Manual de configuración SecureW2

Objeto.

Este manual es, básicamente, una simple traducción al castellano de las opciones de configuración del cliente EAP-TTLS SecureW2.

Se ajusta al SecureW2 versión 3.3.3 y al EAP Suite 1.0.x.

Algunas de las opciones si las he probado pero otras no. Por eso, y por muchas cosas mas, la guía de referencia sigue siendo la de SecureW2.

Cualquier aportación, sugerencia o corrección será bienvenida.

nicolas.velazquez@uam.es

Conceptos previos.

En EAP-TTLS hay tres conceptos básicos a tener en cuenta a la hora de usarlo o configurarlo.

Inner Identity.

Usuario REAL *nombre.apellido@dominio* y la contraseña utilizados para realizar la identificación y obtener el acceso a la red.

Suele ser la dirección de E-mail y la contraseña que se ponen en el pop-up de SecureW2.

Se utiliza en la tercera fase del sistema de autenticación.

Outer Identity.

Usuario no significativo SIN contraseña. Debería ser un usuario de la forma *anonymous@dominio*.

Indica a la red inalámbrica que el usuario solicita la clave pública del radius que gestiona el *dominio*.

Se utiliza en la primera fase del proceso de autenticación.

Clave pública del radius.

La clave pública del radius envía con la que el cliente TTLS hará un túnel TLS con el que enviar la inner identity.

El cliente TTLS, SecureW2, debería solicitar siempre que la red le haga llegar la clave pública del radius de su organización.

Pero, para conseguir eso, la outer identity debería ser de su dominio.

Así, el cliente TTLS podría verificar y asegurar SIEMPRE que SOLO ve su contraseña el radius de su organización.

Se utiliza en la segunda fase del proceso de autenticación.

Pestaña *Connection*.

Opción *(Use alternate outer identity)*.

Desmarcado: La outer identity y la inner identity serán iguales.

Marcado: La outer identity será diferente de la inner identity. **Recomendado**.

Requerido por: (Use anonymous outer identity) y (Specify outer identity)

Requiere: -

Opción *(Use anonymous outer identity)*.

Desmarcado: Supone la selección de (Specify outer identity).

Marcado: La outer identity se compondrá, de forma dinámica, con el dominio que el usuario ponga en la inner, y como usuario se añadirá *anonymous*. **Rec omendado**.

Requerido por: (Use empty outer identity (RFC 4822))

Requiere: (Use alternate outer identity)

Notas de uso: En conjunción con la opción de SI verificar certificados, hace que: a) el usuario en itinerancia deba poner obligatoriamente el dominio en el pop up para que la conexión se realice, y b) en su propia organización, el usuario puede poner username sin dominio en el pop up.

Opción *(Specify outer identity)*.

Desmarcado: Supone la selección de (Use anonymous outer identity).

Marcado: La outer identity será SIEMPRE, de forma estática, la que se escriba en el casillero inmediatamente inferior.

Requerido por: -

Requiere: (Use alternate outer identity)

Notas de uso: Al poner la outer de forma fija, tanto si se verifican certificados como si no, el usuario puede poner en el pop up solo *username* o *username @dominio*, en local o en itinerancia, porque le funcionará en todos los casos. Por eso no es recomendado.

Opción *(Enable session resumption (quick connect))*.

Desmarcado: Supone que en proceso de roaming, cada vez que se cambie de antena, se iniciará de nuevo el intercambio de credenciales y las pedirá al usuario.

Marcado: SecureW2 cachea las credenciales de forma que en proceso de roaming, presentara las credenciales sin intevención por parte del usuario. **Rec omendado**.

Requerido por: -

Requiere: -

Notas de uso: Hay dudas en la efectividad de la opción. Sin embargo, no todo es achacable a SecureW2. El proceso de roaming implica a muchos componentes: red, drivers tarjetas, radius, PMK, etc. Ver este posting de los foros de SecureW2

Pestaña *Certificates*.

Opción *(Verify server certificate)*.

Desmarcado: No se comprobará ningún certificado.

Marcado: SecureW2 comprobará que el certificado que llega está firmado por la CA root y/o incluye un common name determinado. **MUY Recomendado**.

Requerido por: (Verify server name) y (Advanced/Server certificate must be installed on local computer)

Requiere: Es aconsejable añadir un certificado usando el botón Add CA. Si no se añade ningún certificado, el SecureW2 pedirá al usuario, mas adelante, confirmación para utilizar todo el almacen de certificados de CA raiz de confianza.

Notas de uso: Desde la versión 3.3.0, SecureW2 comprueba la cadena de certificación dando sólo la CA root. Ya no es necesario instalar todas las sub CAs. En el caso de usar el servicio SCS, solo hay que dar al botón Add CA para incorporar GTE Cybertrust Global Root, una de las CAs que incorpora Microsoft en sus SOs.

Opción *(Verify server name)*.

Desmarcado: Supone que no se comprobará el nombre completo (CN) o el dominio que aparece en la clave pública del radius.

Marcado: Se comprobará que el nombre completo o el dominio que aparece en la clave pública del radius es lo que se escribe el casillero de al lado. **Reco mendado**.

Nota de la US.ES: SecureW2 hace distinción entre mayúsculas y minúsculas en el nombre del servidor del certificado, por lo que si el nombre del servidor en el certificado está en mayúsculas, se debe poner también en mayúsculas en la parte "*Verify server name*".

Requerido por: -

Requiere: (Verify server certificate)

Pestaña *Authentication*.

Opción *(Select Authentication Method)*.

Selecciones posibles: PAP / EAP

PAP: Dentro del túnel TLS con el que se encripta la inner identity, cuando el radius desencripte, la password se verá en claro porque no se ha hecho hash.

EAP: Dentro del túnel TLS con el que se encripta la inner identity, se negocia OTRO proceso EAP adicional anidado.

Requerido por: (EAP Type)

Requiere: -

Notas de uso: El uso de PAP está sujeto siempre a discusión ya que no suele gustar a los administradores que las contraseñas se vean en claro en los radius. Pero si el radius va a escalar la autenticación a un ldap, PAP es la mejor opción. Sobre las consideraciones de seguridad y si MS-CHAPv2 es solución o no, véase este enlace de la documentación de Freeradius. En este otro enlace se hace referencia dos tablas de compatibilidad entre protocolos y compatibilidad entre protocolos y servidores de autenticación.

Opción *(EAP Type)*.

Selecciones posibles: MS-CHAPv2 / MD5 / PEAP / TLS

Requerido por: -

Requiere: Seleccionar EAP en (Select Authentication Method).

Notas de uso: Hay que configurar el radius para que "entienda" ese EAP. Atención: no es que SecureW2 se pueda utilizar para hacer PEAP como el cliente de Windows, sino que, dentro del túnel TLS en el que va encriptada la inner y la password, se realiza OTRO proceso de EAP anidado adicional que podría llegar a ser hasta otro EAP-TTLS !!!!.

Pestaña *User account*.

Opción *(Prompt for user credentials)*.

Desmarcado: No aparecerá pop-up para solicitar del usuario la inner identity. Se activan los casilleros inferiores para rellenar Username, Password y Domain de forma estática y permanente.

Marcado: Aparecerá pop-up para solicitar del usuario la inner identity. Se desactivan los casilleros inferiores para rellenar Username, Password y Domain. **Recomendado**.

Requerido por: Debe estar desmarcado para que funcione la opción (Use this account to logon computer).

Requiere: -

Notas de uso: Si se marca la opción (Save user credentials) en el pop up para introducir la inner identity, entonces, (Prompt for user credentials) se desmarca.

Opción *(Use this account to logon computer)*.

Desmarcado: Las credenciales de los casilleros superiores NO se utilizarán como credenciales de Windows en el arranque del sistema.

Marcado: Las credenciales de los casilleros superiores SI se utilizarán como credenciales de Windows en el arranque del sistema.

Requerido por: -

Requiere: Que está desmarcada la opción (Prompt for user credentials) y rellenos los casilleros.

Botón *Advanced*.

Opción *(Use alternate account to logon computer)*.

Desmarcado: Aparecerá un pop-up para solicitar a cada usuario del pc la inner identity. Se desactivan los casilleros inferiores para rellenar Username, Password y Domain.

Marcado: No aparecerá pop-up para solicitar del usuario la inner identity a ninguno de los usuarios del pc. Se activan los casilleros inferiores para rellenar Username, Password y Domain. Todos los usuarios del pc se validarán con el usuario escrito en los casilleros.

Requerido por: -

Requiere: -

Opción *(Server certificate must be installed on local computer)*.

Desmarcado: El certificado o clave pública del radius no está instalado en el ordenador personal.

Marcado: El certificado o clave pública del radius tiene que estar instalado en el ordenador personal. Se va comprobar que coinciden completamente el que tiene el ordenador y el que llega por la red.

Requerido por: -

Requiere: Que está activado (Verify server certificate) para que la opción marcada funcione.

Notas de uso: Existe otra forma de conseguir esto. Una vez instalado el certificado del radius en el ordenador personal, al pulsar el botón Add CA de la pestaña Certificates, ponemos el certificado del radius.

Opción *(Check for Microsoft Key extension)*.

Opción *(Allow users to setup new connections)*.

Desmarcado: Si el certificado que llega por la red no coincide con el que se verifica en la pestaña Certificates, se interrumpirá la conexión. No se propondrá al usuario final la aceptación o no de los nuevos certificados que le puedan llegar por la red. **Recomendado**.

Marcado: Si el certificado que llega por la red no coincide con el que se verifica en la pestaña Certificates, se propondrá al usuario final la aceptación o no de los nuevos certificados que le han llegado por la red.

Requerido por: -

Requiere: Que está activado (Verify server certificate) para que la opción marcada funcione.

Opción *(Use empty outer identity (RFC 4822))*.

Desmarcado: La outer identity que se compone en la forma automática, (Use alternate outer identity) + (Use anonymous outer identity), se compondrá de la forma *anonymous@dominio*. **Recomendado**.

Marcado: La outer identity que se compone en la forma automática, (Use alternate outer identity) + (Use anonymous outer identity), se compondrá de la forma *@dominio*.

Requerido por: -

Requiere: (Use alternate outer identity) + (Use anonymous outer identity)

Notas de uso: Según el rfc, la outer ni siquiera debería llevar la palabra anonymous. Pero un username vacío hace que Freeradius o Windows Mobile no funcionen. Si la inner no incluye dominio, entonces la outer se compondría completamente vacía.

Opción *(Renew IP address after authentication)*.

Desmarcado: SecureW2 no intervendrá en el proceso de dhcp. **Recomendado**.

Marcado: SecureW2 intentará pedir una nueva dirección ip después de cada conexión con éxito.

Requerido por: -

Requiere: -

Notas de uso: SecureW2 aconseja dejar esta opción desmarcada y marcarla sólo cuando el proceso dhcp no funcione correctamente en el ordenador.

Configuración recomendada. Pantallazos.

Las opciones con redondel rojo deberían ponerse para obtener una configuración segura. En mi opinión deberían ser obligatorias.

Las opciones con redondel verde deberían ponerse por rendimiento, compatibilidad, etc., pero cambiarlas no supone una merma en la seguridad de la autenticación.

El resto de las opciones que no están redondeadas quedan a la elección del administrador.


SecureW2 Profile: uam02
SecureW2
Connection
Certificates
Authentication
User account
Verify server certificate
Trusted Root CA:
GTE CyberTrust Global Root
Add CA
Remove CA
Verify server name:
uam.es
Advanced
OK
Cancel


SecureW2 Profile: uam02
SecureW2
Connection
Certificates
Authentication
User account
Select Authentication Method:
PAP
EAP Type:
Configure
Advanced
OK
Cancel

Referencias.

La verdadera guía: User Guide SecureW2.