CONVOCATORIA DE PREMIOS @asLAN A PROYECTOS EN LA ADMINISTRACIÓN PÚBLICA

ENTORNO SEGURO DE ACCESO REMOTO A LA FUNCIONALIDAD DE MOVILIDAD Y TELETRABAJO EN MINETAD.

Implantado en:

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

paloalto networks
Microsoft
ALTEN ESPAÑA
Deloitte.

ANTECEDENTES/PROBLEMÁTICA

El Ministerio de Energía, Turismo y Agenda Digital (MINETAD) es pionero en la adopción de las medidas de seguridad requeridas por el **Esquema Nacional de Seguridad** (Real Decreto 3/2010, de 8 de enero), tendente a establecer unas condiciones de confianza en las relaciones por medios electrónicos entre los ciudadanos y las Administraciones Públicas, y entre estas entre sí, y se haya plenamente alineado con uno de los principales objetivos de la **Agenda Digital para España** centrado en **"Reforzar la confianza en el ámbito digital"** y desarrollado a través del **Plan de Confianza Digital**.

Además, uno de los pilares fundamentales del plan estratégico para la **"Transformación Digital"** a nivel interno llevado a cabo por el Ministerio es la adopción de un **programa de teletrabajo** que permita a sus empleados el acceso remoto a los sistemas de información del Ministerio de forma que les permita trabajar en todo momento y lugar en aquellos asuntos que estén tramitando, sin depender de otro tipo de restricciones, favoreciendo así su **movilidad** y contribuyendo a incrementar su **productividad**, a la vez que, de forma subsidiaria, se mejora la conciliación de la vida familiar.

Sin embargo, dichas medidas suponen un riesgo para los activos de la organización y se han debido de implantar unos mecanismos de protección adicionales en los accesos remotos a la red corporativa.

La **Subdirección General de Tecnologías de la Información y de las Comunicaciones** (SGTIC) del Ministerio, que es la encargada de desarrollar, operar y mantener la red informática corporativa y sus servicios asociados, es consciente de la importancia de llevar a cabo una securización de los elementos que componen el entorno de

teletrabajo en base al nivel de seguridad que le es legalmente exigible y, en particular, en lo referido a la medida **op.acc.7** del Esquema Nacional de Seguridad sobre acceso remoto.

Actualmente, la SGTIC proporciona a sus empleados un servicio de **Oficina Móvil** que ofrece la posibilidad de acceder, a través de VPN, a aquellas aplicaciones internas y repositorios de información de interés del empleado para favorecer la movilidad. Además, la Oficina Móvil puede proporcionar un acceso remoto al equipo de escritorio corporativo, siendo esta funcionalidad la más demandada entre los empleados adscritos al programa de teletrabajo que, en la actualidad, suponen un 10% de la plantilla.

El principal problema que entraña este modelo es que no hay control sobre el equipo externo desde el que los empleados acceden y, por ello, el acceso remoto es fuente de numerosos problemas de seguridad ya que no permite implantar el mismo nivel de controles de seguridad que en las instalaciones corporativas.

OBJETIVOS PERSEGUIDOS

El principal objetivo perseguido es **conseguir que la seguridad de los equipos gestionados por la SGTIC y que se proveen a usuarios deslocalizados**, principalmente por motivos de movilidad, aunque también puede darse en un entorno de teletrabajo, **sea equivalente al que tiene un equipo de sobremesa ubicado en el entorno físico corporativo**.

Dado que la SGTIC cuenta con un cortafuego Palo Alto, se ha optado por hacer uso del módulo de **GlobalProtect** que consiste en establecer un túnel SSL entre el dispositivo, al que previamente se habrá instalado un cliente de GlobalProtect, y el propio cortafuegos Palo Alto.

Fig.1 – concepto de GlobalProtect

El utilizado por la VPN de GlobalProtect difiere del túnel utilizado en la VPN de la Oficina Móvil en que en el primer caso el dispositivo adquiere un direccionamiento interno, es decir el equipo pasa a estar dentro del dominio corporativo, mientras que en el segundo caso solo se proveen funcionalidades corporativas a un equipo privado ajeno al dominio y lo que recibe realmente el dispositivo son snapshots de éstas, no existiendo una conexión directa con la propia red corporativa. Cabe destacar que ambos mecanismos de VPN no son compatibles entre sí.

El dispositivo móvil necesita contar con un cliente GlobalProtect instalado y configurado el cual puede descargarse desde un repositorio accesible desde internet si va a utilizarse en un equipo propiedad del usuario, o bien como es más habitual, puede proveerse directamente con el equipo móvil corporativo asignado. En este segundo caso, el cliente se inicia de manera automática al arrancar el dispositivo y no se permite que el usuario lo deshabilite.

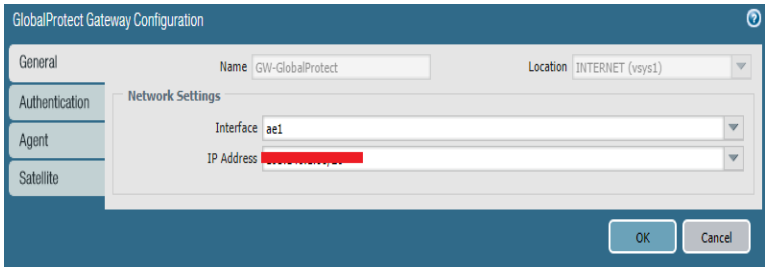

Fig.2 – configuración de la conexión GlobalProtect

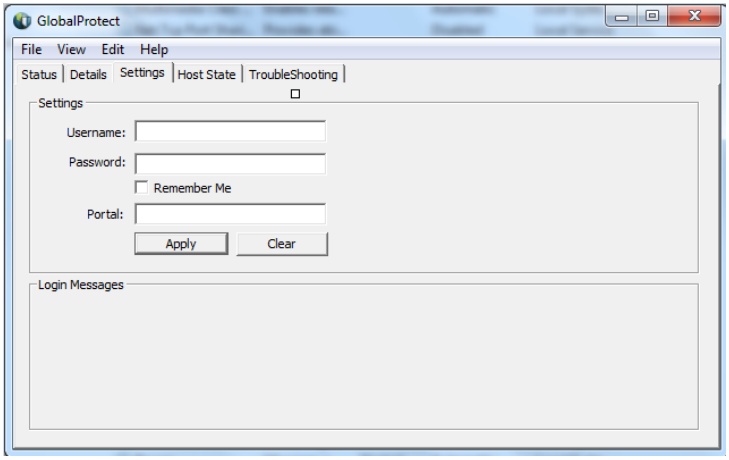

Fig.3 – configuración del agente GlobalProtect

Fig.4 – descarga del agente GlobalProtect

Una vez establecido el túnel mediante credenciales **single sign on**, que se corresponden con las de usuario del dominio y que además ha sido dado de alta en un grupo de seguridad del directorio activo creado adhoc para este fin, el dispositivo móvil recibe una **IP interna corporativa** y se le aplican todas las protecciones definidas en Palo Alto (filtrado de URLs por contenido y por reputación, análisis de descarga de adjuntos mediante Wildfire, detección de malware y análisis de procesos).

Además, se le aplican el resto de medidas de seguridad que tenga instaladas el dispositivo y que sean gestionadas mediante políticas de dominio, entre ellas el antivirus corporativo y, en particular, al estar dicho dispositivo registrado en el dominio, se le aplican también las políticas de despliegue de **parches de actualización y de seguridad** mediante la herramienta **System Center Configuration Manager** (SCCM) de Microsoft. Las políticas establecidas en SCCM por la SGTIC permiten el despliego inmediato, con un mínimo de prueba interna, de cualquier parche crítico en el momento de su publicación en cuanto los equipos inician sesión en el dominio y supone una ventaja competitiva frente a las amenazas avanzadas como, por ejemplo, en el caso **WannaCry** que no tuvo incidencia en el Ministerio.

Con ello se consigue que los dispositivos móviles propiedad del Ministerio que se distribuyan al personal por razones de movilidad o teletrabajo estén **permanentemente actualizados**, sin necesidad de personarse en las dependencias, y que cuenten con todas las protecciones con las que cuentan los puestos de usuario fijos, con independencia de su ubicación o de su método de conexión (Wifi, 3G/4F, red cableada).

Alternativamente, dicha protección podría hacerse extensible a equipos propietarios del usuario, pero habría que tener en cuenta que las restricciones impuestas por la política de seguridad del Ministerio le aplicarían en su propio entorno privado, por lo que este caso de uso no es habitual ni suele ser demandado.

FASES DEL PROYECTO – RECURSOS EMPLEADOS

El proyecto se inició en enero de 2017 y ha tenido una duración de 6 meses. Para su realización fue necesario adquirir el módulo de GlobalProtect.

En ese momento, ya se podía empezar a implementar la medida en los antiguos equipos móviles que habitualmente dotaba el Ministerio (portátiles clásicos) y que solían hacer uso de la funcionalidad de escritorio remoto a través de la Oficina Móvil.

Sin embargo, aprovechando que, por motivos de actualización tecnológica del parque de equipos móviles, durante 2016 y 2017, se han adquirido unos 200 dispositivos Microsoft Surface, se decidió que dichos dispositivos fueran provistos de serie con una maqueta que incluyera el agente de GlobalProtect, en detrimento de la antigua VPN de Oficina Móvil, cuyo uso ha pasado a ser residual y limitado en funcionalidad para aquellos equipos remotos de uso particular, y que se retirasen paulatinamente los antiguos portátiles, muchos de los cuales presentaban graves carencias técnicas, o directamente no estaban actualizados.

Enero	Adquisición Módulo GlobalProtect
Febrero - Marzo	Configuración agentes y pruebas
Abril-Junio	Dotación dispositivos Surface y retirada de equipos obsoletos

Se emplearon los recursos propios de la SGTIC para montar la nueva infraestructura, así como del Centro de Atención a Usuarios del Ministerio para facilitar el cambio de dispositivo.

MEJORAS EN EFICIENCIA Y REDUCCIONES DE COSTE

Con la adopción de la solución GlobalProtect se han logrado varios objetivos:

- Se reduce la fragmentación tecnológica al sustituir un parque disperso de equipos portátiles de distintos fabricantes en un solo tipo de dispositivo y se reducen los costes asociados a mantener distintas maquetas y configuraciones.

- El uso del dispositivo móvil Surface, con su opción de base tipo *dock station*, permite la consolidación de la dualidad presente hasta el momento: ordenador de sobremesa y ordenador portátil, al unificar en un solo dispositivo ambas funcionalidades, con las ventajas que esto supone para el usuario y la eliminación de la duplicidad de costes asociados al licenciamiento y la gestión del soporte para la organización.

- Se incrementa significativamente la seguridad del dispositivo móvil ya que, no solo permite la creación de un canal seguro haciendo uso de medios de conexión inseguros, sino que garantiza que el equipo esté actualizado con los últimos parches configuración y de seguridad en todo momento –a través de la sincronización con SCCM–, además de que todas las protecciones de seguridad corporativas están operativas.

- Se facilita la gestión y mantenimiento de los equipos al no tener que dedicar recursos a mantener numerosas y distintas maquetas ni personal dedicado a su gestión y al poder gestionar la actualización sobre los mismos, de forma centralizada, sin tener que contar con desplazamientos por parte del usuario o del técnico.

- Se incrementa la productividad del empleado al permitirle trabajar con toda seguridad y pleno a acceso a los recursos corporativos en todo momento y lugar.

CONCLUSIONES DE LA ENTIDAD

Dado que el MINETAD es un organismo que siempre se ha caracterizado dentro de la AGE por su carácter puntero en materia de seguridad y que, por otro lado, es un organismo que apuesta decididamente por la transformación digital, la solución adoptada de GlobalProtect le permite aunar ambos intereses y **soslayar la clásica dicotomía de seguridad versus funcionalidad**.

La medida supone un **grado considerable de reducción de coste** al simplificar toda la gestión del equipamiento y al permitir eliminar puestos físicos de sobremesa con el consiguiente ahorro en recursos físicos, energéticos, humanos y de licenciamiento.

Además, los usuarios de la medida se han manifestado de forma muy positiva al respecto, puesto que han **incrementado su productividad** al disponer de un entorno seguro y con acceso equivalente al que tendrían en las instalaciones del Ministerio, en todo momento y lugar.

El Ministerio tiene previsto incrementar el alcance de este proyecto para, de forma paulatina ir expandiendo la medida a todos los usuarios que requieran de necesidades de movilidad o hagan uso del programa de teletrabajo.