Latinoamérica

Microsoft TechNet

Seguridad en LAN inalámbricas con PEAP y contraseñas

Apéndice A: Uso de PEAP en la empresa

Actualizado: abril 2, aaaa

Ver todos los temas de la guía de seguridad

Microsoft® ha producido dos soluciones para la seguridad en redes de área local inalámbrica (WLAN). La primera solución *Solución de Seguridad de LAN inalámbricas — Servicios de Certificate Server de Microsoft Windows Server 2003* utiliza certificados de cliente para autenticar clientes inalámbricos y está pensada principalmente para organizaciones empresariales grandes. La segunda, *Seguridad en LAN inalámbricas con PEAP y contraseñas* (el tema de esta guía), utiliza contraseñas y el protocolo de autenticación extensible protegido (PEAP) para autenticar clientes inalámbricos. Esta última se ha escrito fundamentalmente para organizaciones pequeñas y medianas. No obstante, no hay nada sobre PEAP que restrinja su uso a organizaciones más pequeñas. Las organizaciones empresariales grandes también pueden recurrir a PEAP y a la autenticación por contraseña para asegurar sus WLAN.

Si forma parte de una organización grande que está planeando implementar PEAP con contraseñas, este apéndice le mostrará cómo utilizar las secciones de ambas soluciones para poder implementarlo. Ambas soluciones cuentan con la misma arquitectura técnica y componentes idénticos, así que es relativamente sencillo tomar el contenido centrado en la empresa de la primera solución y reemplazar los protocolos de autenticación de certificados por los protocolos de PEAP y contraseñas. El objetivo es facilitar una guía combinada que incluya detalles relevantes para una solución WLAN para empresas, como una delegación administrativa avanzada, registro de RADIUS y la separación de funciones del servidor, pero con contraseñas para autenticar clientes inalámbricos.

A lo largo de este apéndice, por razones de brevedad, el término "solución EAP-TLS" se utilizará para hacer alusión a la primera solución (*Solución de Seguridad de LAN inalámbricas — Servicios de Certificate Server de Microsoft Windows Server 2003*), mientras que el término "solución PEAP" hará referencia a la segunda (*Seguridad en LAN inalámbricas con PEAP y contraseñas*). Protocolo de autenticación extensible-Seguridad de la capa de transporte es el nombre de certificado de cliente basado en el protocolo de autenticación utilizado en la primera solución.

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

Aspectos necesarios de la solución EAP-TLS

Desde que se confeccionara la guía de la solución EAP-TLS para organizaciones grandes, ésta se ha convertido en la referencia principal. Incluye el planeamiento, la implementación y los detalles operativos (como la delegación de la administración) que probablemente sean de mayor interés para organizaciones grandes. Después de la tabla, encontrará una lista de los capítulos de la solución EAP-TLS. Para cada capítulo se proporciona una descripción que detalla si el contenido de esta solución es relevante o no para la guía "combinada". Asimismo, se destacan aquellos casos en los que el contenido de la solución PEAP se debe utilizar en lugar de las instrucciones de la solución EAP-TLS.

A modo de referencia, la siguiente tabla contempla la asignación entre los capítulos de ambas soluciones.

Debido a diferencias de alcance y utilización de la tecnología, la asignación entre los capítulos no es uno a uno.

Tabla A.1. Asignación de los capítulos entre las soluciones EAP-TLS y PEAP

Solución EAP-TLS	Solución PEAP
Capítulo 1: Información general	Capítulo 1: Seguridad en LAN inalámbricas con PEAP y contraseñas
Capítulo 2: Determinación de una estrategia para redes inalámbricas seguras	Introducción: Elección de una estrategia para la seguridad en LAN inalámbricas
Capítulo 3: Arquitectura de la solución para una LAN inalámbrica segura	Capítulo 2: Planeamiento de la implementación de seguridad en LAN inalámbricas
Capítulo 4: Designing the Public Key Infrastructure	Capítulo 2: Planeamiento de la implementación de seguridad en LAN inalámbricas
Capítulo 5: Diseño de una infraestructura de RADIUS para la seguridad de LAN inalámbricas	Capítulo 2: Planeamiento de la implementación de seguridad en LAN inalámbricas
Capítulo 6: Diseño de la seguridad para LAN inalámbrica mediante 802.1X	Capítulo 2: Planeamiento de la implementación de seguridad en LAN inalámbricas
	Capítulo 3: Preparación del entorno
Capítulo 7: Implementing the Public Key Infrastructure	Capítulo 4: Creación de la entidad emisora de certificados de red
Capítulo 8: Implementación de la infraestructura de RADIUS para la seguridad de LAN inalámbricas	Capítulo 5: Creación de la infraestructura de seguridad de LAN inalámbricas
Capítulo 9: Implementing Wireless Security Using 802.1X	Capítulo 6: Configuración de clientes de LAN inalámbricas
Capítulo 10: Introducción a la guía de operaciones	Capítulo 8: Mantenimiento de soluciones de seguridad en LAN inalámbricas
Capítulo 11: Administración de la infraestructura de claves públicas	Capítulo 8: Mantenimiento de soluciones de seguridad en LAN inalámbricas
Capítulo 12: Administración de la infraestructura de seguridad de RADIUS y LAN inalámbrica	Capítulo 8: Mantenimiento de soluciones de seguridad en LAN inalámbricas
Capítulo 13: Guía de prueba	Capítulo 7: Prueba de soluciones de seguridad en LAN inalámbricas

Cabe destacar que la solución EAP-TLS se estructuró intencionadamente para mantener la infraestructura de claves públicas, RADIUS y los componentes WLAN lo más independientes entre sí posible. Con ello se perseguía

permitir volver a utilizar estos componentes en otras aplicaciones. Esto explica que existan algunas repeticiones en la solución EAP-TLS. Por ejemplo, los capítulos sobre la infraestructura de claves públicas y RADIUS incluyen instrucciones sobre la creación de servidores puesto que, en organizaciones grandes, es posible que la instalación de los servidores IAS y de las entidades emisoras de certificados sea responsabilidad de distintos grupos dentro de TI. Además, algunos de los pasos lógicos descritos en los capítulos de diseño e implementación pueden resultar engañosos en el contexto de una solución PEAP. Por tanto, debe leer la solución PEAP para obtener una introducción general sobre el proceso completo y, a continuación, volver a la solución EAP-TLS para conocer detalles específicos sobre el diseño e implementación.

Las siguientes secciones contienen las descripciones sobre cómo utilizar los capítulos de la solución EAP-TLS en relación con los capítulos de la solución PEAP.

Capítulo 1: Información general

El capítulo 1 consiste en una introducción general de la solución y contiene breves resúmenes de cada capítulo y apéndice de la guía. Como trabajará principalmente con la guía de EAP-TLS, debe utilizar el capítulo 1 de esta solución.

Capítulo 2: Determinación de una estrategia para redes inalámbricas seguras

El contenido de este capítulo es muy parecido al contenido de la introducción, "Elección de una estrategia para la seguridad en LAN inalámbricas", de la solución PEAP. La introducción a la solución PEAP hace las veces de un prefacio de ambas soluciones, así que debe utilizar éste en lugar de recurrir al capítulo 2 de la solución EAP-TLS.

Capítulo 3: Arquitectura de la solución para una LAN inalámbrica segura

Este capítulo proporciona una introducción general sobre la arquitectura de la solución WLAN basada en certificados. Es relevante para todos los siguientes elementos, excepto para el primero:

- Descripción del funcionamiento de 802.1X con EAP-TLS (certificados). En su lugar, debe consultar la descripción contemplada en el capítulo 2, "Planeamiento de la implementación de seguridad en LAN inalámbricas" de la solución PEAP.
- Descripción de la organización de destino.
- Lista de los criterios clave de diseño de la solución.
- Ilustración de la utilización de diversos componentes del servidor en distintas ubicaciones de la organización.
- Descripción de cómo se puede escalar la solución.
- Ejemplos de utilización de elementos de la solución para admitir otras aplicaciones de red como la seguridad 802.1X con cable y la red privada virtual (VPN).

Las referencias incluidas a la entidad emisora de certificados también pueden ser útiles en el capítulo siguiente.

Capítulo 4: Designing the Public Key Infrastructure

Este capítulo contiene una descripción detallada del proceso de planeamiento de una infraestructura de claves públicas sencilla. La solución PEAP también contiene instrucciones para una entidad emisora de certificados sencilla con un solo propósito. Aunque no necesite emitir certificados a los clientes WLAN, debe considerar la utilización del siguiente capítulo como ayuda en el diseño de la infraestructura de claves públicas. Cuanto más grande sea la organización, más probable es que necesite certificados en lugar de simples autenticaciones de red. Este capítulo le ayudará a diseñar una infraestructura de claves públicas más flexible y sólida que la que presenta la solución PEAP.

Capítulo 5: Diseño de una infraestructura de RADIUS para la seguridad de LAN inalámbricas

Debe seguir las instrucciones proporcionadas en este capítulo de la solución EAP-TLS.

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

Debe seguir las instrucciones proporcionadas en este capítulo de la solución EAP-TLS.

Capítulo 7: Implementing the Public Key Infrastructure

Este capítulo sólo es relevante si ha decidido implementar una infraestructura de claves públicas completa tal y como se mencionó anteriormente. De lo contrario, siga el capítulo 4 de la solución PEAP, "Creación de la entidad emisora de certificados de red".

Capítulo 8: Implementación de la infraestructura de RADIUS para la seguridad de LAN inalámbricas

Debe seguir las instrucciones proporcionadas en este capítulo. Para obtener información complementaria, lea el capítulo 5 de la solución PEAP, "Creación de la infraestructura de seguridad de LAN inalámbricas".

Capítulo 9: Implementing Wireless Security Using 802.1X

Debe seguir las instrucciones dadas en el capítulo 5, "Creación de la infraestructura de seguridad de LAN inalámbricas" y en el capítulo 6, "Configuración de clientes de LAN inalámbricas", de la solución PEAP sobre cómo configurar la directiva de acceso remoto IAS y la configuración del objeto de directiva de grupo del cliente. El capitulo 5 de la solución PEAP también ofrece útiles detalles que no se tratan en la solución EAP-TLS sobre la configuración de puntos de acceso inalámbrico y secuencias de comandos para automatizar la entrada de clientes RADIUS y la replicación de la configuración de IAS.

Capítulos 10, 11 y 12 sobre el funcionamiento de la solución

Debe seguir las instrucciones proporcionadas en estos capítulos de la solución EAP-TLS. Además, debe leer las instrucciones sobre la solución de problemas con WLAN proporcionadas en el capítulo 8 de la solución PEAP, "Mantenimiento de soluciones de seguridad en LAN inalámbricas". Los procedimientos y técnicas detallados en este capítulo suponen un complemento útil a los procedimientos de los capítulos de la solución EAP-TLS.

Capítulo 13: Guía de prueba

Debe utilizar el contenido de este capítulo. Asimismo, si ha optado por no implementar una infraestructura de claves públicas completa como se describe en el capítulo 4 de la solución EAP-TLS, "Designing Key Infraestructure", haga caso omiso de las pruebas de este capítulo relacionadas con dicha infraestructura.

Secuencias de comandos

Las secuencias de comandos utilizadas en la solución PEAP se desarrollaron a partir de las secuencias de comandos de la solución EAP-TLS. No obstante, aunque las secuencias de comandos de PEAP contienen una mayor funcionalidad que las de EAP-TLS, no constituyen un superconjunto exacto. Por ejemplo, las secuencias de comandos de EAP-TLS contienen funciones de supervisión de la entidad emisora de certificados más sofisticadas. En la mayoría de los casos se deben utilizar las secuencias de comandos facilitadas en la solución PEAP. Sin embargo, es posible que desee instalar las secuencias de comandos de ambas soluciones en carpetas separadas y utilizar cada una de ellas según sea apropiado. Las secuencias de comandos se proporcionan como ejemplos básicos para ilustrar técnicas. Por lo tanto, no dude en modificarlos para adaptarlos mejor a sus necesidades.

Descargue la solución completa en	(Este artículo contiene referencias a guías de otros productos y vínculos a sitios Web que sólo están disponibles en inglés.)
Seguridad en LAN inalámbricas con PEAP y contraseñas	

Principio de la página

Administre su perfil