IEEE 802.1X como clientes RADIUS para enviar solicitudes de acceso y mensajes de control de cuentas a servidores RADIUS. Estos servidores RADIUS (que ejecutan IAS) controlan el acceso a la red mediante directivas de acceso remoto centralizadas. | | • | Proteja los datos enviados entre los dispositivos inalámbricos y los puntos de acceso inalámbricos utilizando un cifrado de privacidad equivalente por cable (WEP, Wired Equivalent Privacy) de 128 bits o características de integridad y cifrado de acceso protegido Wi-Fi (WPA, Wi – Fi Protected Access) integradas en el equipo de acceso a redes 802.11X. La protección de datos evita la interceptación y el aprovechamiento indebido de datos transmitidos. | |
| 2. | **Decisión entre certificados o contraseñas.** Microsoft ofrece compatibilidad nativa para varios tipos de protocolos de autenticación en combinación con 802.1X. Las contraseñas y los certificados digitales constituyen las formas más comunes de autenticación. La selección del método de autenticación requerido para la organización puede tener un efecto considerable en la infraestructura necesaria para la solución. Este capítulo le ayudará a decidir qué método es el mejor para su organización. |
| 3. | **Requisitos previos de la solución.** Es importante que comprenda los requisitos previos de entorno de esta solución antes de iniciar el diseño. Éstos incluyen requisitos para equipos cliente, infraestructura de servidores y equipo WLAN. En esta sección se detallan estos requisitos previos. |
| 4. | **Consideración de las opciones de seguridad de WLAN.** El planeamiento de las opciones de seguridad es una tarea compleja que deberían compartir los responsables de directivas de seguridad, representantes de las áreas de adquisición de hardware y aprovechamiento, ingenieros de redes y administradores de operaciones de red. Estos expertos deberían tomar en consideración los temas siguientes, que se incluyen de forma detallada en este capítulo:   |  |  | | --- | --- | | • | determinación de los requisitos de autorización de red. | | • | elección de una estrategia de configuración de clientes. | | • | determinación de los requisitos de cifrado de tráfico. | | • | diseño de la infraestructura de red inalámbrica. | | • | consideraciones relacionadas con la creación de una directiva de grupo de red inalámbrica. | |
| 5. | **Determinación de la configuración de software necesaria para redes WAN 802.1X.** Para lograr la seguridad de WLAN 802.1X, necesitará configurar una directiva de acceso de red basada en IAS y una directiva de grupo de servicios de directorio de Active Directory® para equipos cliente. En esta sección se detalla el proceso a seguir. |
| 6. | **Consideración de factores adicionales.** En esta sección se mencionan brevemente algunos temas que deben tenerse en cuenta pero que quedan fuera del alcance de esta solución, aunque puede ser que ejerzan un impacto en el entorno. Estos factores incluyen:   |  |  | | --- | --- | | • | compatibilidad con perfiles móviles y usuarios itinerantes. | | • | compatibilidad con clientes sin conexiones LAN por cable. | |

[Principio de la páginaPrincipio de la página](http://www.microsoft.com/latam/technet/articulos/wireless/pgch06.mspx#top)

**Uso de 802.1X y cifrado para proteger redes WLAN**

Las redes WLAN se están extendiendo rápidamente con la adopción de estándares de la industria como IEEE 802.11 y 802.11b. Las LAN inalámbricas permiten que los usuarios se desplacen por un edificio o recinto y se conecten automáticamente a la red cuando se encuentran cerca de un punto de acceso inalámbrico.

Si bien las WLAN son muy convenientes, presentan los siguientes riesgos de seguridad:

|  |  |
| --- | --- |
| • | Una persona que tenga un adaptador de WLAN compatible puede obtener acceso a la red. |
| • | Las señales de red inalámbrica utilizan ondas de radio para enviar y recibir información. Una persona que se encuentre a una distancia apropiada de un punto de acceso inalámbrico puede detectar y recibir todos los datos enviados a y desde el punto de acceso inalámbrico. |

Para combatir el primer riesgo de seguridad, puede configurar los puntos de acceso inalámbricos IEEE 802.1X como clientes RADIUS para enviar solicitudes de acceso y mensajes de control de cuentas a servidores RADIUS que ejecutan IAS. IAS realiza la autenticación de usuarios y dispositivos y controla el acceso a la red mediante directivas de acceso remoto centralizadas.

Para combatir el segundo riesgo de seguridad, puede proteger los datos enviados entre los dispositivos inalámbricos y los puntos de acceso inalámbricos utilizando un cifrado WEP de 128 bits o características de cifrado WPA integradas en el equipo de acceso a redes 802.11.

La WEP estática presenta errores de diseño graves y no incluye administración nativa de claves de cifrado que permita la actualización frecuente de las mismas. De este modo, las claves pueden quedar expuestas al uso de posibles atacantes. IAS permite la asignación dinámica de claves WEP seguras a equipos con Windows XP durante la autenticación basada en certificados. Además, las claves WEP se pueden actualizar a intervalos regulares para impedir que las herramientas de ataque puedan descubrir las claves.

WPA es un subconjunto del estándar de seguridad 802.11i de próxima aparición para equipos WLAN basados en 802.11. Incluye un cifrado mejorado que ha sido diseñado para resolver los problemas de seguridad de WEP estática. La solución presentada en esta guía resulta igualmente apropiada para su uso con WPA (se requiere hardware compatible con WPA y la actualización del equipo con Windows XP).

[Principio de la páginaPrincipio de la página](http://www.microsoft.com/latam/technet/articulos/wireless/pgch06.mspx#top)

**Decisión entre certificados o contraseñas**

Microsoft ofrece compatibilidad nativa para varios métodos de autenticación que pueden utilizarse con el protocolo 802.1X. Generalmente, las organizaciones seleccionan métodos de autenticación de cliente WLAN que utilizan credenciales basadas en contraseñas o certificados.

Como mencionamos anteriormente, el método de autenticación seleccionado puede tener un efecto considerable en la infraestructura necesaria para la solución. El estándar 802.1X aprovecha un esquema de autenticación acoplable denominado "protocolo de autenticación extensible" (EAP, Extensible Authentication Protocol), que permite el uso de diferentes tipos de autenticación.

En la tabla siguiente se indican los tipos de EAP que se pueden utilizar en una infraestructura 802.1X de Microsoft y las ventajas e inconvenientes de cada tipo.

**Tabla 6.1: Ventajas e inconvenientes de los tipos de EAP**

| **Característica** | **PEAP** | **EAP-TLS** | **EAP-MD5** |
| --- | --- | --- | --- |
| Autenticación mutua | Autenticación mutua. | Autenticación mutua. | Sólo autenticación de cliente. |
| Generación dinámica de claves y actualización programada. | Generada durante la autenticación y actualizada a intervalos regulares. | Generada durante la autenticación y actualizada a intervalos regulares. | No se produce generación ni actualización de claves dinámicas: utiliza claves estáticas. |
| Nivel de tecnología de seguridad | Puede utilizar autenticación segura de contraseñas o certificados digitales. | Autenticación más segura. | Tecnología de seguridad no segura. |
| Protección de credenciales de usuario | Protegido por túnel de Transport Layer Security (TLS). | Autenticación basada en certificados protegida por túnel de Transport Layer Security (TLS). | Abierto a ataque de diccionario. |
| Facilidad de implementación | Con amplia compatibilidad y ofrecido en los clientes de Windows de forma nativa. | Requiere una infraestructura de claves públicas (PKI). Con amplia compatibilidad y ofrecido en los clientes de Windows de forma nativa. | Simple, pero no recomendado para sistemas inalámbricos. |
| Flexibilidad de credenciales | Cualquier EAP aprobado con túnel de TLS, incluido EAP-MSCHAPv2 (método basado en contraseñas). | Sólo certificados digitales | Sólo contraseña |

El tipo de EAP recomendado para realizar la autenticación de cliente basada en certificados es EAP-TLS, y el tipo de EAP recomendado para realizar la autenticación de cliente basada en contraseñas es EAP-MSCHAPv2 dentro del protocolo de autenticación extensible protegido (PEAP, Protected Extensible Authentication Protocol), también conocido como PEAP-EAP-MSCHAPv2.

La autenticación de 802.1X basada en contraseñas con PEAP y MSCHAPv2 constituye una solución rentable y segura. Esta solución es apropiada para organizaciones que no disponen de una infraestructura de certificados y no necesitan certificados para otras finalidades, como el uso del sistema de archivos de cifrado (EFS, Encrypting File System), una red privada virtual (VPN, Virtual Private Network), etc. La migración del sistema de autenticación 802.1X basado en contraseñas a la autenticación basada en certificados es sencilla, lo que proporciona flexibilidad a su organización para pasar de un método a otro en el futuro.

Tenga presente que incluso una solución basada en contraseñas con PEAP requiere la presencia de un certificado en cada servidor RADIUS. Sin embargo, los costos que conlleva la compra de certificados de servidor a un proveedor de certificados deben compararse cuidadosamente con el valor que la infraestructura de certificados otorgará a la organización.

Esta solución utiliza la autenticación de clientes basada en certificados, ya que ofrece un nivel de seguridad superior. Este método de autenticación utiliza el protocolo de autenticación extensible - protocolo de seguridad de la capa de transporte (EAP-TLS, Extensible Authentication Protocol – Transport Layer Security).

Si desea obtener detalles sobre la implementación de una solución 802.1X basada en contraseñas que utiliza PEAP y MSCHAPv2, consulte el capítulo 2, "Determinación de una estrategia para redes inalámbricas seguras", y utilice la referencia a la guía complementaria de la solución, *Seguridad en LAN inalámbricas con PEAP y contraseñas*, incluida al final de este capítulo.

[Principio de la páginaPrincipio de la página](http://www.microsoft.com/latam/technet/articulos/wireless/pgch06.mspx#top)

**Requisitos previos de la solución**

Es importante que comprenda los requisitos previos de entorno de esta solución antes de iniciar el diseño. En esta sección se detallan estos requisitos previos.

**Requisitos del equipo cliente**

El diseño y las pruebas de esta solución se han llevado a cabo en equipos con Windows XP Professional con Service Pack (SP) 1. Windows XP con SP1 proporciona algunas funcionalidades de características de 802.1X y WLAN necesarias para conseguir una solución de costo extremadamente bajo y muy fácil de administrar.

En las pruebas de la solución se incluyeron equipos cliente con Windows XP Professional y Windows XP Professional, Tablet PC Edition. Ambas ediciones de Windows XP proporcionan inscripción automática de certificados y renovación de certificados de autenticación de equipo y usuario de WLAN necesarios para la autenticación de cliente EAP-TLS. Esta característica por sí sola reduce de forma significativa el costo generalmente asociado con los certificados y, por lo tanto, con la solución 802.1X basada en certificados.

Microsoft proporciona clientes 802.1X para Windows 2000 (disponible como descarga gratuita), Windows 9*x* y Microsoft Windows NT® 4.0 (disponible de forma gratuita para clientes que cuentan con un contrato de soporte). No obstante, estos tipos de cliente no se probaron en esta versión de la solución.

**Infraestructura de servidor necesaria**

Esta solución depende de los componentes de Servicios de Certificate Server e IAS de Windows Server 2003. Servicios de Certificate Server e IAS tienen características que han sido diseñadas explícitamente para redes WLAN basadas en 802.1X. Entre estas características se incluyen plantillas de certificado editables y configuraciones de directivas de acceso remoto que permiten la configuración de implementación simplificada para el protocolo 802.1X.

La solución se ha diseñado para funcionar en un entorno de Active Directory con Windows Server 2003 y Windows 2000. No obstante, la solución se ha probado principalmente con controladores de dominio de Windows Server 2003. Si lo desea, puede instalar IAS en controladores de dominio existentes. Si desea consultar una descripción detallada de las consideraciones de co-ubicación relacionadas, consulte el capítulo 5, "Diseño de una infraestructura de RADIUS para la seguridad de LAN inalámbricas".

**Equipos WLAN necesarios**

Esta solución presupone la existencia en su organización de una infraestructura WLAN bien diseñada y plenamente funcional. Esta guía no incluye instrucciones de diseño de redes inalámbricas, por ejemplo, sobre la ubicación de puntos de acceso inalámbricos o la selección de canales. Si no se ha implementado una infraestructura de WLAN en la organización, asegúrese de que dispone del personal especializado necesario para llevar a cabo esta tarea antes de iniciar la implementación de los componentes de seguridad de WLAN.

El hardware de red debe ser compatible con 802.1X y WEP de 128 bits para el cifrado. En esta guía se da por hecho que el funcionamiento de la infraestructura de WLAN es satisfactorio y que, de haber controles de seguridad habilitados, se trata únicamente de los controles de seguridad básicos de 802.11. La migración desde WLAN de clave compartida (WEP estática) o WLAN 802.11 de sistema abierto (sin protección) a esta solución es muy similar. Cualquiera de estos dos tipos de migración debería poderse llevar a cabo sin problemas de gran magnitud.

[Principio de la páginaPrincipio de la página](http://www.microsoft.com/latam/technet/articulos/wireless/pgch06.mspx#top)

**Consideración de las opciones de seguridad de WLAN**

Si no lo ha hecho todavía, debería dedicar algún tiempo a planear una directiva de seguridad WLAN para su organización. En dicho planeamiento deben participar representantes de las áreas de adquisición de hardware, directivas de seguridad, aprovechamiento, ingeniería y operaciones de red. Las consideraciones de directivas de seguridad a tratar con estos representantes deberían incluir el modo en que la organización hará frente a las amenazas que se presenten y los controles de seguridad que se utilizarán para mitigarlas.

También es importante documentar la directiva de seguridad de WLAN y ponerla a disposición de todos los usuarios de la red. Esta solución proporciona controles de seguridad para mitigar el riesgo asociado con la tecnología WLAN moderna. Sin embargo, no puede mitigar los riesgos de que los usuarios de la organización utilicen un acceso a redes ad-hoc no seguro e implementen puntos de acceso inalámbricos defectuosos.

**Selección de autenticación basada en usuarios o en equipos**

La autenticación de usuarios es una elección natural al considerar la identificación en una infraestructura WLAN. No obstante, en la mayoría de los casos será deseable implementar también autenticación de equipos (o dispositivos) para garantizar que la solución de seguridad sea completa.

Windows XP Professional contiene algunas funciones que sólo funcionan correctamente si hay una conexión de red activa. El uso de la autenticación de equipos con 802.1X garantiza que la conexión de red WLAN se establezca durante la secuencia de arranque y antes de que los usuarios vean la pantalla de inicio de sesión de Windows. El equipo repite la autenticación con la WLAN cuando el usuario cierra la sesión, lo que garantiza una conexión permanente a la red.

**Tabla 6.2: Consideraciones para la autenticación de equipos**

| **Característica** | **Escenario que requiere autenticación de equipos** |
| --- | --- |
| Directiva de grupo en equipo con Active Directory | La directiva de grupo basada en equipos se aplica durante el arranque del equipo y a intervalos regulares, aunque ningún usuario haya iniciado la sesión en Windows. |
| Secuencias de comandos de inicio de sesión de red | Las secuencias de comandos de inicio de sesión de red se ejecutan durante el inicio de sesión de usuario inicial. |
| Agentes de Systems Management | Los agentes de la aplicación Systems Management, como los que se incluyen en Microsoft Systems Management Server (SMS), con frecuencia requieren acceso a la red sin intervención del usuario. |
| Conexión a Escritorio remoto | Es posible obtener acceso a los equipos desde la conexión a escritorio remoto de Windows cuando ningún usuario ha iniciado la sesión en Windows. |
| Carpetas compartidas | Los archivos y carpetas compartidos de un equipo continúan estando disponibles, aunque ningún usuario haya iniciado una sesión. |

La mejor estrategia es utilizar la autenticación basada en usuarios siempre que sea posible y la autenticación basada en equipos cuando sea necesaria. La orientación que se ofrece en esta solución especifica el comportamiento predeterminado del cliente de 802.1X en Windows XP Professional. Este comportamiento implica realizar la autenticación de equipos cuando ningún usuario ha iniciado una sesión, la autenticación de usuarios cuando los usuarios inician una sesión en Windows y nuevamente la autenticación de equipos cuando los usuarios cierran la sesión. Esto garantiza que el proceso de autenticación en la red utilice las credenciales de cuenta del usuario siempre que sea posible para realizar el control, sin que las funciones de Windows que requieren acceso a la red dejen de funcionar correctamente cuando no hay usuarios conectados.

**Validación de credenciales basada en certificados**

La comprobación de la validez de las credenciales es importante en una estrategia de autenticación de WLAN basada en certificados. La comprobación de certificados revocados permite bloquear el uso de credenciales almacenadas en equipos informáticos perdidos o robados. El hecho de forzar la verificación de certificados de servidor por parte de los clientes contribuye a evitar los sofisticados ataques de intermediario mediante servidores RADIUS y puntos de acceso falsos.

Windows proporciona amplio soporte para validar certificados al realizar operaciones basadas en certificados. Las funciones 802.1X tanto de IAS como de Windows XP Professional aprovechan este soporte para garantizar que los certificados utilizados para EAP-TLS sean válidos y representen un principal de seguridad de confianza.

**Tabla 6.3: Validación IAS de credenciales de certificados de cliente**

| **Validación IAS de credenciales de certificados de cliente** | **Comportamiento predeterminado** | **Configuración utilizada en esta solución** |
| --- | --- | --- |
| Comprobar que el certificado se encuentre dentro de las fechas de validez. | Habilitada | Sin cambios |
| Comprobar la posibilidad de crear una cadena desde el certificado hasta un directorio raíz confiable. | Habilitada | Sin cambios |
| Comprobar que las directivas de aplicación y los usos de claves requeridos estén presentes en el certificado. | Habilitada | Sin cambios |
| Comprobar que el cliente demuestre su propiedad firmando una clave privada. | Habilitada | Sin cambios |
| Comprobar que el certificado no sea denegado. | Habilitada | Sin cambios |

Windows XP Professional realiza también la siguiente validación de credenciales de servidor IAS de forma predeterminada.

**Tabla 6.4: Validación de credenciales de certificado IAS en Windows XP**

| **Validación de credenciales de certificados de servidor en Windows XP** | **Comportamiento predeterminado** | **Configuración utilizada en esta solución** |
| --- | --- | --- |
| Comprobar que el certificado se encuentre dentro de las fechas de validez. | Habilitada | Sin cambios |
| Comprobar la posibilidad de crear una cadena desde el certificado hasta un directorio raíz confiable. | Habilitada | Sin cambios |
| Comprobar que las directivas de aplicación y los usos de claves requeridos estén presentes en el certificado. | Habilitada | Sin cambios |
| Comprobar que el servidor demuestre su propiedad firmando una clave privada. | Habilitada | Sin cambios |

Durante la autenticación en una WLAN, el equipo cliente no puede realizar una comprobación completa de revocación del certificado del servidor, ya que el acceso de red no está disponible hasta que se lleva a cabo la autenticación de forma satisfactoria.

No obstante, debe considerar la posibilidad de habilitar las siguientes opciones adicionales de validación de credenciales (llevadas a cabo por el cliente) para incrementar la seguridad de la comprobación.

**Tabla 6.5: Validación avanzada de credenciales de certificados IAS en Windows XP**

| **Validación de credenciales de certificados de servidor en Windows XP** | **Comportamiento predeterminado** | **Configuración utilizada en esta solución** |
| --- | --- | --- |
| El sujeto del certificado coincide con un valor de cadena del sistema de nombres de dominio (DNS) configurable en el cliente. | No habilitado | Sin cambios |
| Selección explícita de entidades emisoras raíz de confianza a las que el certificado de servidor puede encadenarse. | No habilitado | Habilitada |

La opción de comprobación del nombre de sujeto en equipos cliente hará que los usuarios vean un mensaje donde deben indicar si la entidad emisora de certificados es de confianza. Adicionalmente, deberá implementar un proceso de administración para mantener actualizados los nombres de sujeto de certificados de servidor en los clientes WLAN. Para ello puede utilizarse la configuración de GPO de directivas de red inalámbrica. Por estos motivos, esta solución no implementa esta opción. Si trabaja en un entorno con un nivel de seguridad alto, debe considerar las amenazas que plantean los falsos servidores IAS con puntos de acceso inalámbricos a la hora de decidir si necesita este nivel adicional de validación.

La selección explícita de entidades emisoras raíz de confianza minimiza el riesgo de la existencia de certificados de servidor falsos de entidades emisoras de certificados alternativas en el almacén raíz de confianza. No obstante, esta configuración requiere un proceso de administración adicional para garantizar que los cambios en los certificados de entidades emisoras raíz de confianza se reflejen en la configuración de cliente WLAN. La implementación de estas opciones también se lleva a cabo mediante la configuración de GPO de directivas de red inalámbrica.

**Determinación de los requisitos de autorización de red**

Algunos de los principales objetivos del diseño de directivas de administración de acceso de red son igualarlas al máximo con las directivas de seguridad organizativas y minimizar el costo de administración. Una representación centralizada de directiva de autorización de red, como las directivas de acceso remoto IAS, se adapta bien a la tarea.

**Nota:** esta solución utiliza administración de autorización de red mediante directiva de acceso remoto IAS. Si desea obtener más información sobre las decisiones utilizadas en la selección de un modelo de administración de directivas de acceso, consulte los recursos enumerados en la sección "Información adicional" al final de este capítulo.

Conseguir una administración de la autorización de red flexible pero simple debería ser uno de los objetivos principales de cualquier organización. La clave para conseguir una administración simplificada es minimizar el número de directivas de acceso remoto al tiempo que se garantiza que todas las directivas de seguridad organizativa estén representadas.

**Determinación de los criterios de conexión**

Las directivas de acceso remoto IAS pueden permitir o denegar conexiones. Una directiva contiene una serie de criterios que se utilizan para comprobar cada intento de conexión. La primera directiva encontrada que coincida con una conexión particular se usará para permitir o denegar el acceso. Los atributos de conexión principales que se utilizan en esta comprobación son los siguientes:

|  |  |
| --- | --- |
| • | Pertenencia al grupo |
| • | Tipo de conexión |
| • | Hora del día |
| • | Métodos de autenticación |

Adicionalmente, puede especificar otros criterios de filtro avanzados, como los siguientes:

|  |  |
| --- | --- |
| • | Identidad del servidor de acceso |
| • | Número de teléfono del cliente de acceso o dirección de control de acceso al medio (MAC) |
| • | si se ignoran las propiedades de marcado de la cuenta de usuario. |
| • | si se permite el acceso sin autenticación. |

Esta solución utiliza criterios de conexión IAS basados en el grupo de seguridad del dominio y el tipo de red de origen, en lugar de la hora del día, el método de autenticación u otras condiciones. Esto garantiza que las directivas de acceso remoto se creen para un tipo de acceso de red concreto (como inalámbrico, VPN, de cableado o de marcado) y con agrupación de clientes, pero manteniéndose suficientemente amplias para minimizar el número de directivas necesarias.

**Nota:** esta solución utiliza grupos de seguridad personalizados (directiva de acceso remoto - usuarios inalámbricos y la directiva de acceso remoto - equipos inalámbricos) para restringir el acceso a la WLAN de usuarios y equipos. Si desea que todos los usuarios y equipos del dominio puedan acceder a la WLAN, puede incluir los grupos de usuarios y equipos del dominio en estos grupos de seguridad personalizados para simplificar el proceso de administración.

**Determinación de las restricciones de conexión**

Una vez que la conexión queda autorizada, la directiva de acceso remoto especifica las restricciones de conexión, entre otros atributos, que deben aplicarse a dicha conexión. Entre estas operaciones se incluyen las siguientes:

|  |  |
| --- | --- |
| • | tiempo de espera de inactividad. |
| • | Tiempo máximo de conexión |
| • | Intensidad de cifrado |
| • | filtros de paquetes estáticos. |

Adicionalmente, puede aplicar los siguientes atributos a la conexión:

|  |  |
| --- | --- |
| • | Dirección IP para conexiones de protocolo punto a punto (PPP) |
| • | Rutas estáticas |

La determinación real del número de directivas de acceso remoto requeridas en la organización radicará en el número de tipos distintos de usuarios que necesitan obtener acceso a la red inalámbrica. Por ejemplo, en muchas organizaciones el personal que trabaja a tiempo completo necesita acceso total y sin restricciones a toda la red corporativa. No obstante, las empresas auxiliares y los socios sólo necesitan obtener acceso a aplicaciones concretas en determinadas subredes de la red.

Los perfiles de restricción de la conexión son específicos para cada directiva de acceso remoto. Por tanto, si se requieren varios tipos de perfiles de restricción de la conexión, también se necesitan varias directivas de acceso remoto.

La tabla siguiente contiene algunos ejemplos de los distintos tipos de usuarios y las posibles restricciones de conexión que pueden aplicarse mediante la directiva de acceso remoto.

**Tabla 6.6: Ejemplos de restricciones de conexión WLAN**

| **Tipo de grupo de usuarios** | **Ejemplo de restricción de la conexión** |
| --- | --- |
| Personal a tiempo completo | Acceso ilimitado con autenticación a la red corporativa |
| Empresas auxiliares y socios | Acceso restringido con autenticación a redes y aplicaciones concretas. |
| Visitantes | Acceso sin autenticación a segmentos sólo de Internet para la exploración Web o el acceso a la organización de origen a través de VPN. |

Esta solución sólo configura el soporte para personal a tiempo completo autenticado. Por tanto, sólo se necesita una directiva de acceso remoto con un perfil de restricción de la conexión simplificado. Si la organización tiene requisitos adicionales, como el de permitir el acceso restringido de invitados a la red inalámbrica, deberán considerarse directivas de acceso remoto adicionales. Consulte las referencias de la sección "Información adicional" al final de este capítulo para obtener más información sobre el planeamiento de otros tipos de directivas de acceso remoto.

**Elección de una estrategia de configuración de clientes**

La automatización de la configuración de equipos cliente es un paso esencial a la hora de reducir el costo de implementación del acceso seguro a redes inalámbricas y minimizar los problemas de compatibilidad derivados de configuraciones incorrectas.

Windows XP Professional cuenta con funciones sofisticadas para minimizar la configuración y reconfiguración manual de la red inalámbrica y las opciones de seguridad de 802.1X en los clientes WLAN. Windows Server 2003 agrega capacidades adicionales para automatizar la configuración de clientes utilizando las opciones de directivas de red inalámbrica en la directiva de grupo. Esta solución utiliza la directiva de red inalámbrica en Windows Server 2003 para configurar automáticamente todos los clientes de red inalámbricos.

La implementación de esta configuración de GPO en equipos cliente se puede realizar incluso antes de la distribución de tarjetas de interfaz de red (NIC, Network Interface Card) WLAN. Bastará entonces con que los usuarios finales instalen las NIC inalámbricas y se conecten automáticamente a la WLAN 802.1X segura mediante la configuración de WLAN implementada por medio de GPO.

**Determinación de los requisitos de cifrado de tráfico**

Debe considerar las amenazas en constante evolución al cifrado WEP 802.11 al determinar su estrategia para proteger la privacidad del tráfico WLAN. Como mencionamos anteriormente, es posible que algunos atacantes consigan aprovechar los defectos de cifrado de WEP para llevar a cabo ataques que permitan descubrir la clave de cifrado WEP. Para realizar este tipo de ataque, el intruso necesitará capturar varios millones de paquetes protegidos con la misma clave de cifrado.

La mejor forma de mitigar amenazas contra la seguridad de una WLAN basada en WEP es garantizar que las claves utilizadas para cifrar el tráfico de red se actualizan periódicamente. Esto puede hacerse con una frecuencia que impida a posibles atacantes capturar el tráfico suficiente para llevar a cabo un ataque con éxito. Para ello puede establecer las opciones RADIUS de IAS para imponer la reautenticación automática de clientes, que inicia la actualización de clave WEP.

Esta solución configura las opciones RADIUS de IAS para imponer la reautenticación de cliente en Windows XP cada 10 minutos y garantizar que las claves de sesión WEP sean de corta duración. Esta decisión se ha basado en herramientas de ataque y escenarios WEP conocidos en el momento de redactar este capítulo. El cifrado WEP básico incluye errores, como secuencias de vector de inicialización (IV, Initialization Vector) poco eficaces, que los atacantes pueden utilizar para descubrir las claves más rápidamente. Asegúrese de que los puntos de acceso cuentan con la capacidad de generar vectores de inicialización menos previsibles y, por lo tanto, más seguros.

**Importante:** un tiempo de espera de sesión de 10 minutos puede resultar insuficiente en variedad de escenarios. Los tiempos de espera breves suponen una carga inaceptable en los servidores IAS. Además, incrementan la posibilidad de que el servidor IAS deje de funcionar temporalmente, con lo que los clientes perderán la conexión con la WLAN. Por estas razones, puede utilizar un tiempo de espera de 60 minutos sin que el riesgo para la seguridad de la WLAN aumente significativamente.

Además, el uso de EAP-TLS garantiza que se generen claves de sesión WEP únicas para cada cliente durante el proceso de negociación de TLS y se transporten de forma segura por la red entre los componentes de la solución. Al contrario que ocurre con WEP estática, las claves de cifrado no se utilizan más de una vez y no se comparten entre clientes.

**Elección de una estrategia de migración WLAN**

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.

Los estudios demuestran que muchas organizaciones disponen de redes WLAN basadas en 802.11 y que las utilizan sin autenticación de red o protección de datos. Este tipo de estrategia de seguridad de red 802.11 se denomina autenticación de *sistema abierto*. Otras organizaciones han implementado autenticación de red estática y cifrado. Este tipo de seguridad de red 802.11 se conoce como autenticación de *clave compartida*.

Las migraciones desde modelos de seguridad de red de sistema abierto o clave compartida a 802.1X son muy similares. La principal diferencia radica en que la seguridad de clave compartida proporciona una cierta protección de seguridad, con lo que los programas de migración desde seguridad de clave compartida pueden ser más distendidos para algunas organizaciones.

La migración desde cualquiera de estas estrategias de autenticación al modelo de seguridad 802.1X suele comprender los pasos siguientes:

|  |  |
| --- | --- |
| 1. | **Implementación de certificados en equipos y usuarios**: esto debería realizarse con anterioridad a la implementación de 802.1X para garantizar que los certificados se implementan en equipos móviles con acceso ocasional a la LAN. |
| 2. | **Configuración de directivas de acceso remoto a redes inalámbricas en servidores IAS**: incluye la información necesaria para configurar una directiva de acceso remoto inalámbrico. |
| 3. | **Implementación de configuraciones de red inalámbrica en equipos cliente**: generalmente, la nueva red compatible con 802.1X requerirá un nuevo identificador de grupo de servicios (SSID, Service Set Identifier) de red. La configuración de red para este SSID se puede implementar con una directiva de grupo de Active Directory. La directiva de grupo WLAN debe implementarse con suficiente antelación a la reconfiguración de los puntos de acceso inalámbricos para garantizar que los equipos móviles con acceso ocasional a la LAN reciban la configuración de GPO de WLAN. |
| 4. | **Configuración de los puntos de acceso inalámbricos para requerir seguridad 802.1X**: normalmente, este paso se realiza ubicación por ubicación, por ejemplo, en cada campus o edificio del entorno. Se deben planear los procedimientos de restauración apropiados por si se produjera un comportamiento inesperado, y dotar a los servicios de asistencia del personal adecuado para atender las llamadas asociadas. |

Igual que en las estrategias de migración, es esencial realizar un buen planeamiento. La configuración errónea de equipos cliente y puntos de acceso inalámbricos puede ocasionar cambios molestos en el entorno. Pruebe detenidamente los cambios deseados antes de implementarlos.

**Nota:** algunos puntos de acceso inalámbrico admiten la configuración de una radio 802.11 para seguridad de WEP estática y otra radio 802.11 para 802.1X. No obstante, los problemas de separación de canales de 802.11 hacen que esta estrategia resulte poco práctica para la mayoría de las grandes organizaciones.

Obtenga de sus proveedores de equipo WLAN el compromiso de ofrecerle soporte para la actualización de puntos de acceso inalámbricos y NIC inalámbricas a WPA. Microsoft ha publicado una actualización de Windows XP que proporciona compatibilidad con WPA (incluida en el SP2). Asimismo, planee la actualización de la infraestructura WLAN en el futuro para hacerla compatible con 802.11i, que probablemente requerirá actualizaciones del firmware en sus puntos de acceso y NIC inalámbricas.

Esta guía no incluye el planeamiento detallado de la migración para redes WLAN que utilizan seguridad de propietario o seguridad de sistema abierto o clave compartida. Si desea obtener ayuda para el planeamiento detallado de la migración desde redes WLAN de producción, consulte a su socio Microsoft o póngase en contacto con su ejecutivo de cuenta Microsoft, quien puede ponerle en contacto con el socio o profesional de los servicios de consultoría de Microsoft.

**Diseño de la infraestructura de red inalámbrica**

El debate general sobre equipos WLAN basados en 802.11 y diseño de redes queda fuera del alcance de esta guía. El capítulo dedicado a WLAN en el *kit de implementación de Microsoft Windows Server 2003* proporciona amplia información al respecto.

Se ha hecho todo lo posible por garantizar que esta solución funcione con productos de varios proveedores de equipos de red. El planeamiento y los procedimientos de configuración para los productos de punto de acceso inalámbrico específicos quedan fuera del alcance de esta solución.

No obstante, cuando se disponga a considerar la configuración y la administración de seguridad del equipo 802.11, infórmese sobre los temas siguientes utilizando los recursos disponibles del fabricante de hardware:

|  |  |
| --- | --- |
| • | **Nombre SSID y contraseña predeterminada**: este tema incluye el cambio del SSID predeterminado en todos los puntos de acceso y la elección de una estrategia si se desea configurar los puntos de acceso para que difundan sus SSID. |
| • | **Cambio de la contraseña predeterminada de la consola y las cadenas de protocolo simple de administración de redes (SNMP)**: este tema incluye el cambio de las contraseñas de administración y las cadenas de acceso predeterminadas en los puntos de acceso inalámbricos y el mantenimiento de las mismas a lo largo del tiempo. |
| • | **Administración segura de puntos de acceso inalámbricos**: este tema describe el uso de comunicaciones seguras al realizar la administración en puntos de acceso inalámbricos aprovechando protocolos como el protocolo de shell seguro (SSH, Secure Shell) o el protocolo de transferencia de hipertexto (HTTP, Hypertext Transfer Protocol) con SSL o TLS. |
| • | **Configuración de cliente RADIUS**: este tema incluye la configuración de los puntos de acceso para utilizar servidores RADIUS para la autenticación y la contabilidad. Encontrará la descripción de la configuración de puntos de acceso para un servidor RADIUS principal y secundario, el uso de secretos de RADIUS seguros y el atributo autenticador de mensajes en el capítulo 5, "Diseño de una infraestructura de RADIUS para la seguridad de LAN inalámbricas", y en el capítulo 9, "Implementación de la infraestructura de seguridad para LAN inalámbricas". El capítulo 9 incluye instrucciones para el uso de una secuencia de comandos suministrada para la generación de secretos de RADIUS seguros. |
| • | **Conmutación y filtrado de tráfico en una red de área local virtual (VLAN)**: se describe el uso de redes VLAN para restringir el acceso a varios tipos de usuarios en distintos escenarios. IAS puede proporcionar valores RADIUS basados en directivas de acceso remoto para ayudar en la selección automatizada de redes VLAN adecuadas durante la conexión de clientes. Si desea obtener información adicional acerca de las opciones de IAS para especificar redes VLAN en puntos de acceso inalámbricos, consulte las referencias que se incluyen en la sección "Información adicional", al final de este capítulo. |
| • | **Táctica para limitar las fugas de las transmisiones por radio de redes LAN inalámbricas fuera de los límites del edificio**: este tema incluye consejos como, por ejemplo, sobre la colocación de puntos de acceso en paredes o ventanas que dan al exterior, algo que debe evitarse. También incluye la reducción de la intensidad de la difusión de los puntos de acceso en la medida de lo posible para limitar la cobertura al área necesaria y evitar cubrir otras áreas, como aparcamientos, de forma no intencionada. |
| • | **Detección de puntos de acceso inalámbricos falsos**: este tema incluye la exploración activa y periódica para detectar puntos de acceso falsos en la red corporativa utilizando herramientas de administración de WLAN disponibles basadas en Windows XP y Windows CE, como NetStumbler o AirMagnet. |

Si desea obtener ayuda en torno a estos temas y la configuración de puntos de acceso inalámbricos, consulte la documentación específica del proveedor o solicite la ayuda de un especialista en este tipo de equipos. Varios de estos temas se tratan en el documento "802.11 Wireless Network Technical Reference", que ofrece información técnica sobre redes inalámbricas 802.11 y que se incluye en la *guía de referencia técnica de Windows Server 2003* en la sección "Información adicional" al final de este capítulo.

**Consideraciones entorno a directivas de grupo de redes inalámbricas**

Consulte a sus administradores de GPO del dominio para determinar la estrategia adecuada de aplicación de la directiva de grupo de red inalámbrica a los equipos cliente. En la tabla siguiente se enumeran los elementos clave sobre los que tendrá que tomar decisiones para su entorno y la configuración que se ha seleccionado en esta solución.

**Tabla 6.7: Planeamiento de la directiva de red inalámbrica**

| **Consideración de la directiva de red inalámbrica** | **Estrategia de la solución** | **Detalles de la solución** |
| --- | --- | --- |
| Criterios de aplicación de la directiva | Filtrado de grupo de seguridad de Active Directory para incluir los equipos seleccionados. | Directiva de red inalámbrica - Grupo global de equipos. |
| Número de GPO necesarios | Directiva de red inalámbrica única. | El GPO utilizado en esta solución se denomina “directiva de red inalámbrica”. |
| Ubicación de GPO | Creado y aplicado desde el objeto de dominio. | woodgrovebank.com |
| Número de perfiles WLAN configurados dentro de la directiva | Un perfil WLAN se configura para las organizaciones que implementan 802.1X. | El GPO contiene un perfil WLAN para entornos cuyas WLAN no se encuentran en uso productivo.  Se pueden agregar perfiles WLAN adicionales a medida que se necesitan para una migración por fases desde una WLAN de producción heredada. |

**Nota:** esta solución concede a un grupo de seguridad personalizado (directiva de red inalámbrica - equipo) el permiso de aplicación de directiva en el GPO de directiva de red inalámbrica. Por lo tanto, la pertenencia a este grupo determina los equipos que recibirán la configuración de GPO de WLAN. Si desea que todos los equipos reciban la configuración de la WLAN, puede incluir los grupos de usuarios autenticados o equipos del dominio a este grupo para simplificar el proceso de administración. Sin embargo, tenga en cuenta que, al hacerlo, la configuración de la directiva se aplicará a todos los servidores y clientes del dominio (equipos del dominio) o del bosque (usuarios autenticados).

Esta solución presenta una estrategia de administración de directivas de red inalámbrica simplificada mediante la creación de un único GPO y vinculado al objeto de dominio. Esto significa que cualquier equipo del dominio que sea miembro del grupo de directiva de red inalámbrica - equipo recibirá la configuración de la directiva. Quizás debería considerar estándares de administración de directivas de grupo más sofisticados para aplicarlos a las directivas de red inalámbrica en consecuencia. Sin embargo, muchas organizaciones se encontrarán con la necesidad de crear un único GPO de directiva de red inalámbrica, aunque optarán por vincularlo a una ubicación distinta del objeto de dominio.

[Principio de la páginaPrincipio de la página](http://www.microsoft.com/latam/technet/articulos/wireless/pgch06.mspx#top)

**Determinación de la configuración de software necesaria para redes WAN 802.1X**

Esta solución consta de dos componentes principales de software que deben configurarse para conseguir la seguridad de una red WLAN 802.1X:

|  |  |
| --- | --- |
| • | directiva de acceso de red basada en IAS. |
| • | directiva de grupo basada en Active Directory para equipos cliente. |

La directiva de acceso de red basada en IAS constituye la base de la solución de administración del acceso de red. La configuración que representa la directiva de seguridad de WLAN se implementa en cada servidor RADIUS basado en IAS de forma automatizada. Esta directiva incluye configuración para:

|  |  |
| --- | --- |
| • | Directivas de acceso remoto |
| • | Directivas de solicitud de conexión |

Las directivas de acceso remoto imponen el acceso a las redes a través de los puntos de acceso inalámbricos. Las directivas de solicitud de conexión determinan el tratamiento de las solicitudes RADIUS de varios puntos de acceso inalámbricos configurados como clientes RADIUS.

La directiva de grupo basada en Active Directory para equipos cliente contiene toda la configuración que se implementará en los equipos cliente basados en Windows XP. Esta directiva de grupo afecta a la interacción del cliente con los puntos de acceso inalámbricos, el servidor RADIUS y otras redes inalámbricas.

**Configuración de directivas de acceso remoto**

Debe planear la creación de las directivas de acceso remoto en servidores IAS para que se adapten a las necesidades de la estrategia de acceso de red inalámbrica de la organización. La creación y configuración de directivas de acceso remoto implica el establecimiento de tres tipos de configuración para cada directiva:

|  |  |
| --- | --- |
| • | Condiciones de la directiva |
| • | Permiso de la directiva |
| • | Perfil de la directiva |

Esta solución utiliza una única directiva de acceso remoto que otorga acceso ilimitado a la red inalámbrica a los empleados a tiempo completo. En la tabla siguiente se detallan las condiciones de la directiva de acceso remoto elegidas para esta solución.

**Tabla 6.8: Condiciones de la directiva de acceso remoto**

| **Condición de la directiva** | **Condición equivalente** | **Comentarios** |
| --- | --- | --- |
| NAS - Puerto - Tipo | Inalámbrico - Otro  o bien  Inalámbrico - IEEE 802.11 | Esto identifica las solicitudes entrantes como originadas en hardware de puntos de acceso inalámbricos. |
| Windows - Grupo | Pertenencia al grupo de seguridad de directiva de acceso remoto - acceso inalámbrico | Éste es un grupo de seguridad universal que contiene grupos globales anidados para usuarios y equipos que obtendrán acceso a la WLAN. |

El permiso de la directiva para la directiva de acceso remoto de esta solución está establecido en **conceder** y las cuentas de usuario están configuradas con el valor de **controlar el acceso a través de la directiva de acceso remoto**.

En la tabla siguiente se detallan las opciones del perfil de la directiva de acceso remoto utilizadas en esta solución. Tal vez sea necesario agregar otras opciones de configuración para ajustarla al entorno específico.

**Tabla 6.9: Opciones del perfil de la directiva de acceso remoto**

| **Opción de perfil** | **Valor de perfil** | **Comentarios** |
| --- | --- | --- |
| Restricciones de marcado: establece los minutos que el cliente puede permanecer conectado (tiempo límite de sesión). | 10 minutos | Esta opción obliga a los equipos cliente a reautenticarse y crear claves de cifrado nuevas cada 10 minutos. |
| Autenticación - Métodos EAP | Tarjeta inteligente u otro certificado | Esta opción selecciona EAP - TLS como el tipo de EAP para el perfil inalámbrico. |
| Atributo RADIUS omitir - usuario - propiedades de marcado | Atributo establecido como Verdadero | Este atributo garantiza que la configuración de marcado (como la devolución de llamada) en cuentas de usuario de Active Directory no se envíe a los puntos de acceso inalámbricos. Esto se hace para evitar problemas con algunos productos de acceso de red. |
| Atributo RADIUS Acción-Terminación | Atributo establecido como Solicitud RADIUS | Este atributo garantiza que cuando se obliga a los clientes a reautenticarse, los puntos de acceso inalámbricos no los desconectarán. |

**Importante:** un tiempo de espera de sesión de 10 minutos puede resultar insuficiente en variedad de escenarios. Los tiempos de espera breves suponen una carga inaceptable en los servidores IAS. Además, incrementan la posibilidad de que el servidor IAS deje de funcionar temporalmente, con lo que los clientes perderán la conexión con la WLAN mucho antes. Por estas razones, puede utilizar un tiempo de espera de 60 minutos sin que el riesgo para la seguridad de la WLAN aumente significativamente.

**Configuración de directivas de solicitud de conexión**

Debe planear la forma en que IAS tratará las solicitudes RADIUS cuando funcione como servidor RADIUS y como proxy RADIUS. Encontrará las consideraciones sobre la selección de la función RADIUS para IAS en el capítulo 5, "Diseño de una infraestructura de RADIUS para la seguridad de LAN inalámbricas".

Independientemente de la función que elija para el servidor IAS, deberá configurar los componentes siguientes de las directivas de solicitud de conexión para obtener acceso a la red inalámbrica:

|  |  |
| --- | --- |
| • | Condiciones de la directiva |
| • | Perfil de la directiva |

Esta solución utiliza IAS como servidor RADIUS y, por tanto, las solicitudes de conexión se procesan localmente en cada servidor. La configuración que se detalla en la tabla siguiente muestra las condiciones de directiva configuradas en la directiva de solicitud de conexión de esta solución.

**Nota:** la configuración de la directiva de solicitud de conexión de esta solución utiliza los valores predeterminados que se instalan con IAS en Windows Server 2003.

**Tabla 6.10: Condiciones de la directiva de solicitud de conexión**

| **Condición de la directiva** | **Condición equivalente** | **Comentarios** |
| --- | --- | --- |
| Restricciones de fecha y hora | "Domingo 00:00 - 24:00;Lunes 00:00 - 24:00;Martes 00:00 - 24:00; Miércoles 00:00 - 24:00; Jueves 00:00 - 24:00;  Viernes 00:00 - 24:00;  Sábado 00:00 - 24:00" | Esta condición de la directiva de solicitud de conexión predeterminada garantiza que las solicitudes de conexión que lleguen en todo momento se ajusten a la directiva. |

En la tabla siguiente se muestra la configuración de perfil utilizada en la directiva de solicitud de conexión de esta solución.

**Tabla 6.11: Configuración del perfil de la directiva de solicitud de conexión**

| **Opción de perfil** | **Valor de perfil** | **Comentarios** |
| --- | --- | --- |
| Autenticación | Autenticar solicitudes en este servidor | Esta configuración garantiza que las solicitudes se autenticarán directamente contrastándolas con Active Directory en lugar de reenviarlas a servidores RADIUS adicionales. |

**Configuración de la directiva de grupo para equipos cliente**

Antes de utilizar una directiva de grupo basada en Active Directory para configurar los parámetros de la WLAN y la configuración de seguridad de 802.1X en equipos cliente a través de directivas de redes inalámbricas (IEEE 802.11) es necesario realizar un cierto planeamiento. En esta sección se describen varias opciones de configuración elegidas para esta solución y los motivos para cada una de ellas. Las directivas de red inalámbrica (IEEE 802.11) se pueden encontrar en el objeto \configuración del equipo\configuración de Windows\configuración de seguridad\directivas de redes inalámbricas (IEEE 802.11) en el editor de objetos de la directiva de grupo.

**Configuración de los parámetros de la red inalámbrica**

La configuración de los parámetros de la WLAN se realiza editando las propiedades de los objetos de directiva de la WLAN dentro de la directiva de grupo: Se incluyen los siguientes tipos de configuración:

|  |  |
| --- | --- |
| • | Configuración general |
| • | Redes preferidas |
| • | Propiedades de red |

En la tabla siguiente se muestra la configuración general de la directiva de redes inalámbricas elegida para esta solución.

**Tabla 6.12: Configuración general de directivas de redes inalámbricas**

| **Opción** | **Configuración** | **Comentarios** |
| --- | --- | --- |
| Nombre | Configuración inalámbrica de equipo cliente | Cambie este valor para adaptarlo a los estándares de nomenclatura de la organización. |
| Red de acceso | Cualquier red disponible (preferiblemente punto de acceso) | Esta opción impedirá que los equipos cliente intenten conectar a otros equipos configurados con el mismo SSID que la red habilitada para 802.1X. No obstante, permitir el acceso a redes ad-hoc hace posible que los empleados utilicen otras redes cuando sea necesario (en su domicilio, por ejemplo) y, por tanto, se ha dejado habilitada. |
| Conectar automáticamente a redes no preferidas | Sin seleccionar | Windows XP Professional proporciona automáticamente a los usuarios notificación de las redes inalámbricas disponibles sin conectar automáticamente a las mismas. Al proporcionar a los usuarios notificación sin conexión automática se consigue un equilibrio entre seguridad y utilidad. |

Debe crear una entrada para el SSID de WLAN 802.1X en la ficha de **redes preferidas** de la directiva de redes inalámbricas. Una vez se ha creado una red preferida, se deben editar las propiedades de red a partir de los valores predeterminados.

En la tabla siguiente se describe la configuración de las propiedades de la red para la red 802.1X que se acaba de habilitar en la directiva de redes inalámbricas de esta solución.

**Tabla 6.13: Configuración de las propiedades de la directiva de redes inalámbricas**

| **Opción** | **Configuración** | **Comentarios** |
| --- | --- | --- |
| Nombre | MSSWLAN | Cambie este valor para adaptarlo a los estándares de nomenclatura de la organización. Debe asegurarse de elegir un nombre que sea distinto del resto de redes WLAN de producción existentes. |
| Clave de red inalámbrica (WEP) – Cifrado de datos (WEP habilitada) | Seleccionado | El cifrado es esencial para proteger la privacidad del tráfico de la red inalámbrica en redes 802.11. Si tiene compatibilidad con redes 802.11, debe asegurarse de que estén protegidas por WEP o alguna otra forma de cifrado. |
| Clave de red inalámbrica (WEP) – Autenticación de red (modo compartido) | Sin seleccionar | 802.11 inalámbrico de clave compartida es una estrategia de seguridad basada en claves WEP estáticas. Esta solución utiliza 802.1X para proporcionar autenticación de RADIUS y, por tanto, esta opción no se activa. |
| Clave de red inalámbrica (WEP) – La clave de red se proporciona automáticamente. | Seleccionado | Esta opción permite a 802.1X proporcionar claves de sesión WEP dinámicas para el cifrado del tráfico de forma automática. |
| Ésta es una red de equipo a equipo (ad-hoc); no se utilizan puntos de acceso inalámbricos. | Sin seleccionar | Esta solución utiliza el modo de infraestructura de WLAN 802.11 con puntos de acceso inalámbricos configurados para 802.1X en lugar del acceso a redes ad-hoc punto a punto. |

**Configuración de los parámetros de 802.1X en equipos cliente**

La configuración de los parámetros de 802.1X se realiza mediante la directiva de redes inalámbricas e incluye los siguientes tipos de configuración:

|  |  |
| --- | --- |
| • | Parámetros de 802.1X |
| • | Tipo EAP |
| • | Validación de credenciales |
| • | Comportamiento de la autenticación de equipos |

La tabla siguiente contiene la configuración de 802.1X para la red 802.1X que se acaba de habilitar en la directiva de redes inalámbricas elegida para esta solución.

**Tabla 6.14: Configuración de la directiva de redes inalámbricas para 802.1X**

| **Opción** | **Configuración** | **Comentarios** |
| --- | --- | --- |
| Habilitar el control de acceso a la red mediante IEEE 802.1X | Habilitada | Esta opción permite al equipo cliente participar en redes protegidas mediante 802.1X. |
| Mensaje EAPOL - Inicio | Transmitir | Este mensaje indica al cliente que inicie el proceso de autenticación. |
| Parámetros (segundos) - Inicio máx. | 3 | Este valor determina el número de mensajes EAP a través de LAN (EAPOL) - Inicio sucesivos que transmitirá este cliente tras no recibir ninguna respuesta. A menos que se requiera lo contrario, este valor predeterminado no debe modificarse. |
| Parámetros (segundos) - Período de retención | 60 | Este valor determina el período de tiempo que el cliente esperará antes de volver a intentar la autenticación en 802.1X. A menos que se requiera lo contrario, este valor predeterminado no debe modificarse. |
| Parámetros (segundos) - Período de inicio | 60 | Este valor determina el intervalo de tiempo entre los mensajes EAPOL - Inicio que se reenvían. A menos que se requiera lo contrario, este valor predeterminado no debe modificarse. |
| Período de autenticación | 30 | Este valor determina el intervalo de tiempo entre los mensajes de solicitud de 802.1X que se reenvían tras no recibir ninguna respuesta. A menos que se requiera lo contrario, este valor predeterminado no debe modificarse. |
| Tipo EAP | Tarjeta inteligente u otro certificado | Esta opción especifica EAP-TLS como tipo EAP. |

A continuación se describe la configuración de EAP para la red 802.1X que se acaba de habilitar en la directiva de redes inalámbricas elegida para esta solución.

**Tabla 6.15: Configuración EAP de directivas de redes inalámbricas**

| **Opción** | **Configuración** | **Comentarios** |
| --- | --- | --- |
| Al conectar | Utilizar un certificado en este equipo. | Esta opción especifica el uso de certificados basados en software y claves privadas en lugar de credenciales basadas en tarjeta inteligente. |
| Usar un certificado en este equipo - Utilizar selección de certificado simple (se recomienda) | Seleccionado | Esta opción determina que Windows intentará elegir el certificado más adecuado según las propiedades de certificado. Se puede desactivar para permitir la selección manual del certificado correcto durante la solución de problemas. |
| Validar certificado de servidor | Seleccionado | Esta opción determina si el certificado presentado al cliente durante la autenticación EAP-TLS es válido (que el nombre DNS correcto del servidor IAS está en el certificado y que el certificado para la autenticación del servidor no ha caducado y está encadenado a una entidad emisora raíz en el almacén de certificados del cliente). |
| Validar certificado de servidor - Conectar a estos servidores | Sin seleccionar | Esta opción habilita la comprobación del sufijo del nombre de dominio completo (FQDN, Fully Qualified Domain Name) en el campo de sujeto del certificado del servidor. Al habilitar esta opción se visualizará un globo de texto en los equipos cliente donde se les solicitará que confirmen que el servidor IAS es de confianza. Si selecciona esta opción debe evaluar el equilibrio entre aprovechamiento y seguridad. |
| Validar certificado de servidor - Conectar a estos servidores - Valor | Vacío | Este valor especifica el sufijo FQDN con el que debe coincidir la información de sujeto del certificado presentado al cliente durante la autenticación EAP-TLS. |
| Entidades emisoras de certificados (CA) raíz de confianza | Entidad emisora de certificados empresa seleccionada | Esta opción permite a los administradores especificar las entidades emisoras raíz de confianza con las que se permite el encadenamiento de las credenciales de certificado del servidor 802.1X. Para esta opción, debe seleccionar sus propias entidades emisoras raíz de confianza. |
| Usar un nombre distinto para la conexión | Sin seleccionar | Permite a los usuarios especificar un nombre de usuario distinto al que contiene el certificado presentado durante la autenticación EAP-TLS. Esta opción está deshabilitada de forma predeterminada. |

En la tabla siguiente se detalla la configuración de la autenticación de equipos para la red 802.1X que se acaba de habilitar en la directiva de redes inalámbricas elegida para la solución.

**Tabla 6.16: Opciones de comportamiento de autenticación de equipos en 802.1X**

| **Opción** | **Configuración** | **Comentarios** |
| --- | --- | --- |
| Autenticar como invitado cuando la información de usuario o equipo no esté disponible | Sin seleccionar | Esta opción determina si el equipo intentará autenticarse como invitado cuando no haya credenciales disponibles. Resulta especialmente útil para escenarios de redes WLAN públicas o para visitantes en la organización. |
| Autenticar como equipo cuando la información del equipo esté disponible | Seleccionado | Esta opción es esencial para garantizar que se produzca la autenticación del equipo cuando no haya usuarios en una sesión interactiva en el mismo. |
| Autenticación de equipo | Con reautenticación de usuario | Esta opción predeterminada garantiza que las credenciales de usuario se utilicen siempre que sea posible. No obstante, cuando ningún usuario ha iniciado una sesión en el equipo, las credenciales de equipo se utilizan para garantizar que haya siempre una conexión de red disponible. |

[Principio de la páginaPrincipio de la página](http://www.microsoft.com/latam/technet/articulos/wireless/pgch06.mspx#top)

**Consideraciones adicionales**

En esta sección se mencionan brevemente algunos temas que deben tenerse en cuenta pero que quedan fuera del alcance de esta solución, aunque puede ser que ejerzan un impacto en el entorno.

**Compatibilidad con perfiles móviles y usuarios itinerantes**

Los componentes 802.1X basados en EAP-TLS de Windows dependen de que los certificados y el material de clave privada estén disponibles en el almacén de certificados de los equipos cliente. En muchas organizaciones, los usuarios inalámbricos utilizan equipos portátiles o Tablet PC que llevan consigo y, de este modo, los certificados y el material de claves están siempre disponibles.

No obstante, si en su estrategia de WLAN se incluye la existencia de usuarios que comparten equipos, debería considerar la implementación de perfiles móviles. Los perfiles móviles se pueden utilizar para garantizar que la información de las claves privadas y los certificados estén siempre disponibles para utilizarlos en su entorno basado en 802.1X.

Alternativamente, la directiva de redes inalámbricas permite configurar los equipos con Windows XP para realizar autenticación sólo de equipo. Aunque no se implementa en esta solución, podría resultar útil para algunas organizaciones.

**Compatibilidad con clientes sin conexiones LAN de cableado**

Aunque no suele ser el caso en las organizaciones grandes, es posible que algunos entornos no cuenten con LAN por cable. Esta infraestructura es necesaria a la hora de unir equipos cliente a un dominio y recibir de este modo los certificados y la directiva de grupo. Sin certificados de equipo y usuario, ni la configuración adecuada de la WLAN en el cliente, los usuarios no podrán acceder a la WLAN basada en 802.1X. Éste es también el caso cuando una organización implementa una red por cable que requiere siempre autenticación de 802.1X.

Si tiene un entorno de este tipo, debería considerar una estrategia en la que los usuarios proporcionen una credencial basada en contraseñas utilizando PEAP-MSCHAPv2 al servidor RADIUS para la conexión a una VLAN controlada con las páginas de inscripción Web de Servicios de Certificate Server. Desde ahí, los usuarios pueden inscribir e instalar certificados para obtener acceso total a la red WLAN de la empresa utilizando EAP-TLS. Esta estrategia actualmente queda fuera del alcance de esta solución y requeriría una directiva de acceso remoto adicional para los servidores IAS, además de un diseño específico de la VLAN.

[Principio de la páginaPrincipio de la página](http://www.microsoft.com/latam/technet/articulos/wireless/pgch06.mspx#top)

**Resumen**

Este capítulo se ocupa del proceso de diseño de la seguridad de redes WLAN mediante el uso de 802.1X e incluye la determinación de los requisitos previos, la consideración de las opciones de seguridad, el establecimiento de una estrategia y consideraciones adicionales. Una vez establecido el diseño a partir de las opciones cubiertas en este capítulo, podrá implementar la seguridad de redes WLAN basadas en 802.1X en su entorno.

El diseño que se describe aquí se utilizará en los capítulos de generación y operaciones de esta solución para implementar la infraestructura de seguridad de WLAN 802.1X.

**Información adicional**

Si desea obtener información adicional acerca de redes inalámbricas seguras, consulte:

|  |  |
| --- | --- |
| • | El sitio Web de la [documentación del producto Windows Server 2003](http://www.microsoft.com/windowsserver2003/proddoc/default.mspx) en http://www.microsoft.com/windowsserver2003/proddoc/default.mspx.  La documentación del producto ofrece una descripción general de las características de IAS, instrucciones básicas de configuración y las mejores prácticas de implementación. |
| • | La solución de Microsoft [*Seguridad en LAN inalámbricas con PEAP y contraseñas*](http://go.microsoft.com/fwlink/?LinkId=23459), que está disponible en http://go.microsoft.com/fwlink/?LinkId=23459*.* |
| • | El capítulo “[IAS Technical Reference](http://www.microsoft.com/resources/documentation/windowsServ/2003/all/techref/en-us/W2K3TR_ias_intro.asp)” de la *guía de referencia técnica de Microsoft Windows Server 2003* en http://www.microsoft.com/resources/documentation/windowsServ/2003/all/techref/en-us/W2K3TR\_ias\_intro.asp.  Este capítulo del kit de recursos proporciona información técnica sobre IAS más detallada que la documentación del producto y puede utilizarse como referencia en caso de necesitar información adicional.   |  |  | | --- | --- | | La [*guía de referencia técnica de Microsoft Windows Server 2003*](http://www.microsoft.com/windows/reskits/default.asp) y el[*kit de implementación de Microsoft Windows Server 2003*](http://www.microsoft.com/windows/reskits/default.asp) en http://www.microsoft.com/windows/reskits/default.asp. | | | • | El capítulo “Deploying a Wireless LAN”, que trata de la implementación de una LAN inalámbrica, incluido en la guía *Deploying Network Services*, sobre implementación de servicios de red, del [*kit de implementación de Microsoft Windows Server 2003*](http://www.microsoft.com/windowsserver2003/techinfo/reskit/deploykit.mspx)en http://www.microsoft.com/windowsserver2003/techinfo/reskit/deploykit.mspx.  Este capítulo del kit de implementación contiene instrucciones de implementación para el uso de IAS en distintos escenarios que quedan fuera del alcance de esta guía sobre seguridad de redes inalámbricas pero que afectan a las decisiones sobre diseño. | | • | Encontrará información exhaustiva sobre WLAN 802.1X, problemas de seguridad de WLAN y estándares relacionados en la página Web no oficial sobre seguridad de 802.11,<http://www.drizzle.com/~aboba/IEEE/>. | | • | Para obtener información sobre soluciones de WLAN y sobre el sector, visite el sitio Web de la [Wi-Fi Alliance](http://www.wi-fialliance.org/) en http://www.wi-fialliance.org. | | • | Para obtener información sobre WLAN, con información general, estudios de mercado, notas de producto y programas de aprendizaje, visite el [centro de formación de la asociación de LAN inalámbricas (WLANA, Wireless LAN Association)](http://www.wlana.org/learning_center.html) en http://www.wlana.org/learning\_center.html. | | • | Para obtener información sobre EAP-TLS, EAPOL, EAP-RADIUS, RADIUS y otros estándares de Internet que se utilizan con 802.1X, visite el sitio Web del grupo de trabajo de ingeniería de Internet (IETF, The Internet Engineering Task Force) en <http://www.ietf.org/>. | | • | Si desea información sobre estándares de WLAN relevantes, que incluyen 802.11, 802.11a, 802.11b, 802.1X y 802.11i, entre otros, visite el sitio Web de la [zona de estándares inalámbricos del IEEE](http://standards.ieee.org/wireless/) en http://standards.ieee.org/wireless/. | | • | La guía [802.11 Wireless Technical Reference](http://www.microsoft.com/resources/documentation/windowsServ/2003/all/techref/en-us/W2K3TR_wir_intro.asp), con información técnica sobre redes inalámbricas 802.11, está disponible en http://www.microsoft.com/resources/documentation/windowsServ/2003/all/techref/en-us/W2K3TR\_wir\_intro.asp. | |

Tutorial completo

<http://www.virusprot.com/cursos/redes-inal%C3%A1mbricas-curso-gratis0.htm>