Latinoamérica

Microsoft TechNet

Seguridad en LAN inalámbricas con PEAP y contraseñas

Capítulo 1: Seguridad en LAN inalámbricas con PEAP y contraseñas

Actualizado: abril 2, aaaa

Ver todos los temas de la guía de seguridad

En esta página

- Introducción
- Información general de la solución
- Convenciones de estilo
- Soporte técnico y comentarios

Descargue la solución completa en

Seguridad en LAN inalámbricas con PEAP y contraseñas

Descargar la solución completa

Guía de defensa en profundidad antivirus

En esta guía

- Introducción: Elección de una estrategia para la seguridad en LAN inalámbricas
- Capítulo 0 - Descripción general
- Capítulo 1 - Introducción
- Capítulo 2 - Planeamiento
- Capítulo 3 - Preparación
- Capítulo 4 - Creación de la entidad emisora de certificados de red
- Capítulo 5 - Creación de la infraestructura
- Capítulo 6 - Configuración
- Capítulo 7 - Prueba
- Capítulo 8 - Mantenimiento
- Apéndice A - Uso de PEAP en la empresa
- Apéndice B - Uso de WPA en la solución
- Apéndice C - Versiones de sistemas operativos compatibles
- Apéndice D - Secuencias de comandos y archivos auxiliares

Introducción

Hoy en día, la tecnología inalámbrica es un tema de debate de gran actualidad en el mundo empresarial. La mayoría de las organizaciones ya han implementado redes de área local inalámbricas (WLAN) o están en plena discusión sobre las ventajas e inconvenientes de esta tecnología. Son innegables las mejoras en productividad percibidas por los usuarios y el atractivo que suponen las redes de bajo mantenimiento para los departamentos de tecnología de la información (TI). No obstante, la gran preocupación por la seguridad de la mayoría de los directores de TI ha hecho que reaccionen con prudencia, si no con rotunda hostilidad, ante la idea de introducir redes WLAN en las organizaciones. Al mismo tiempo, la implementación de las soluciones propuestas por los analistas y proveedores de redes para afrontar estas preocupaciones ha parecido demasiado compleja y costosa.

Seguridad en LAN inalámbricas con PEAP y contraseñas es la segunda solución de seguridad para WLAN de Microsoft®. Es un complemento de la primera solución, *Solución de Seguridad de LAN inalámbricas — Servicios de Certificate Server de Microsoft Windows Server 2003*. Mientras que la primera solución estaba dirigida a grandes organizaciones, ésta es considerablemente más sencilla, más fácil de implementar y está diseñada para organizaciones pequeñas y medianas. La primera diferencia tecnológica entre las dos soluciones es que la primera utiliza certificados con clave pública para autenticar el acceso de usuarios y equipos a WLAN, mientras que la segunda utiliza nombres de usuario y contraseñas. Otra característica distintiva de esta solución es el uso de hardware existente del servidor (en lugar de utilizar hardware nuevo), el empleo de un modelo de delegación administrativa más sencillo y la automatización de muchas más tareas de configuración mediante secuencias de comandos y configuraciones predefinidas.

La documentación de esta solución presenta dos características significativas que la distinguen de la documentación general de productos del sistema operativo Microsoft Windows® y de muchas notas técnicas del producto de Microsoft. La primera es la naturaleza *normativa* de la guía, en la que las opciones de diseño estaban disponibles y las decisiones se tomaron en base a los conocimientos obtenidos a partir de la implementación interna y los comentarios de los clientes recibidos por Microsoft. La solución se basó en estas prácticas recomendadas y se creó y probó en los laboratorios de Microsoft para garantizar que el funcionamiento de la solución era el esperado. La segunda característica es que se trata de una solución *integral* que engloba el ciclo completo de diseño, planeamiento,

creación, prueba y administración de la solución.

Como se detallará en los capítulos siguientes, la solución se basa en el estándar 802.1X del Instituto de ingenieros de electricidad y electrónica (IEEE) y requiere una infraestructura RADIUS (Servicio de usuario de acceso telefónico de autenticación remota). Se sirve de una arquitectura flexible que se puede adaptar tanto a organizaciones con decenas de usuarios, como a aquéllas con miles de ellos. La solución se creó y probó en equipos cliente con Microsoft Windows® XP, con Microsoft Pocket PC 2003 y en servidores con Microsoft Windows Server™ 2003.

Principio de la página

Información general de la solución

Esta guía se divide en cuatro secciones, cada una de la cuales corresponde a una fase del ciclo de la solución. Estas fases son el planteamiento, la implementación, la prueba y el funcionamiento. Dichas fases se vuelven a dividir en capítulos.

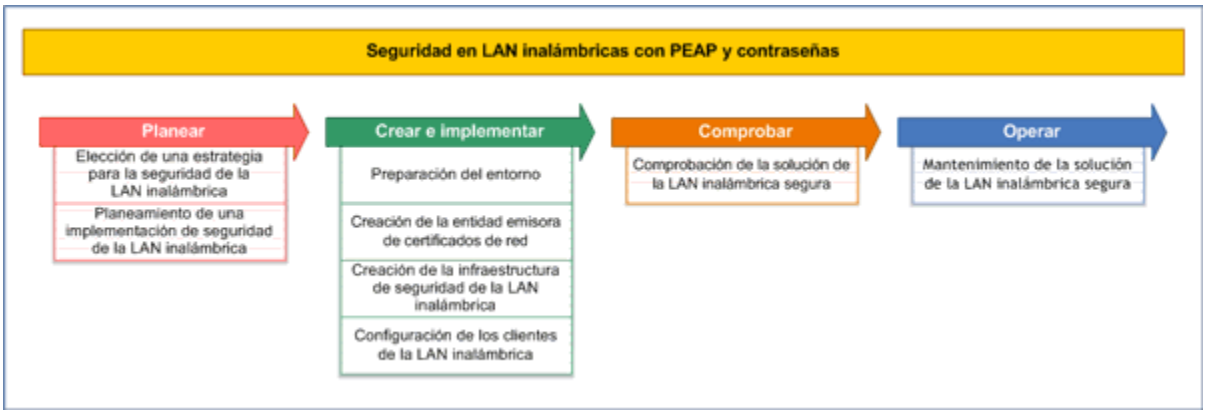

Figura 1.1. Información general de Seguridad en LAN inalámbricas
Vista de imagen a pantalla completa

La sección de planeamiento consiste en una introducción, "Elección de una estrategia para la seguridad en LAN inalámbricas" y el capítulo 2, "Planeamiento de la implementación de seguridad en LAN inalámbricas". Los cuatro capítulos siguientes constituyen la sección de la guía dedicada a la creación e implementación. Estos capítulos ofrecen instrucciones para implementar los servidores RADIUS utilizando el Servicio de autenticación de Internet (IAS) de Windows Server 2003, así como para implementar los equipos clientes inalámbricos y la infraestructura compatible. Cada capítulo ofrece procedimientos detallados sobre la instalación y configuración de los componentes de software, y sobre el modo de integrarlos en la solución. También incluyen procedimientos de comprobación que ayudan a minimizar errores.

La sección dedicada a la prueba cubre un capítulo que explica cómo confirmar que la solución funciona correctamente antes de su implementación. La sección sobre el funcionamiento ocupa también un único capítulo. Éste explica cómo manejar, supervisar y modificar todos los componentes de la solución, y cómo solucionar los problemas de éstos.

La guía viene acompañada de un conjunto de herramientas y de secuencias de comandos utilizadas para automatizar muchas de las tareas de implementación y funcionamiento.

La siguiente sección ofrece una descripción más detallada de cada capítulo.

Elección de una estrategia para la seguridad en LAN inalámbricas

Este documento sirve de introducción a las dos soluciones de seguridad en WLAN descritas anteriormente. Su objetivo es ayudarle a seleccionar la estrategia adecuada para la infraestructura de seguridad de la red inalámbrica. Describe las razones empresariales que conducen a la adopción de la tecnología WLAN y las preocupaciones sobre la seguridad que la rodean. Trata las diferentes opciones disponibles para abordar estas preocupaciones y destaca una solución basada en la autenticación segura y en la protección de los datos de red.

Del mismo modo, contiene un análisis sobre los méritos relativos de los diferentes enfoques sobre seguridad en WLAN, incluidas las soluciones originarias de seguridad en WLAN, las redes privadas virtuales (VPN) y la seguridad IP.

Capítulo 1: Seguridad en LAN inalámbricas con PEAP y contraseñas

Este capítulo es el que nos ocupa y proporciona información general sobre el contenido de la guía de la solución.

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

Este capítulo describe el diseño de la arquitectura de la solución de seguridad en LAN inalámbricas. Cubre los siguientes temas:

- Funcionamiento de una solución basada en el protocolo 802.1X y en el Protocolo de autenticación extensible protegido (PEAP).
- Descripción de la organización de destino para esta solución y los criterios de diseño clave de la solución.
- Desarrollo de un diseño de la solución de seguridad en WLAN según las necesidades de la organización de destino.
- Adaptación del diseño básico a organizaciones de mayor tamaño.
- Análisis de las variaciones del diseño para ajustarse a las necesidades que no se encuentran en la solución, como la introducción de VPN o de redes 802.1X con cable.

El capítulo se centra en el diseño de una infraestructura RADIUS (utilizando IAS, la implementación RADIUS incluida en Windows Server) para proporcionar una autenticación segura y servicios de administración clave. El capítulo incluye además un análisis de los equipos cliente inalámbricos compatibles con la solución y con los requisitos de certificados.

Capítulo 3: Preparación del entorno

Este capítulo se ocupa de la tecnología de la información (TI) subyacente necesaria para admitir esta solución de WLAN. Describe la preparación del directorio activo de Microsoft Active Directory®, el Protocolo de configuración dinámica de host (DHCP), los servicios del Sistema de nombres de dominio (DNS) y los requisitos de redes subyacentes. Además incluye una serie de procedimientos para aplicar las configuraciones de seguridad y para instalar las actualizaciones de seguridad necesarias en los servidores utilizados en la solución.

Capítulo 4: Creación de la entidad emisora de certificados de red

Este capítulo describe cómo instalar una sencilla entidad emisora de certificados en un controlador de dominio con el objetivo de proporcionar certificados a los servidores IAS. Los procedimientos para su consecución se automatizan en gran parte mediante secuencias de comandos incluidas en la guía. La entidad emisora creada para esta solución se dedica a la tarea específica de emitir certificados para los servidores IAS y, en consecuencia, requiere un mantenimiento escaso o periódico.

Capítulo 5: Creación de la infraestructura de seguridad en LAN inalámbricas

Este capítulo ofrece instrucciones sobre la implementación de los componentes de seguridad en WLAN, los servidores IAS y los puntos de acceso inalámbricos. Incluye instrucciones paso a paso sobre cómo instalar IAS en un controlador de dominio (o servidor miembro), cómo establecer la configuración y las directivas de IAS, cómo instalar puntos de acceso inalámbricos para utilizar los servidores IAS y cómo replicar la configuración de IAS entre los servidores IAS.

Capítulo 6: Configuración de clientes de LAN inalámbricas

Este capítulo contiene los procedimientos necesarios para configurar los clientes compatibles con esta solución. Las tres secciones principales del capítulo se centran en el control del acceso de usuarios y equipos a la WLAN, la configuración de las directivas de grupo para clientes WLAN en Windows XP y la configuración manual de WLAN para los clientes Pocket PC 2003.

Capítulo 7: Prueba de soluciones de seguridad en LAN inalámbricas

Este capítulo es el resultado del plan de prueba utilizado por el equipo de Microsoft al probar esta solución. Los capítulos dedicados a la creación (3-6) contienen procedimientos de comprobación habituales utilizados en todo el proceso de creación para comprobar que todo avanzaba correctamente. Este capítulo complementa aquellos procedimientos con un conjunto de pruebas adicionales que debería llevar a cabo antes de implementar la solución en producción.

Capítulo 8: Mantenimiento de soluciones de seguridad en LAN inalámbricas

Este capítulo se centra en mantener el funcionamiento adecuado de la infraestructura de seguridad en la WLAN. La primera parte del capítulo incluye las tareas operativas clave que necesita para mantener el sistema. Se dividen en diferentes categorías que abarcan lo siguiente: tareas de mantenimiento diario, supervisión y alertas; introducción de modificaciones en el entorno, optimización del rendimiento y solución de problemas. La sección final sobre solución de problemas contiene una serie de diagramas de flujo, tablas y procedimientos, descripciones detalladas de herramientas y técnicas para la solución de problemas que puede utilizar en el diagnóstico y resolución de éstos.

Apéndices

Apéndice A: Uso de PEAP en la empresa

Esta solución se diseñó para pequeñas y medianas empresas. Esto contrasta con la solución de WLAN basada en certificados (mencionada anteriormente) que se diseñó para organizaciones de nivel empresarial. No obstante, una solución de WLAN que utilice PEAP y contraseñas también se puede utilizar en organizaciones de gran tamaño.

Este apéndice muestra cómo puede adaptar la información sobre la solución de WLAN basada en certificados y orientada a la empresa, con el objetivo de implementar una solución de WLAN basada en PEAP y contraseñas.

Apéndice B: Uso de WPA en la solución

Este apéndice facilita información sobre el estado de compatibilidad con la seguridad en el Acceso protegido WiFi (WPA) y sobre cómo puede utilizar la protección de datos mediante WPA en lugar de WEP (Privacidad equivalente por cable) dinámica. Esta solución se diseñó para admitir WPA, el cual se menciona a lo largo de esta guía. No obstante, cuando la solución se estaba desarrollando, la compatibilidad con WPA no era aún universal y, por tanto, no se utilizó como opción predeterminada.

Apéndice C: Versiones de sistemas operativos compatibles

Este apéndice consta de una tabla en la que se muestran las versiones de sistemas operativos en esta solución compatibles con clientes inalámbricos y con varias funciones de servidor. Su finalidad es responder a las dudas sobre la posibilidad de utilizar versiones alternativas de Windows y de otras plataformas en las diversas funciones de esta solución.

Apéndice D: Secuencias de comandos y archivos auxiliares

Los procedimientos descritos en los capítulos dedicados a la implementación y funcionamiento utilizan una serie de secuencias de comandos y otros archivos auxiliares. Este apéndice describe las secuencias de comandos y su funcionamiento. Esta información también aparece en el archivo SecuringWirelessLANs.rtf incluido con las secuencias de comandos.

Principio de la página

Convenciones de estilo

La siguiente tabla describe las convenciones de estilo utilizadas en la guía.

Tabla 1.1. Convenciones de estilo

Elemento	Significado
Negrita	Caracteres que se escriben exactamente tal y como se muestran, incluidos comandos y modificadores. Los elementos de la interfaz de usuario (UI) que aparecen en el texto con carácter normativo también se muestran en negrita.

Cursiva	La cursiva se utiliza en dos contextos especiales: —Si la cursiva aparece en el cuerpo principal del texto, indica que se trata del título de otro documento. —Si la cursiva aparece en comandos o códigos (o en texto que haga referencia a un comando o código), indica que se trata de marcadores de posición para variables donde se han de insertar valores específicos. Por ejemplo, *nombreDeArchivo.ext* indica que debe sustituir el texto en cursiva *nombreDeArchivo.ext* con el nombre de archivo de su elección. La cursiva también se utiliza en ocasiones para enfatizar texto normal.
Texto en pantalla	Para el texto visualizado en pantalla (por ejemplo, los resultados de una herramienta de línea de comandos) y para comandos que hay que escribir en la línea de comandos. Algunos comandos no se ajustan a los márgenes de la página. Cuando sucede esto, el texto del comando se divide en varias líneas con las líneas posteriores con sangría (indicado en una nota a continuación del comando).
Fuente monoespaciada	Ejemplos de código y contenidos de archivos de configuración.
%SystemRoot%	Carpeta en la que se instala el sistema operativo Windows Server 2003.
Nota	Avisa al lector de la existencia de información adicional.
Importante	Avisa al lector de la existencia de información adicional esencial para finalizar la tarea.
Precaución	Avisa al lector de que el incumplimiento u omisión de una acción concreta puede producir pérdida de datos.
Advertencia	Avisa al lector de la situación en la que el incumplimiento u omisión de una acción concreta puede producir lesiones físicas al usuario o daños al hardware.

Principio de la página

Soporte técnico y comentarios

Soporte técnico

Para obtener más ayuda sobre la implementación de las tecnologías tratadas en esta solución, póngase en contacto con la oficina de Microsoft de su zona o con una empresa asociada a los servicios de Microsoft.

- Para encontrar la oficina de Microsoft de su zona, visite la siguiente dirección URL y seleccione el país y región pertinente

  http://www.microsoft.com/worldwide/.

- Para buscar una empresa asociada a Microsoft en su región, consulte la sección de servicios del Directorio de recursos de Microsoft, en la siguiente dirección URL:

  http://directory.microsoft.com/ResourceDirectory/Solutions.aspx.

- Para obtener más información sobre el soporte técnico de los componentes de Windows Server 2003 utilizados en esta solución, que incluye niveles superiores de notificación, ofertas de soporte técnico, recursos y niveles de soporte técnico, consulte la siguiente dirección URL:

http://support.microsoft.com.

Envíenos sus comentarios

Microsoft está interesado en sus comentarios sobre este material. Sobre todo, no dude en enviarnos su opinión sobre los siguientes temas:

- Utilidad de la información proporcionada
- Precisión de los procedimientos descritos paso a paso
- Facilidad de lectura y grado de interés de los capítulos
- Valoración general de la solución

Envíe sus comentarios a la siguiente dirección de correo electrónico: SecWish@Microsoft.com.

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

Principio de la página

Administre su perfil