UNIVERSITAT POLITÈCNICA DE VALÈNCIA

_ TELECOM ESCUELA TÉCNICA VLC SUPERIOR DE INGENIERÍA DE TELECOMUNICACIÓN

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería de Telecomunicación

Implantación de Sistemas de Monitorización y Seguridad en una red corporativa.

Trabajo Fin de Grado

Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación

AUTOR/A: Moreno Iniesta, Pedro

Tutor/a: León Fernández, Antonio

CURSO ACADÉMICO: 2021/2022

Resumen

En este trabajo de fin de grado se describe la implantación y mejora de seguridad en sistemas de redes corporativas mediante el uso de las aplicaciones de Software comercial:

- **inWebo**: herramienta que nos permite establecer una seguridad de doble autenticación en diversos entornos como por ejemplo Office 365, el inicio de sesión de Windows o las conexiones VPN.
- **WhatsUp Gold**: herramienta que nos proporciona una monitorización muy visual y completa de sistemas ya sean servidores, switches, AP's.
- **KeePass**: herramienta que nos permite almacenar y generar credenciales de sitios web, aplicaciones… de forma segura y protegida mediante una Master Key.

Summary

This final degree project describes the implementation and improvement of security in client systems through the use of commercial software applications:

• **inWebo**: a tool that allows us to establish double authentication security in various environments such as Office 365, Windows login or VPN connections.

• **WhatsUp Gold**: a tool that provides us with a very visual and complete monitoring of systems, whether they are servers, switches, AP's.

• **KeePass**: tool that allows us to store and generate credentials for websites, applications... in a safe and protected way by means of a Master Key.

Resum

En aquest treball de fi de grau es descriu la implantació i millora de seguretat en sistemes de clients mitjançant l'ús de les aplicacions de programari comercial:

• inWebo: eina que ens permet establir una seguretat de doble autenticació a diversos entorns com ara Office 365, l'inici de sessió de Windows o les connexions VPN.

• WhatsUp Gold: eina que ens proporciona un monitoratge molt visual i complet de sistemes ja siguin servidors, switches, AP's.

• KeePass: eina que ens permet emmagatzemar i generar credencials de llocs web, aplicacions,… de manera segura i protegida mitjançant una Master Key.

Contenido

Ilustraciones

1. Introducción

1.1 Justificación y contexto

Hoy en día la seguridad existe una gran necesidad a la garantizar la seguridad en equipos tanto de entorno personal como los pertenecientes a redes corporativas. Esto es debido la gran cantidad de amenazas, ataques informáticos, sabotajes y malware que tienen como principal objetivo el robo de información, inutilizar y comprometer los mismos. Por esta razón existen una serie de aplicaciones que ayudan a facilitar la creación de entornos seguros que ayudan a elevar en nivel de seguridad.

Las **herramientas de doble autenticación** son esenciales a día de hoy ya que constituyen una de protección sobre la contraseña empleada ya sea para iniciar sesión en un dispositivo, una cuenta de correo, un servicio web, etc.

Esta tecnología se puede configurar de varias formas como por ejemplo mediante el envío de un código vía mensaje a un dispositivo que normalmente suele ser un teléfono o mediante la verificación en una aplicación móvil.

A día de hoy, para darnos cuenta de la importancia de la doble autenticación esta ya se utiliza en universidades como la Universidad Politécnica de Valencia a la hora de realizar las conexiones VPN por lo que, cuando hemos iniciado sesión con nuestras credenciales mediante la aplicación de Microsoft Authenticator podremos proceder a la segunda validación necesaria para poder establecer la conexión VPN correctamente.

Mediante gran cantidad de métodos se puede llegar a obtener la clave de inicio de sesión que dar acceso al servicio web, portal o equipo personal donde, sin la doble autenticación configurada se puede producir una gran cantidad de pérdida de información que varía dependiendo del equipo, persona o entidad que sufra dicho ataque. Algunos de los métodos por los cuales se pueden obtener contraseñas brevemente explicados son:

- Filtraciones de datos: si nuestras credenciales quedan expuestas en la web ya sea mediante fallo nuestro o mediante la adquisición por ejemplo de listas de nombres de usuarios y contraseñas por parte de “hackers” la seguridad de nuestras cuentas y equipos quedarán gravemente comprometidas.
- Spyware: tipo de software malicioso que por ejemplo puede, mediante un keyloger, almacenar las pulsaciones de teclado para obtener credenciales de acceso a servicios web, aplicaciones o equipos.
- Phishing: método de ingeniería social por el cual los estafadores o hackers se hacen pasar por una empresa o servicio web aparentemente fidedigno mediante herramientas como el correo electrónico para la obtención de datos.

Estos y muchos más métodos pueden resultar dañinos para empresas o particulares por lo que si se configura debidamente un factor de doble autenticación aunque tengan nuestras credenciales de acceso los hackers no podrán acceder a los servicios, aplicaciones o equipos deseados.

La doble autenticación fue implantada con carácter obligatorio para transacciones bancarias en España desde 2018 mediante el real Decreto Ley 19/2018.

Debido a este decreto se procedió a utilizar la normativa PSD2 (Payment Services Directive 2) que es la directiva Europea que se encarga de regular los servicios de pago ya sean transferencias, domiciliaciones, pagos por tarjeta de crédito/débito, etc.

También permite que terceras empresas puedan participar en estos pagos que es lo que se conoce como “open banking”.

Lo que se pretende conseguir mediante la implantación de la doble autenticación en este ámbito es una mayor transparencia, innovación y competencia en los servicios de pago.

De acuerdo con dicha normativa identificación a la hora de la doble autenticación deberá incluir 2 o más factores de autenticación que se encuentren en las siguientes categorías:

1. Inherencia: algo que el propio usuario es.
2. Posesión: algo que posee solo el usuario.
3. Conocimiento: algo que solo conoce el usuario.

Esto lo podemos ver en bancas españolas como por ejemplo BBVA, Banco Santander o las cajas rurales que utilizan desde 2018 la doble autenticación mediante el envío de un código por mensaje SMS al número de teléfono enlazado a la cuenta bancaria para el inicio de sesión lo que significa que los dispositivos móviles se vuelven de capital importancia en este ámbito.

Para elevar el nivel de seguridad tanto en entornos personales como corporativos de clientes reales gracias a las prácticas realizadas en la empresa Consultoría tecnológica Abenet Soluciones S.L. he dispuesto del software de inWebo como herramienta de doble autenticación:

- **inWebo:** herramienta software utilizada para establecer una doble autenticación en entornos de aplicaciones como Office 365 o en el inicio de sesión de Windows por ejemplo.

Mediante **inWebo** se puede elevar un nivel más la seguridad ya que es una herramienta de doble autenticación que permite proteger determinados entornos de forma que, aunque accedan a cualquier servicio gestionado por esta aplicación necesiten otra autenticación mediante PIN para poder iniciar sesión en cualquiera de los servicios en los que esta herramienta esté implementado. Esta basada en la generación de códigos OTP para el inicio de sesión y gestión de la herramienta.

La necesidad de herramientas para incrementar el nivel de seguridad en redes corporativas es capital ya que mediante el software de **KeePass** podemos establecer mediante un **generador automático de contraseñas** parametrizable gran cantidad de credenciales de alta seguridad, robustez y variedad. Estas quedarán protegidas por una contraseña maestra por lo que únicamente tendremos que memorizar la contraseña que nos da acceso a la base de datos en la que alojamos las credenciales.

Para crear entornos de contraseñas más seguros en empresas he utilizado el software de Keepass.

- **KeePass:** herramienta software que sirve para almacenar contraseñas de diversos sitios web, aplicaciones, cuentas bancarias etc. Es una forma segura de almacenar contraseñas de forma que estas no sean interceptadas mediante malware como phishing o keylogers.

La necesidad de una **herramienta de monitorización** exhaustiva en redes corporativas debido a que, por ejemplo si una empresa de TI da un servicio de mantenimiento a clientes, esa empresa tiene que asegurarse mediante la monitorización de que la red corporativa de cada cliente está en correcto estado, además de poder analizar todo tipo de prestaciones como el consumo de CPU, de memoria RAM, si responde la máquina mediante ping… de forma que si existe alguna carencia, problema o ataque en la red corporativa del cliente la detectemos de una forma rápida y anticipada.

Esto también permite elevar en gran medida la seguridad en redes corporativas reales ya que se puede detectar el punto en el que está siendo vulnerable atacada o deteriorada la infraestructura de la red corporativa mediante alertas de correo en tiempo real para poder acometer e intentar solucionar dicho problema.

Para la monitorización de equipos en redes corporativas la empresa Progress Softwre Corporation ha desarrollado el software de **WhatsUp Gold** que permite monitorizar diferentes recursos de una red corporativa como por ejemplo servidores, switches, firewalls, AP’s (Access Points) o servidores.

1.2 Objetivos

El principal objetivo de este trabajo de fin de grado es implementar una serie de herramientas que nos permitan asegurar y monitorizar el estado de una red corporativa.

Con ello se pretende dar una visión de cómo, gracias a las prácticas realizadas en la empresa Consultoria tecnológica Abenet Soluciones S.L. he dispuesto de las herramientas de inWebo, WhatsUp Gold y KeePass con las que se ha podido elevar en gran medida la seguridad en los distintos equipos en las redes corporativas de clientes reales en las que se implementen estas aplicaciones software.

Para ello la cronología que seguirá este trabajo como objetivo es la siguiente:

1. Desarrollo de un entorno seguro en inicio de sesión de Windows, Office 365 y VPN's.
2. Puesta en marcha del contenedor de contraseñas KeePass para la protección de credenciales.
3. Creación de entornos de monitorización en WhatsUp Gold de redes corporativas:

    3.1 Mediante túneles Ipsec entre la red que da servicio y la que se ha de proteger

    3.2 Mediante montaje de máquina virtual en una red corporativa

1.3 Memoria

La memoria se estructura en 6 capítulos.

En el primer capítulo se especifican los objetivos principales del trabajo de fin de grado.

En el segundo punto se exponen las motivaciones y distribuciones de tareas junto con un diagrama temporal que refleja la progresión de las mismas.

En el tercer lugar se pone nombre, mediante una introducción, a cada una de las herramientas utilizadas para la implementación de mejoras de seguridad en redes corporativas reales.

El cuarto capítulo es el más extenso del trabajo ya que se trata del desarrollo de cada uno de los softwares en redes corporativas reales en cada uno de los escenarios implementados para dichas herramientas.

El quinto punto trata sobre las conclusiones obtenidas a lo largo del trabajo y del trabajo futuro y labor de mantenimiento que habrá que hacer para los distintos softwares en cada red corporativa.

El sexto y último epígrafe es la bibliografía/webgrafía donde se da visión a las distintas webs e informaciones en las que me he apoyado para realizar mi trabajo de fin de grado.

2. Estructuración de la Metodología

2.1Realización del trabajo

Incentivado por la necesidad de un aumento de seguridad en las redes corporativas para proteger la integridad de las corporaciones se decidió implantar nuevas herramientas que ofrezcan y garanticen el aumento en cuanto al nivel de seguridad mediante el software de WhatsUp Gold, KeePass e inWebo.

En añadido, pero no menos importante se ha pensado también realizar un análisis de las distintas VLAN's existentes en algunas redes corporativas de algunos clientes para establecer a cuales VLAN's pueden acceder sus diferentes equipos y a cuales no regulando así el tráfico de red y el acceso a las mismas de equipos o direcciones no permitidas o no deseadas.

Finalmente se ha puesto lo mencionado en marcha aplicándolo a algunas redes corporativas comprobando así que su nivel de seguridad se elevaba exponencialmente.

2.2División de tareas

La división de tareas se ha efectuado de la siguiente manera:

a. Fase de identificación de problemas de seguridad en redes corporativas. En esta primera etapa se analizaron las fugas de seguridad de algunas redes corporativas.

b. Análisis de redes corporativas. En esta fase se decidió a que redes corporativas era factible aplicar las mejoras de seguridad en base a la forma de trabajar y a la distribución que estas tienen.

c. Personalización de la herramienta. Una vez analizadas las redes corporativas deseadas se decidió la forma de implementar las herramientas para cada red corporativa ya que no todas funcionan de la misma manera.

d. Desarrollo y puesta en marcha de las herramientas de seguridad. Se fue implementando cada herramienta en las redes corporativas analizadas previamente. Es la fase más extensa.

e. Depuración del software de seguridad implantado. En esta fase se identificaron posibles errores y mejoras de las herramientas desarrolladas en las distintas redes corporativas.

f. Desarrollo y de la memoria

g. Desarrollo de la presentación.

2.3Planificación temporal

En el diagrama que aparece a continuación se muestra la evolución de las tareas a lo largo del espacio temporal de Abril de 2022 a Septiembre de 2022.

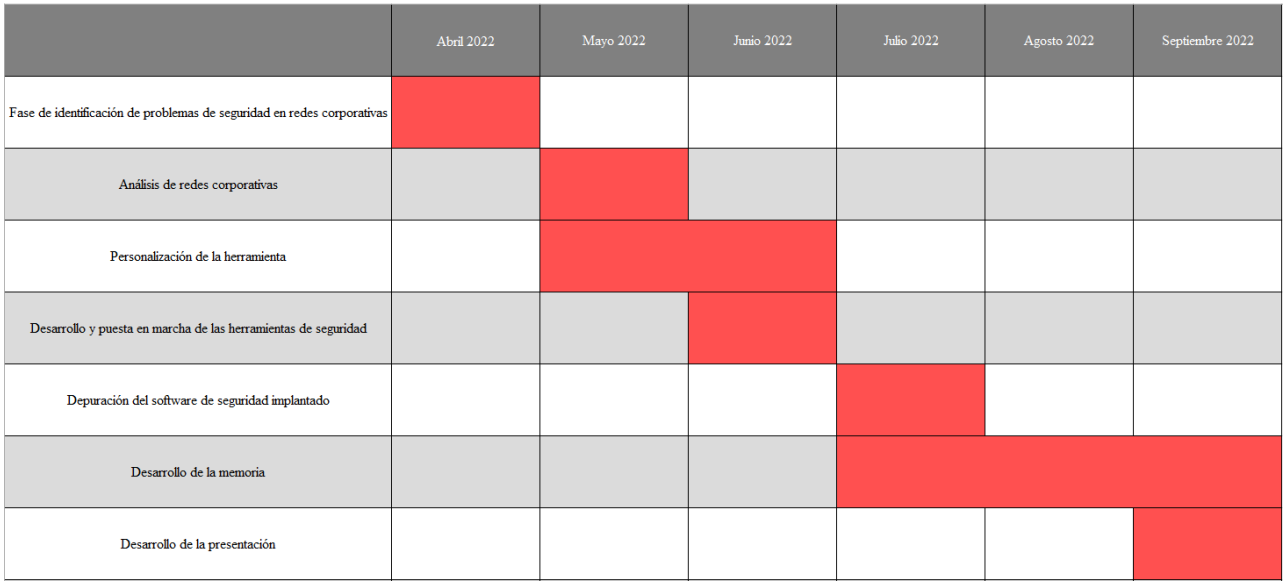

Ilustración 1. Diagrama de planificación temporal

3. Herramientas software utilizadas

3.1Funcionamiento y descripción del software utilizado

3.1.1 Introducción a inWebo

inWebo es un software que permite desarrollar distintos entornos de doble autenticación (fundamentalmente a través de una notificación push) mediante el uso de contraseñas de un solo uso. Este tipo de cifrado se denomina One Time Password (OTP).

Fue creado en 2008 por la empresa Progress y actualmente es utilizado en más de 5.000.000 de usuarios convirtiéndose así en la aplicación puntera de autenticación fuerte.

Ilustración 2: Fundamentos de inWebo

Al focalizar el trabajo en un aumento de la seguridad en redes corporativas esta aplicación resulta capital para mejorar la seguridad de los entornos en los que se ha configurado y que estos no puedan ser saboteados, aunque se obtenga la contraseña que de acceso a dicho servicio ya que posteriormente pedirá ingresar un PIN anteriormente establecido por el usuario cuando se autentifique correctamente mediante el ingreso de usuario y contraseña.

Previamente a la configuración de entornos de inWebo es necesario registrar a los usuarios en los que se quiere implementar una o varias de las políticas de configuración posibles.

No significa que, porque un usuario este registrado en la plataforma de inWebo se le han de aplicar todas las políticas ya que, por ejemplo, en el caso de la configuración de inWebo para Office 365 las personas implicadas en dicha política se añaden desde el menú de políticas de Microsoft Azure.

Por ejemplo, en entornos como:

- Aplicaciones en la nube. Por ejemplo, Office 365 (tanto online como en local). Esta configuración se realiza por medio de Microsoft Azure.
- VPN para que las conexiones establecidas por las redes corporativas sean fidedignas.
- Inicio de sesión de los equipos. Esta opción resulta muy útil ya que al iniciar sesión en el equipo y poner la contraseña correctamente, se lanzará una notificación push al dispositivo móvil (configurado previamente) para que el usuario mediante el ingreso de su PIN personal introducido correctamente hará que la aplicación genere paralelamente un código OTP al servidor de autentificación que se encarga de verificar que el PIN es correcto para permitir el inicio de sesión.

3.1.2 Introducción a KeePass Password Safe

KeePass Password Safe es una herramienta software basada utilizada como aplicación de gestor de contraseñas que permite proteger credenciales.

Fue creado en 2003 por Dominik Reichl y actualmente es uno de los administradores de contraseñas más recomendados y utilizados en el mundo.

Ilustración 3: Fundamentos de KeePass

Actualmente se puede utilizar para los sistemas operativos de Windows, MacOS y Linux. También existe versión para móviles en los sistemas operativos de Windows Phone, Android e Ios.

Permite el almacenamiento de nombre de usuario, contraseña, URL de acceso al sitio web en caso de que se acceda por medio de un navegador y no sea una aplicación o fecha de vencimiento si esas credenciales están programadas para expirar en una determinada fecha.

Estas credenciales se pueden almacenar en distintos grupos dentro de la aplicación. Por defecto existen algunos grupos predefinidos y dentro de cada uno el usuario podrá añadir entradas almacenando así la información de las credenciales que desee.

Tras la instalación de KeePass, se ha de crear una base de datos donde almacenar las contraseñas. Estas serán protegidas mediante una clave maestra definida por el usuario una vez creada la base de datos. La seguridad de esta contraseña ha de ser alta es decir, se recomienda el uso de mayúsculas, minúsculas, números y signos para que esta sea robusta y difícil de interceptar.

KeePass ofrece como característica añadida el uso de la escritura automática que se puede configurar de forma individual para cada entrada lo que, mediante un simple atajo de teclado permitirá rellenar las credenciales de acceso a la página web o aplicación que se desee sin necesidad de tener que escribir a mano el usuario y la contraseña de acceso.

También se puede utilizar el generador de contraseñas que ofrece KeePass si se desean utilizar contraseñas distintas y con poca similitud para cada servicio web o aplicación. Este se puede parametrizar eligiendo así tanto el tipo de caracteres que queremos que compongan las contraseñas como la longitud de las mismas lo que, posteriormente generará un lista con contraseñas que cumplen los requisitos preestablecidos para la creación de las mismas.

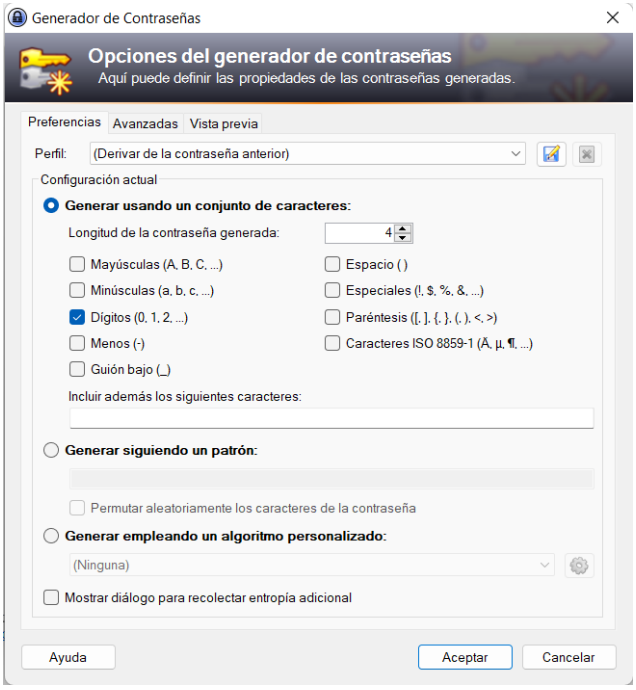

Ilustración 4: Generador de contraseñas de KeePass

Como método adicional de seguridad al establecer la clave maestra se puede generar un archivo de clave que generará el propio usuario de forma aleatoria mediante el movimiento del cursor sobre una pantalla lo que nos proporcionará dicho archivo. Aunque interceptasen la contraseña de nuestra base de datos, sin este archivo no podrían acceder a nuestra base de datos siendo un mecanismo que incrementaría exponencialmente la seguridad de nuestro entorno. Es altamente recomendable que el archivo de la base de datos y el de archivo de clave no compartan ruta ya que, si el archivo es interceptado sería poco útil.

En el entorno de una red corporativa se puede utilizar como gestor de credenciales a la hora de almacenar gran cantidad de contraseñas en un lugar común de forma que si, por ejemplo, 2 personas de la misma corporación cada una de un departamento necesitan una contraseña determinada de dicha corporación, mediante la creación de una base de datos conjunta entre dichos departamentos de la corporación, podrán, de forma segura, tanto acceder a la base de datos para consultar las credenciales como añadir nuevas credenciales que puedan ser utilizadas por otro empleado de dicha corporación.

Por tanto, este software es muy útil para proteger las credenciales de los trabajadores de una red corporativa y proteger la integridad de la empresa ya que mediante 1 contraseña (la clave maestra) se pueden almacenar un sinfín de credenciales en nuestra base de datos de forma segura.

3.1.3 Introducción a WhatsUp Gold

WhatsUp Gold es un software web enfocado a la monitorización de redes corporativas pudiendo monitorizar dispositivos como AP's, firewalls, servidores, switches, Virtual Data Centers, ESX's o aplicaciones de cualquier tipo.

Fue desarrollada por la empresa Progress Software y actualmente también es un software utilizado en gran cantidad de empresas.

Ilustración 5: Fundamentos de WhatsUp Gold

Esta herramienta esta basada en la búsqueda de dispositivos mediante dirección IP en su funcionalidad de análisis de red. Se puede parametrizar el rango de IP's que se quiere analizar ya que mediante la máscara de red se le puede indicar si se desea escanear un dispositivo determinado, parte de la red corporativa o la red corporativa en su totalidad.

Generalmente es utilizada por una corporativa para dar servicios de seguridad que otra empresa demanda o para el propio uso y seguridad de una misma empresa.

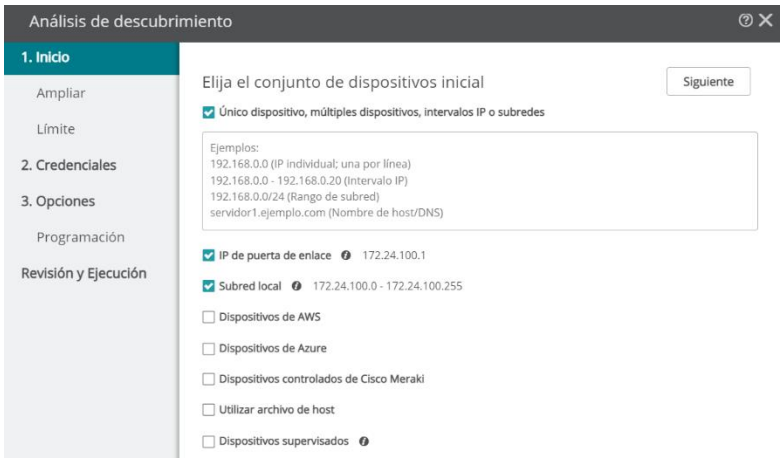

Ilustración 6: Escaneo de red mediante IP en WhatsUp Gold

Para la monitorización de dispositivos se utilizan monitores de rendimiento. WhastUp Gold tiene varios monitores creados por defecto como son el de memoria RAM, el de almacenamiento de disco, el de respuesta de ping o el del estado de las interfaces que posee el dispositivo. También existe la opción mediante la cual se pueden crear monitores de rendimiento personalizados para monitorizar una determinada característica de un dispositivo que uno de los monitores por defecto no es capaz de hacer.

Estos monitores se pueden configurar para que aparezcan luego en el panel de alertas para poder detectar así de manera rápida y visual los fallos o deterioros que puedan ocasionarse en la red corporativa que se está monitorizando.

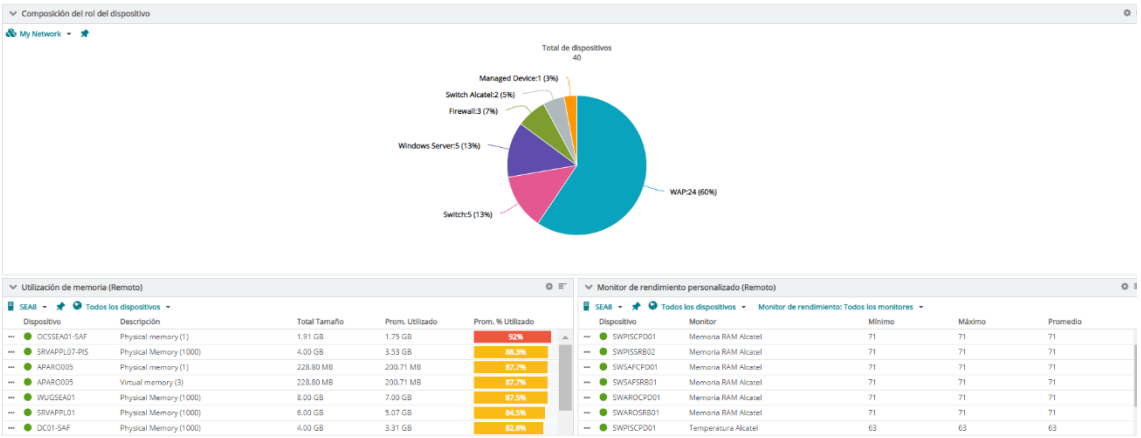

Ilustración 7: Panel de alertas en WhatsUp Gold

La implementación WhatsUp Gold se puede configurar de 2 formas distintas.

1) **En remoto**
   - Esta forma de configuración de WhatsUp Gold es característica por ejemplo de empresas como consultoras tecnológicas las cuales ofrecen servicios a otras corporativas que poseen un entramado de red de tamaño considerable.
   - Se realiza mediante la creación de una máquina virtual en el Virtual Data Center de otra red corporativa.
   - Una vez actualizada la máquina solo será necesario descargar en ella WhatsUp Gold y una vez descargada se configurará de forma que replique los datos desde el servidor de la empresa a la que se ofrecen los servicios de monitorización mediante esta herramienta al servidor de la empresa que los ofrece.
2) **En local**
   - Esta forma de configuración de WhatsUp Gold puede ser tanto como para empresas que ofrecen servicios a otras empresas con un tamaño de red corporativa reducido como para el uso propio en una misma empresa
   - Se realiza mediante la creación de una máquina virtual en el VDC de la red corporativa que ofrece los servicios
   - Si se quiere realizar un uso propio únicamente se tendrá que instalar la aplicación de WhatsUp Gold en el servidor creado
   - Por el contrario, si lo que se desea es dar servicio a otra empresa se ha de utilizar un túnel IPSec entre la empresa que ofrece servicios y la que los demanda para su correcto funcionamiento

Por tanto, este software posee una gran utilidad para empresas que ofrecen servicios a otras empresas ya que les permite monitorizar la estructura de red pudiendo detectar así por ejemplo algunos de los siguientes casos:

- Si un dispositivo deja de estar activo no dar respuesta de ping al servidor de WhatsUp Gold.
- Si el espacio de disco o de memoria RAM de un dispositivo esta lleno o parcialmente lleno con antelación a que el llenado de disco genere un problema en dicha máquina.
- Si la temperatura de dicho dispositivo excede los márgenes preestablecidos por los monitores lo que puede significar un sobrecalentamiento y deterioro de la misma.

4. Desarrollo

4.1 Implementación de inWebo en redes corporativas reales

Para la implementación de las mejores de seguridad proporcionadas por inWebo se ha decidido enfocarse en los siguientes escenarios:

- Office 365 tanto en su entorno de aplicaciones como en su entorno web
- Conexiones VPN con otras redes corporativas
- Inicio de sesión en equipos Windows

4.1.1 Implementación de inWebo en el entorno de Office 365

Para la configuración de inWebo en el entorno de Office 365 la red corporativa ha de cumplir los siguientes prerrequisitos:

- Tener una cuenta de Microsoft Azure de nivel premium, es decir, P1 o P2.
- Tener una cuenta de inWebo con un perfil registrado para realizar la configuración (la cuenta debe tener permisos de administrador desde la consola de inWebo).
- Iniciar sesión en dicha cuenta para poder configurar el conector inWebo Azure AD necesario para el correcto funcionamiento de inWebo para el entorno de Office 365.

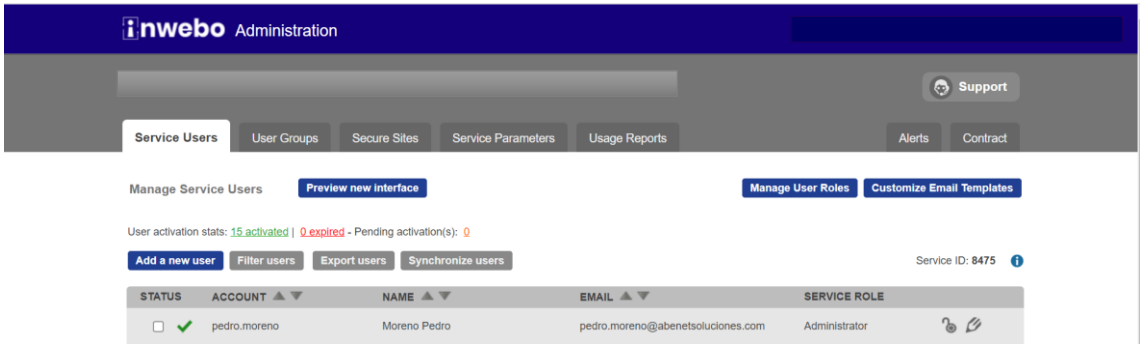

Ilustración 8: Consola de administración de inWebo

Una vez se cumplan los prerrequisitos mencionados anteriormente se han realizado los siguientes pasos:

1. Iniciar sesión en la cuenta con permisos de administrador
2. Acceder al menú de “Secure Sites” de la consola de inWebo

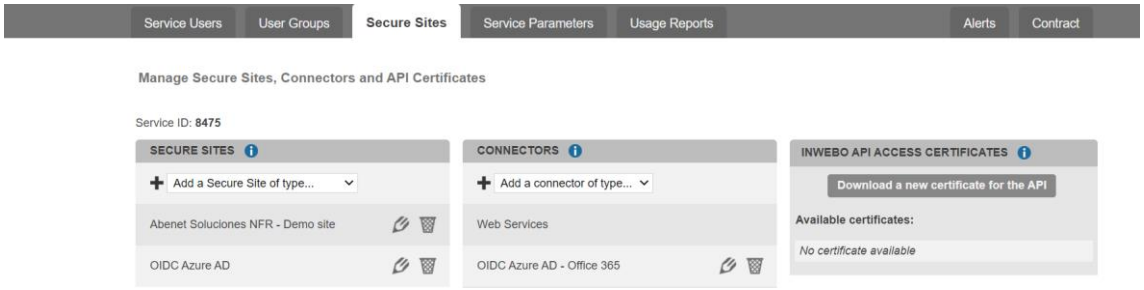

Ilustración 9: Secure Sites de inWebo

3. En el submenú “Connectors” ha configurado el conector Azure AD Connector de la siguiente forma.

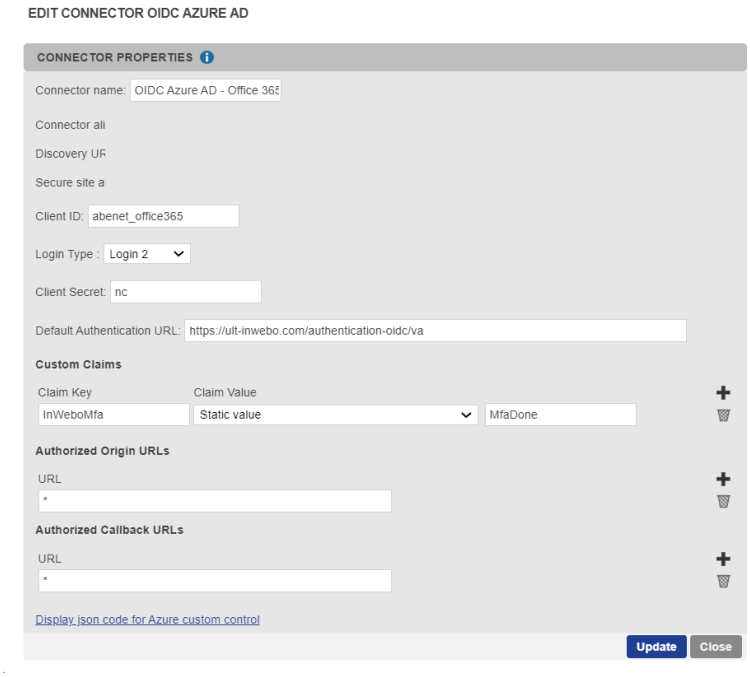

Ilustración 10: Conector Azure AD de inWebo

4. En la parte inferior de la configuración del conector aparece el archivo JSON correspondiente al conector Azure AD creado. Copiamos el código JSON que aparece.
5. En el entorno de Microsoft Azure iniciamos sesión en la cuenta de administrador (mencionada en los prerrequisitos).
6. Creamos un nuevo control de acceso personalizado en Azure AD en dicha cuenta accediendo al menú Todos los servicios>Identidad>Acceso condicional de Azure AD>Controles personalizados> Nuevo control personalizado donde introduciremos el archivo JSON obtenido anteriormente.
7. Procedemos a la creación de una directiva de acceso condicional en el entorno de Microsoft Azure accediendo al menú Azure Active Directory>Seguridad>Acceso Condicional>Nueva Directiva

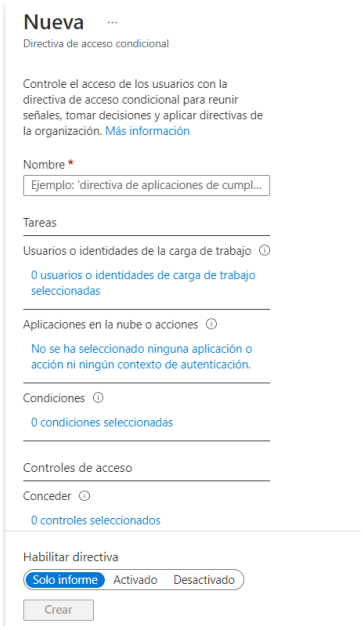

Ilustración 11: Nueva directiva Azure AD de inWebo

8. Ya que cada red corporativa puede tener una forma y/o estructura distinta a la hora de funcionar en este apartado de la directiva se puede configurar lo siguiente:

    8.1) El/los usuario(s) de la red corporativa a los que se les aplicará la directiva.

    8.2) La(s) 18plicación(es) a la(s) que se aplicará la política. Por ejemplo Office 365.

    8.3) Las condiciones que se pueden aplicar a la política las siguientes configuraciones:

        8.3.1) Plataformas de dispositivos a los que aplicar la política (Android, Ios, Windows, etc)

        8.3.2) Ubicaciones donde se pueden incluir y excluir direcciones IP dentro de la política

        8.3.3) Aplicaciones cliente a las que se puede aplicar (Navegador, aplicaciones móviles, aplicaciones de escritorio, etc)

        8.3.4) Filtro para dispositivos donde se puede crear una regla dentro de la directiva para que esta se aplique a dispositivos específicos

    8.4) Controles de acceso donde se puede permitir o bloquear acceso

    8.5) Que se puede configurar para establecer una frecuencia de inicio de sesión con un periodo de tiempo parametrizable (horas o días).

9. Finalmente se activará la política seleccionando el botón activado y se guardará dicha política pulsando el botón guardar. Desde ese momento la política estará en ejecución.

Cabe destacar que la frecuencia de inicio de sesión comenzará una vez inicie sesión el usuario en servicio sobre el que se aplica.

4.1.2 Implementación de inWebo en el entorno de Windows Logon

Antes de iniciar la configuración para implementar inWebo en el inicio de sesión de Windows es necesario comprobar que en la consola de inWebo de la red corporativa está activada la opción **Windows Logon** en ajustes generales.

Ilustración 12: Activación de Windows Logon en la consola de inWebo

Posteriormente se han de ejecutar los siguientes pasos:

1. Acceder al servicio de administración de usuarios dentro de la consola de inWebo.

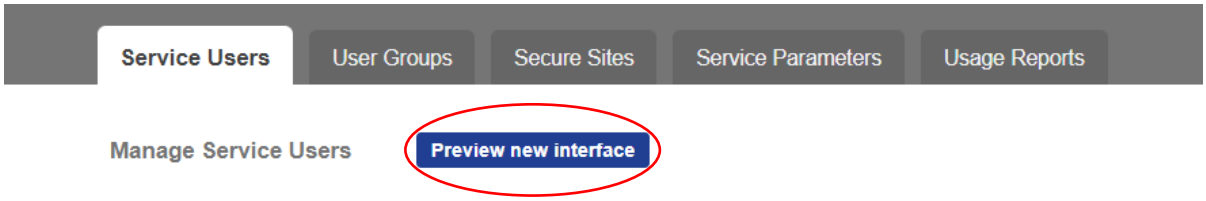

Ilustración 13: Servicio de administración de usuarios en la consola de inWebo

2. Accedemos al menú “Windows Logon” o “Inicio de sesión de Windows” y agregamos un conector. En mi caso he creado el conector “Inicio de sesión Windows Abenet” para poder implementar en la empresa en la que he realizado las prácticas.

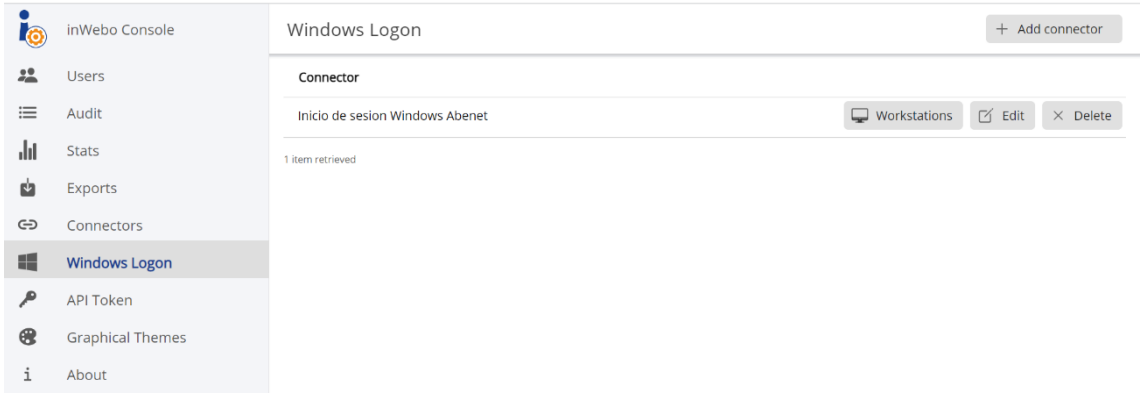

Ilustración 14: Conector de Windows Logon en la consola de inWebo

Cabe destacar que en la opción edit podremos ver tanto el alias del conector como la clave AES que posteriormente utilizaremos para finalizar esta implementación.

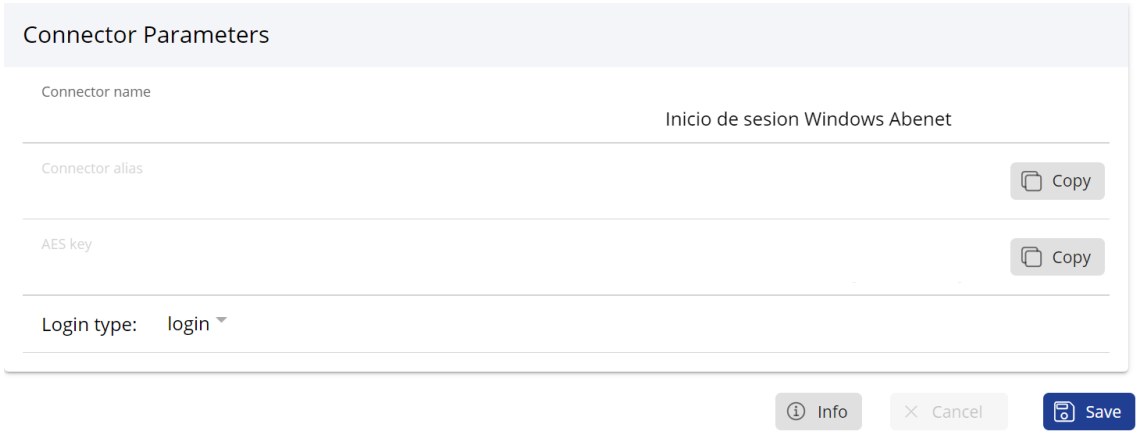

Ilustración 15: Parámetros conector de Windows Logon en la consola de inWebo

3. Posteriormente procederemos en una estación de trabajo a descargar el archivo MSI proporcionado por inWebo y una vez hayamos ejecutado el instalador nos pedirá tanto el alias del conector como la clave AES que hemos mencionado anteriormente, por tanto las introducimos.

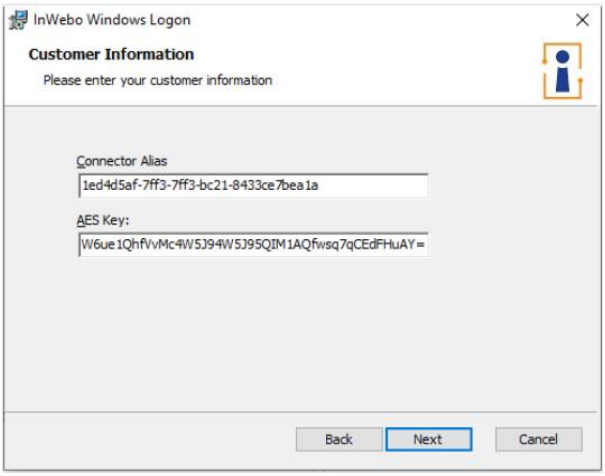

Ilustración 16: Parámetros conector de Windows Logon en archivo .msi de inWebo

4. Una vez tenemos instalado el archivo .msi podremos configurar una GPO de forma que nos obligue a iniciar sesión mediante la doble autenticación de inWebo. Si no realizamos esto no tendrá sentido realizar esta implementación ya que no se incrementará el nivel de seguridad en este ámbito.

5. Una vez ya esta implementado iniciamos sesión ingresando las credenciales del usuario. Posteriormente se lanzará una notificación push al móvil con el que tengamos configurada la doble autenticación donde deberemos ingresar el PIN que tiene dicha cuenta para iniciar sesión en el portal de inWebo para que se autentifique contra el servidor inWebo correctamente mediante la verificación de códigos OTP comentada anteriormente.

Finalmente cabe añadir que desde la consola en el menú de Windows Logon de inWebo

4.1.3 Implementación de inWebo en el entorno VPN de Sophos XG

Antes de detallar la configuración, cabe destacar que se ha realizado la implementación en el entorno de Sophos XG ya que es el proveedor de firewall y VPN de la empresa en la que he realizado las prácticas.

Para la configuración de inWebo en el entorno VPN SSL de Sophos XG he seguido los siguientes pasos:

1. Se ha de iniciar sesión en la consola de administración de inWebo y en sitios seguros agregar un conector de tipo Radius Push.

2. En el conector de Radius se tienen que añadir tanto la IP del servidor Radius al que el conector ha de apuntar como la password o secreto Radius que se ha establecido en dicha IP.

3. Posteriormente accedemos al portal de Sophos XG y accedemos al menú **Autenticación > Servidores** y seleccionamos agregar añadiendo los campos correspondientes al servidor que queramos configurar

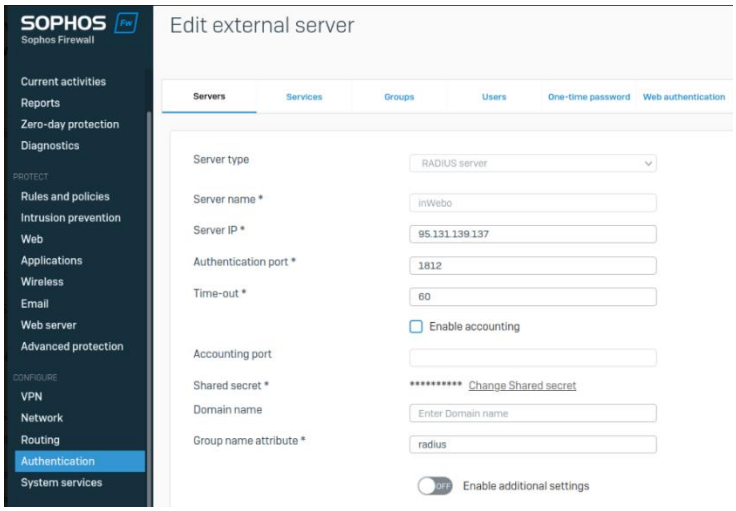

Ilustración 17: Parámetros conector de VPN en Sophos XG de inWebo

4. Posteriormente se ha de configurar el método de autenticación para VPN SSL accediendo al menú **Autenticación>Servicios** en el apartado de **métodos de autenticación SSL VPN**.

5. Hacemos click en aplicar y probamos a iniciar sesión en la aplicación Sophos Connect (es la aplicación proporcionada por Sophos para los servicios de VPN) en la VPN sobre la que hayamos realizado la configuración.

Ilustración 18: Inicio de sesión en Sophos Connect para la VPN configurada.

6. Tras ingresar las credenciales nos mandará una notificación push al dispositivo móvil del cual tengamos configurado para la doble autenticación donde ingresaremos el PIN de acceso para que se produzca la verificación mediante OTP y nos permita establecer dicha conexión VPN mediante el uso de doble autenticación.

4.2 Implementación de KeePass en redes corporativas reales

Para la implementación de KeePass en Abenet primero hemos tenido varias reuniones para acordar la forma de actuar y como organizarnos en la instalación y gestión de las bases de datos de KeePass.

Para la instalación se han de seguir los siguientes pasos:

1. Acceder al sitio oficial de KeePass y descargar dicho software
2. Una vez descargado abrimos el programa y nos aparecerá la siguiente:

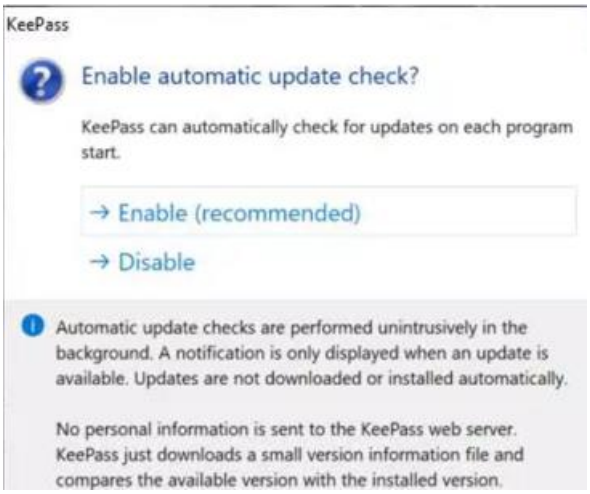

Ilustración 19: Actualizaciones automáticas en KeePass

donde seleccionaremos la opción “Enable” para que KeePass este permanentemente actualizado y no quede obsoleto y vulnerable.

3. Tras haber realizado esto nos aparecerá el menú principal de KeePass donde procederemos a crear la base de datos en la que se almacenarán las claves de la persona/departamento/empresa a la que pertenezca.

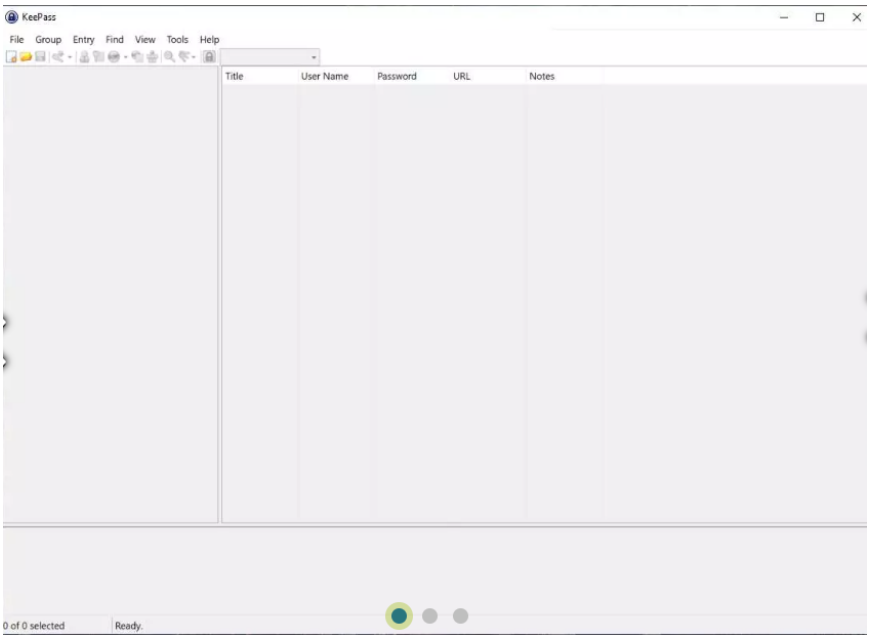

Ilustración 20: Menú principal de KeePass

4. Para la creación de una nueva base de datos se accede al menú de archivo donde se crea una nueva base de datos de la cual se podrá configurar el nombre y la ruta en la que alojarse tanto de la base de datos como del archivo de claves de que explicare a continuación.
5. Llegados a este momento habrá que elegir como y donde queremos almacenar nuestra base de datos. En mi estancia en prácticas expuse las siguientes opciones:

    a. **Almacenar tanto la base de datos como el archivo clave o key en One Drive Personal**
        - Pros
            - Los archivos están en la nube y por tanto es más difícil acceder a ellos
            - Los archivos son accesibles en caso de que el equipo se cambie o sea perdido
        - Contras
            - Si perdemos el equipo o cae en manos de alguien no deseado, en el periodo en el que estamos verificados mediante doble autenticación de inWebo podría acceder fácilmente a nuestro OneDrive y sustraer ambos archivos

    b. **Almacenar la base de datos en una ruta local en nuestro equipo y el archivo key en la nube**
        - Pros
            - Aunque consiguiesen tener acceso a nuestro equipo necesitarían el acceso a OneDrive para poder obtener el archivo clave .keyx y abrir así la base de datos.
        - Contras
            - El mismo que en el caso anterior ya que si el equipo cae en manos de alguien pueden tener acceso igualmente.

    c. **Almacenar la base de datos en One Drive al igual que el archivo .keyx pero cambiándole el nombre y extensión a este**
        - Pros
            - Ambos archivos estarían en la nube con el añadido de que el archivo .keyx al no tener ni nombre ni extensión de un archivo clave pudiendo parecer aparentemente por ejemplo un archivo Word o Excel
            - Internamente la empresa decidiría la forma en la que configurar dicho archivo clave sin dejar constancia de ello para que solo el departamento técnico pueda saber que realmente el archivo clave es lo necesario para acceder a la base de datos en cuestión
        - Contras
            - El mismo en ambos casos anteriores con la dificultad de encontrar el archivo clave ya que sin el no podrán acceder a la base de datos

d. **Almacenar la base de datos en un servicio en la nube como puede ser One Drive y el archivo clave en otro servicio en la nube como puede ser Dropbox**
    - Pros
        - Ambos archivos se encuentran en la nube y por tanto es más complicado tener acceso a ellos
    - Contras
        - Hay gran cantidad de empresas que no trabajan con documentos almacenados en Dropbox o Google Drive debido a su vulnerabilidad
        - Si accediesen al sitio en el que el archivo clave estuviese almacenado este no estaría ni con nombre ni formato distinto al original por lo que sería fácilmente detectable si el equipo cae en manos de alguien no deseado.

4.3 Implementación de WhatsUp Gold en redes corporativas reales

Para la implementación de WhatsUp Gold como herramienta de monitorización se han de contemplar 2 escenarios distintos:

- **Implementación en remoto:** es característica de empresas con una infraestructura de red amplia. El procedimiento a realizar es la instalación de WhatsUp Gold en una máquina virtual creada en el Vcenter de dicha empresa que detallare a continuación. Cabe destacar que al haber realizado las prácticas en la empresa Abenet Soluciones he podido ver el funcionamiento del departamento técnico de una consultora tecnológica por lo que tenemos acceso a las credenciales de la infraestructura de red de los clientes actuando así como departamento técnico de las empresas en cuestión.

    1. Se accede al Vcenter de la empresa en la que se quiera realizar el montaje de WhatsUp Gold.
    2. Se accede a la Vapp en la que se quiere crear la máquina virtual.
    3. Se accede al apartado de máquinas virtuales.
    4. Se crea una nueva máquina virtual. En prácticas he estado utilizando los siguientes parámetros:
        a. Espacio memoria RAM: 8GB
        b. CPU's: 2
        c. Espacio de almacenamiento asignado: 40 GB revisando el tipo de almacenamiento para elegir el adecuado (SSAS, etc)
        d. Elegir la opción necesaria en el adaptador NIC
        e. Elegir la configuración mediante Ipv4 (por defecto esta Ipv6)
    5. Tras haber personalizado los parámetros anteriores se ha de cambiar el nombre de la máquina virtual para poder localizarla en análisis posteriores
    6. Una vez la máquina ya esta configurada se ha de arrancar y se ha de instalar el software de WhatsUp Gold en dicha máquina activando previamente la licencia contratada
    7. Para la seguridad de dicha máquina virtual hemos instalado el producto antivirus de Sophos
    8. Comprobar desde el servidor central de WhatsUp Gold de Abenet que replica correctamente los datos

- **Implementación en local:** es características de empresas que tienen un entramado de red más simple o más reducido que las anteriores.

    En este caso basta con simplemente utilizar lo siguiente:
    - El servidor de WhatsUp Gold de Abenet
    - Realizar un túnel IPSec desde el firewall de Abenet hacia el firewall del cliente en cuestión para poder añadir posteriormente los dispositivos en el servidor central.

Cabe añadir también que se realiza de forma automática una reserva de recursos de los servidores de WhatsUp Gold ya que si se quiere acceder a un servidor que, aunque este encendido, lleva un tiempo considerablemente largo (entiéndase por esto 12 horas o más) por medio de la búsqueda por dirección IP del navegador este tardará un tiempo (entorno a unos 2 minutos) en devolvernos la página web de WhatsUp Gold de dicho servidor.

4.3.1 Implementación de monitores en dispositivos para WhatsUp Gold

La implementación de monitores para los distintos dispositivos (ya sean switches, servidores, Vcenters, ESX, NAS o AP's) que se han de monitorizar en esta herramienta resulta crucial para detectar y prevenir posibles problemas mediante umbrales que se explicarán posteriormente se pueden recibir notificaciones que avisen de ello en redes corporativas como pueden ser:

- Dispositivos que están quedándose sin espacio de disco disponible.
- Dispositivos que no tienen ping o a los que no se puede comunicar desde el servidor de WhatsUp Gold.
- Uso demasiado elevado de memoria física o CPU's.
- Interfaces de dispositivos que se encuentran inoperativas.
- Temperaturas elevadas por ejemplo en switches.

A continuación, voy a detallar los monitores que he implementado para cada tipo de dispositivo en las distintas redes corporativas:

- Dispositivos de almacenamiento NAS:
  - Monitor de ping: para comprobar la actividad de dicho dispositivo.
  - Monitor de memoria física: para controlar el estado de la parte física de la memoria RAM de los dispositivos.
  - Monitor de CPU's: para comprobar el estado de cada una de ellas.
  - Monitor de interfaces: donde podemos seleccionar las interfaces del dispositivo que queremos monitorizar.
- AP's:
  - Monitor de ping: para comprobar la actividad de dicho dispositivo.
  - Monitor de memoria física: para controlar el estado de la parte física de la memoria RAM de los dispositivos.
  - Monitor de CPU's: para comprobar el estado de cada una de ellas.
  - Monitor de interfaces: en este caso deshabilité las interfaces inactivas
- ESX's:
  - Monitor de ping: para comprobar la actividad de dicho dispositivo.
  - Monitor de almacenamiento de disco de sus distintas unidades: para controlar el espacio disponible en cada una de ellas.
  - Monitor de memoria física: para controlar el estado de la parte física de la memoria RAM de los dispositivos.
  - Monitor de CPU's: para comprobar el estado de cada una de ellas.
  - Monitor de interfaces: donde podemos seleccionar las interfaces del dispositivo que queremos monitorizar.
- Switches: este tipo de dispositivos no utilizan los monitores que WhatsUp Gold proporcionan por defecto. Normalmente he trabajado con switches Alcatel aunquede los cuales creábamos los siguientes monitores:
  - Monitor de ping: para comprobar la actividad de dicho dispositivo.
  - Monitor de interfaces: donde podemos seleccionar las interfaces del dispositivo que queremos monitorizar.
  - Monitor de temperatura de Alcatel: para comprobar que la temperatura del switch Alcatel no se exceda lo que provocaría la inutilización del dispositivo por su deterioro.
  - Monitor de temperatura de RAM: para comprobar el estado de la memoria RAM de switches Alcatel
  - Monitor de CPU's de Alcatel: para comprobar el estado de las CPU's de switches Alcatel.

Cabe destacar en cuanto a las credenciales SNMP la importancia del **campo OID** de SNMP en las propiedades principalmente de los Switches que se monitoricen ya que para la creación de monitores SNMP en los switches para poder obtener información acerca de la temperatura, la RAM o las CPU's se necesitará buscar cual es el OID necesario para que los switches muestren las características anteriormente citadas.

Ilustración 21: Campo OID de SNMP en WhatsUp Gold

Para ello he utilizado el programa Paessler SNMP Tester que, además de poder confirmar mediante él si el servicio SNMP esta activo, podemos ver la información que obtenemos de él y por tanto comprobar la configuración de los monitores de rendimiento SNMP.

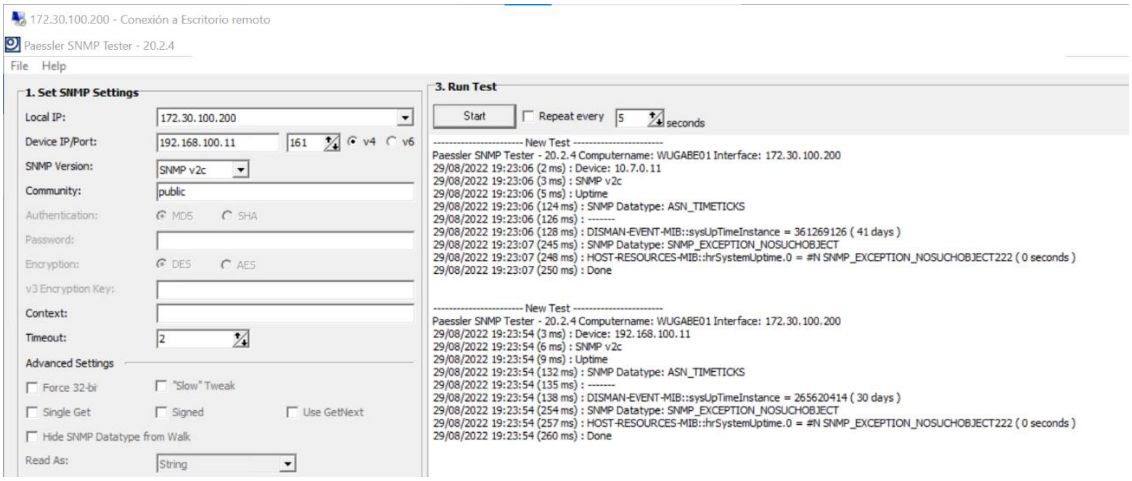

Ilustración 22: Paessler en WhatsUp Gold

En esta imagen se pueden ver algunos resultados desde el servidor de WUG de Abenet de los test SNMP de algunos switches así como los días que lleva el servicio SNMP activo.

Los campos más importantes para poder testear correctamente el servicio SNMP las IP's necesarias son:

- Local IP: campo en el que hemos de introducir la dirección IP del servidor de WUG desde el que se están haciendo las pruebas SNMP en el programa.
- Device IP/port: IP de la cual se quieren consultar las características SNMP.
- SNMP version: se utiliza la versión snmpv2, posteriormente se justifica por que.
- Community: tanto el nombre de la comunidad de lectura como la de escritura por defecto son public al activar SNMP por tanto en este campo introduciremos "public" también.

- Servidores:
  - Monitor de ping: para comprobar la actividad de dicho dispositivo.
  - Monitor de almacenamiento de disco de sus distintas unidades: para controlar el espacio disponible en cada una de ellas.
  - Monitor de memoria física: para controlar el estado de la parte física de la memoria RAM de los dispositivos.
  - Monitor de CPU's: para comprobar el estado de cada una de ellas.

4.3.2 Implementación de credenciales en dispositivos para WhatsUp Gold

Para que los monitores mencionados puedan mostrar los datos es necesario que los dispositivos tengan asignados algún tipo de credenciales.

En WhatsUp Gold a la hora de la realización del escaneo de red para añadir los dispositivos podemos asignar un tipo de credenciales.

Ilustración 23: Tipos de credenciales en WhatsUp Gold

Dichas credenciales también se pueden asignar una vez el dispositivo este escaneado y monitorizado en la red corporativa.

En la Biblioteca de credenciales podemos configurar los tipos de credenciales que tenemos.

Muestro en este caso la biblioteca de credenciales del Servidor de WhatsUp Gold de Abenet con las distintas credenciales que hemos necesitado crear para la monitorización de clientes VPN sobre dicho servidor:

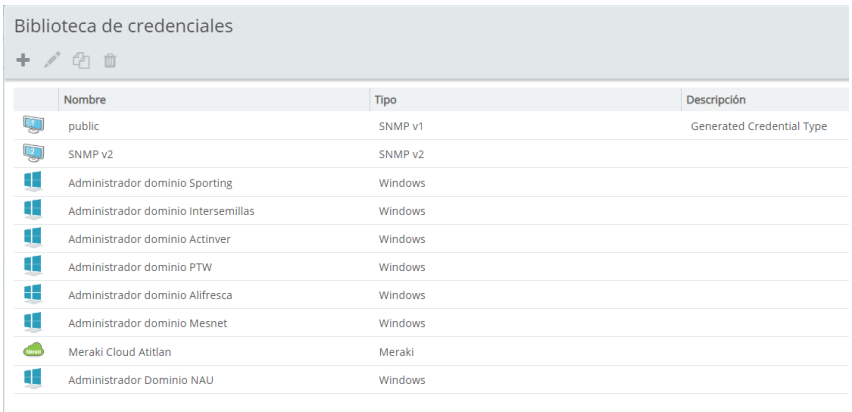

Ilustración 24: Biblioteca de credenciales en WhatsUp Gold

Durante la implementación de esta herramienta en redes corporativas reales he utilizado principalmente los siguientes tipos de credenciales:

- **Credenciales Windows:** utilizado para los servidores cada red corporativa. He utilizado las credenciales de administrador de dominio para cada una de ellas de la siguiente forma:

Ilustración 25: Credenciales Windows en WhatsUp Gold

- **Credenciales SNMP**: utilizado para switches, la mayoría de los firewalls, NAS, AP's, ESX's y Vcenter's. Existen 3 versiones de SNMP; SNMPv1, SNMPv2 y SNMPv3.
  - SNMPv1: primera versión de SNMP, comparte gran cantidad de características con SNMPv2.
  - SNMPv2: apareció en 1993 mejorando la versión primaria mediante 3 nuevas operaciones en este protocolo:
    - GetBulk: para recuperar grandes cantidades de datos de forma eficiente como por ejemplo las columnas de una tabla
    - Inform: para que el agente envíe información de forma espontánea al gestor y reciba una confirmación del mismo.
    - Report: para que el agente envíe espontáneamente errores y excepciones de protocolo
  - SNMPv3: apareció en 1997 y es un estándar que reemplaza a SNMPv1 y SNMPv2 ya que define una capacidades extra de administración y seguridad que sus versiones anteriores. Existen 3 tipos de SNMPv3:
    - NoAuthNoPriv: sin autenticación ni privacidad. Los mensajes no se encuentran encriptados. Es obvio que este tipo solo ha de utilizarse en redes cerradas y seguras ya que en otro entorno serían vulnerables
    - AuthNoPriv: con autenticación y sin privacidad. Los mensajes no se encuentran encriptados durante la transmisión pero estos han de ser autenticados para poder actuar sobre ellos.
    - AuthPriv: con autenticación y privacidad. Es la implementación de SNMPv3 más segura. Todos los datos se cifran durante la transmisión y los mensajes SNMP han de autenticarse.

Para la implementación de WhatsUp Gold en redes corporativas reales he utilizado SNMPv2 ya que es más seguro que SNMPv1 pero no tan complejo como SNMPv3 a la hora de activarlo y utilizarlo.

Ilustración 26: Credenciales SNMP en WhatsUp Gold

A continuación describo brevemente como he activado el protocolo SNMP en los dispositivos enumerados anteriormente:

- NAS: accediendo al dispositivo de almacenamiento mediante sus credenciales y activando en la pestaña de Servicios con la comunidad public de lectura y escritura.
- AP's: accediendo a la controladora WLC de AP's donde se supervisan los AP's de cada red corporativa y en la pestaña SNMP he activado el servicio SNMP con comunidad public.
- ESX's: he accedido por conexión SSH mediante putty y he lanzado los comandos necesarios para activar SNMPv2.
- Vcenter's: he accedido por conexión SSH mediante putty y he lanzado los comandos necesarios para activar SNMPv2.
- Switches: he accedido por conexión SSH mediante putty y he lanzado los comandos necesarios para activar SNMPv2.
- Firewall: he accedido al firewall de cada red corporativa y en el aparado de Servicios>SNMP he activado SNMPv2.

4.3.3 Implementación de umbrales en servidores para WhatsUp Gold

Para la implementación de umbrales en los servidores de WhatsUp Gold se ha de acceder al menú de Biblioteca de Credenciales y dentro de el al submenú de Umbrales.

Dentro de Umbrales podremos ver que por defecto hay 19 umbrales creados sobre los monitores por defecto y funcionalidades por defecto que incorpora WhatsUp Gold. Estos umbrales se pueden parametrizar de la forma que se desee ya que se pueden modificar los parámetros de los mismos por ejemplo si queremos que nos avise si la disponibilidad de ping desciende del 75% en nuestros dispositivos:

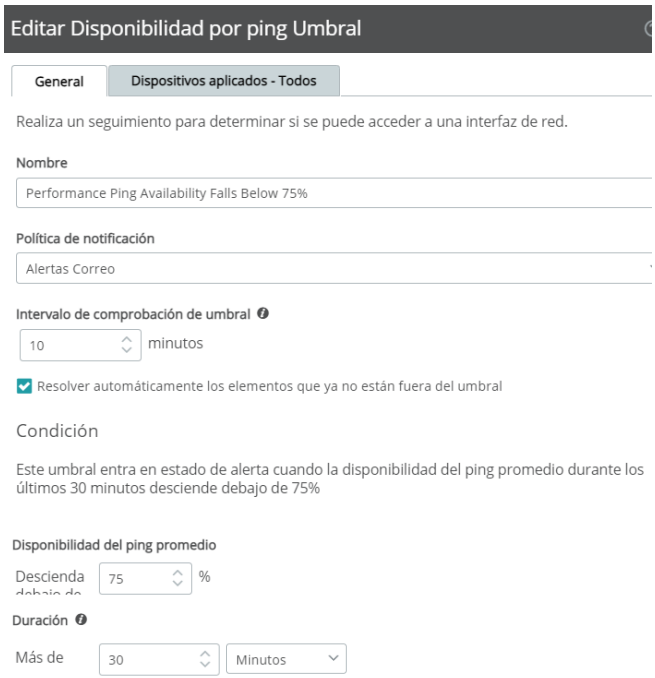

Ilustración 27 Configuración de umbrales en WhatsUp Gold

Cabe destacar que los umbrales se aplican por defecto a todos los dispositivos que tengan el monitor correspondiente a dicho umbral activo.

Si no se desea que se aplique a todos los dispositivos activos y supervisados se puede filtrar sobre cuales ha de actuar dicho umbral y sobre cuales no en la pestaña de “Dispositivos aplicados” y también se puede definir sobre que dispositivos si se debe aplicar, según se prefiera. A continuación se refleja dicho menú:

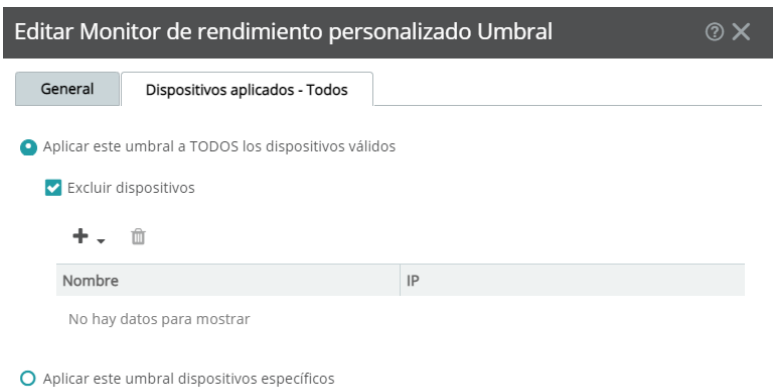

Ilustración 28 Filtrado de dispositivos para umbrales en WhatsUp Gold

Esto se puede aplicar por ejemplo en el servidor central de Whats Up Gold de Abenet ya que tiene varios dispositivos del mismo tipo (switches, AP's, servidores, Vcenter's, …) si por ejemplo no queremos recibir alertas de caída de porcentaje de ping por debajo de un límite en AP's que se encuentran en una sede con problemas de conexión a internet debido a la inestabilidad o reserva de recursos de los túneles IPSec creados.

Para que dichos monitores generen alertas y por tanto utilicen los umbrales establecidos, dentro del umbral, como vemos en la imagen anterior, hemos de establecer que el umbral ha de utilizar la política de notificación creada que explicaré a continuación.

Como hemos visto antes, existen casos como por ejemplo los switches Alcatel en los que los monitores por defecto no sirven y por tanto hay que crear unos monitores de rendimiento SNMP. Es por ello que también será necesaria la creación de umbrales para poder controlar los monitores por ejemplo de temperatura sin que esta sobrepase de un número de grados Celsius parametrizables dentro del propio umbral.

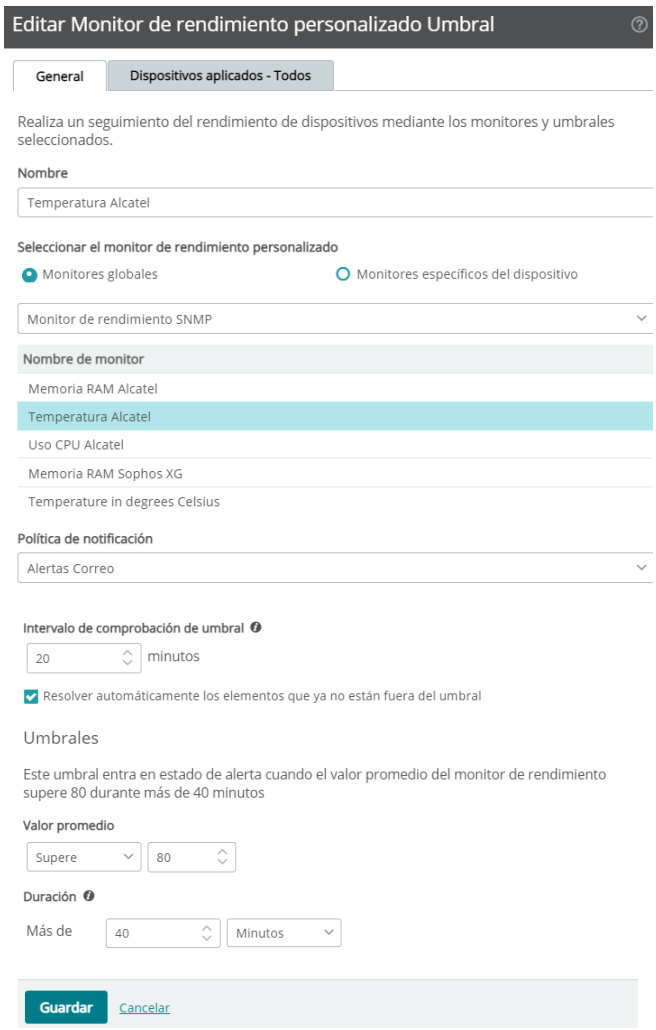

Ilustración 29 Umbrales SNMP personalizados en WhatsUp Gold

En el caso de los monitores de rendimiento SNMP personalizados, además de seleccionar la política de notificación y establecer los criterios a seguir en el umbral se ha de marcar el monitor de rendimiento SNMP personalizado sobre el que actuará dicho umbral. En esta imagen vemos que el umbral SNMP personalizado de temperatura en grados Celsius se aplicará para el monitor de rendimiento SNMP de Temperatura Alcatel.

4.3.4 Implementación de alertas en servidores para WhatsUp Gold

Para la implementación de alertas en los distintos servidores de WhatsUp Gold he seguido los siguientes pasos:

1. He accedido a la IP del servidor del cual he querido configurar las alertas

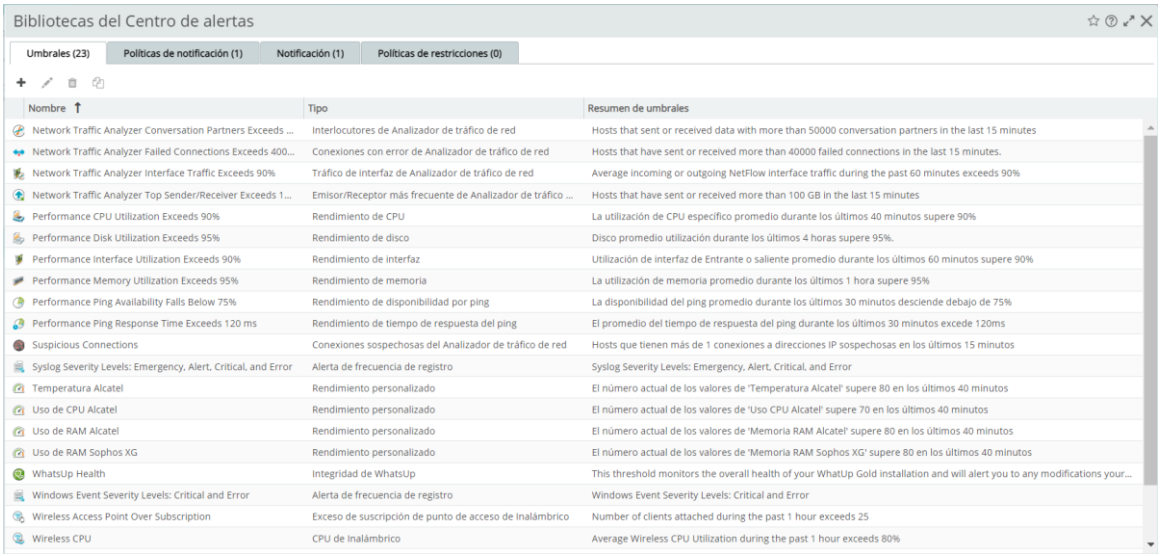

Ilustración 30: Biblioteca de centro de alertas en WhatsUp Gold

2. He accedido al menú de Biblioteca del centro de alertas y dentro de ahí al menú de Notificación donde aparecen las acciones de alertas de correo.

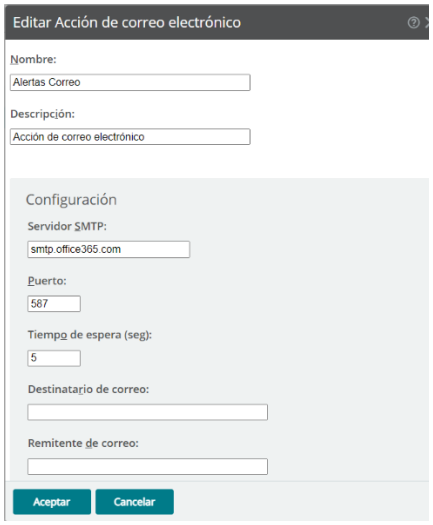

Ilustración 31: Alertas de Correo (I) en WhatsUp Gold

Los parámetros a configurar son:

- Nombre: se puede poner cualquiera.
- Descripción: se puede añadir una breve descripción de la efecto que tendrá la acción
- Servidor SMTP: se ha de configurar correctamente el servidor SMTP necesario para que WhatsUp Gold pueda enviar correctamente correos al destinatario que añadamos.
- Puerto: en nuestro caso para que envíe correos el puerto que se ha de especificar el es 587.
- Tiempo de espera: es parametrizable, por defecto aparecen 5 segundos.

- Destinatario del correo: se ha de añadir la dirección de correo a la que se quiere que lleguen las alertas
- Remitente de correo: se ha de añadir la dirección de correo que se encargará de enviar los correos al destinatario. Para ello se ha de configurar una cuenta de correo como la responsable de ello, en nuestro caso es alertas.wug@abenetsoluciones.com.

3. Configuro el contenido del correo pudiendo seleccionar si el tipo de formato quiero que sea HTML o sin formato (uso HTML) y configurar el cuerpo de dicho mensaje:

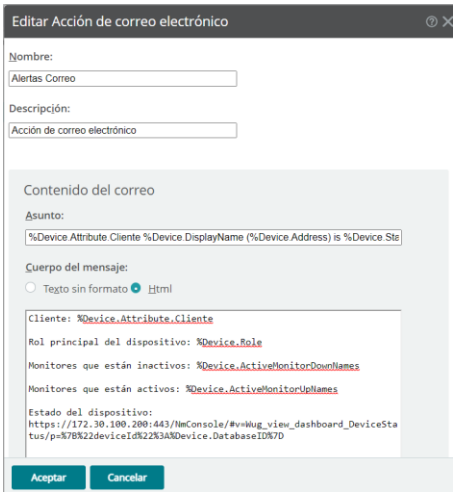

Ilustración 32: Alertas de Correo (II) en WhatsUp Gold

4. Configuración del centro de alertas donde se puede modificar el asunto del correo electrónico a enviar, incluir un hipervínculo que te redireccione dashboard del centro de alertas correspondiente, elegir si utilizar el protocolo HTTP o HTTPS, elegir si utilizar una dirección IP dinámica o estática y el puerto sobre el que queremos que trabaje dicha dirección.

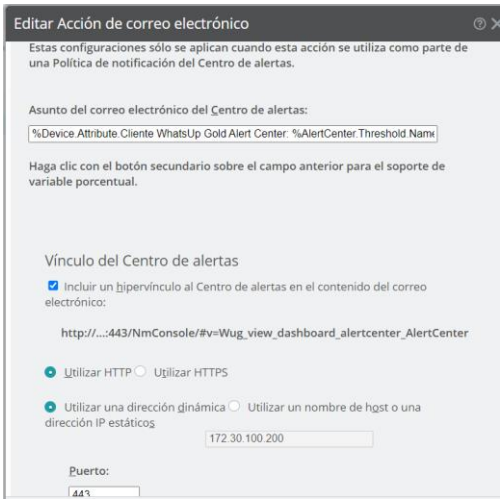

Ilustración 33: Alertas de Correo (III) en WhatsUp Gold

Una vez esta configurado todo en el submenú de notificación accedemos ahora al submenú de **Políticas de notificación** donde crearemos una política de notificación denominada también Alertas Correo donde podremos seleccionar los pasos a seguir:

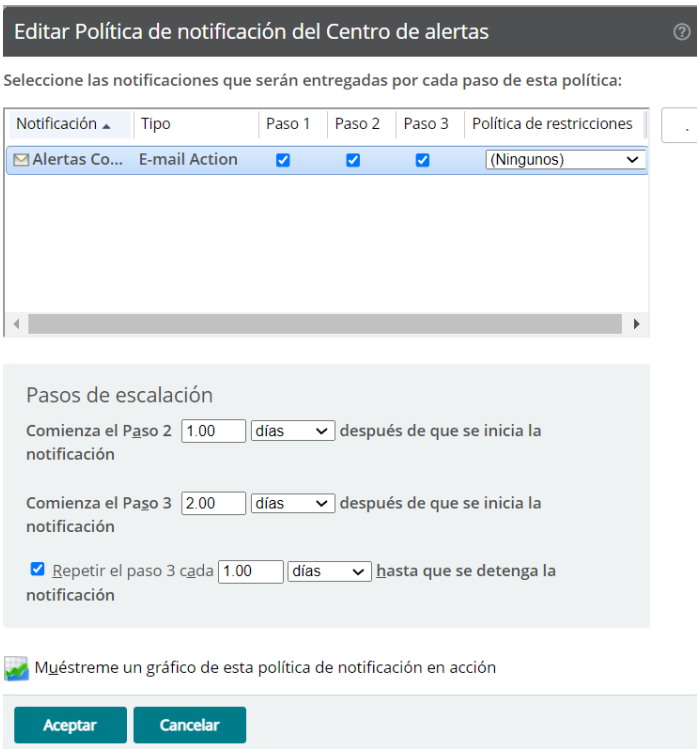

Ilustración 34: Pasos de alertas de notificación en WhatsUp Gold

En el caso de los servidores que he configurado se han parametrizado notificaciones de la siguiente forma:

- Si un monitor sobrepasa un umbral comienza el paso 1 y envía una notificación
- Si este sigue sobrepasando dicho umbral 24 horas pasará al paso 2 y volverá a enviar otra notificación
- Si se sigue excediendo el umbral pasadas 48 horas se pasará al paso 3 y se enviará notificación al correo configurado en las alertas cada 24 horas hasta que se solucione dicha alerta y el monitor vuelva a estar por debajo del umbral en cuestión.

4.3.5 Implementación de dependencias en servidores para WhatsUp Gold

La creación de dependencias es una de las principales ventajas en esta herramienta de monitorización de infraestructura de redes corporativas ya que se puede configurar de forma que un monitor de rendimiento, como puede ser el del ping, de varios dispositivos dependa a su vez del monitor de rendimiento de ping de otro dispositivo que se establece como raíz de la dependencia.

A la hora de realizar estas dependencias he establecido como raíz de dicha dependencia al firewall en cada red corporativa. Existe algún caso en el que la raíz de la dependencia se ha establecido en el Switch de Core (switch principal).

Un ejemplo de ello podría ser la infraestructura de red del Delibreads ya que posee 4 líneas de firewall distintas y por tanto habría que establecer una de ellas como raíz de la dependencia pero estas son independientes entre si y por tanto podría dejar de tener ping 1, 2 o 3 líneas y que en la que establecemos como raíz de dependencia siga el monitor de ping activo y por tanto no recibir una alerta por correo en relación a la pérdida de ping.

Una vez establecida la raíz de dependencia seleccionamos todos los dispositivos (AP's, switches, Vcenter's, ESX's, etc) que queremos que tengan el monitor de ping dependiente de la raíz y establecemos dependencia de la actividad

Ilustración 35: Dependencia de la actividad en WhatsUp Gold

Una vez esté creada la dependencia podemos comprobar su existencia accediendo al Tablero de Inicio en la versión Web del servidor de WhatsUp Gold de la infraestructura de red en que desarrollemos dicha dependencia.

Ahí seleccionaremos la opción de agregar informes y buscaremos "Dependencias" seleccionando la localización que queremos que tenga el informe de dependencias en dicho Tablero de Inicio (se puede agregar tanto al encabezado, como al pie de página, como en una columna determinada que seleccionemos).

Aquí podemos ver un ejemplo de dependencia de los dispositivos de la infraestructura de Alifresca sobre su Firewall en referencia al monitor de ping:

Ilustración 36: Dependencia en la infraestructura de Alifresca en WhatsUp Gold

Vemos que tanto AP's (APB090, AP00FE, APC4B3), como Switches (SWCORE1, SWACCESO01), como servidores (SERVER, FSALI01, DCALI02) dependen del monitor de ping del Firewall y que por tanto no enviarán alertas si se sobrepasan los umbrales predefinidos en referencia al monitor de ping si el propio firewall no sobrepasa dicho umbral.

En el momento en el que esto suceda se enviará al correo configurado en las alertas 1 correo notificando que el monitor de Ping esta inactivo.

Esto es una ventaja ya que, si el ping del firewall deja de estar activo, los demás dispositivos también dejarán de tener el monitor de ping activo, lo que se traduce en que WhatsUp Gold enviará un correo por cada uno de los dispositivos que hayan dejado de tener ping lo que, además de resultar molesto, masificaría el envío de correos y dificultaría la tarea de detección de problemas de los distintos servidores de WhatsUp Gold.

Aquí tenemos un ejemplo de correo de un servidor de la infraestructura de red de Parqueluz que no tiene dependencia generada y que por tanto envía correo al haber estado al menos 2 minutos sin ping:

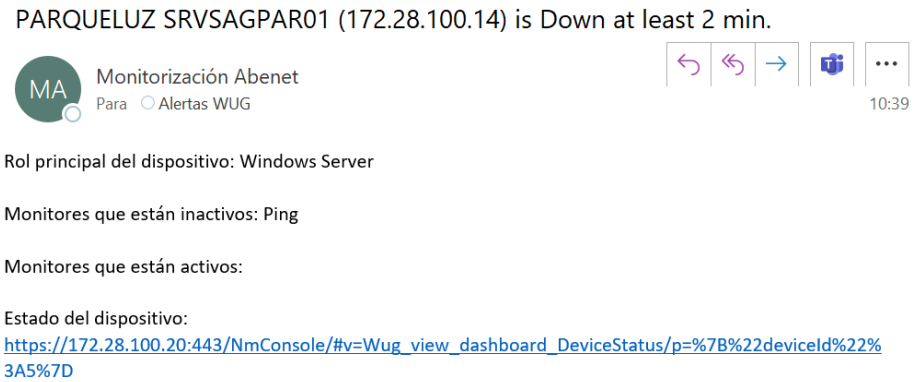

Ilustración 37: Notificación mediante correo de monitor inactivo en WhatsUp Gold

4.3.6 Implementación de políticas de acción en servidores para WhatsUp Gold

Es aquí cuando aparece en escena la importancia de las políticas de acción.

Estos parámetros configurables se pueden parametrizar en el menú de acciones y políticas accediendo al submenú de Políticas de acción.

Ahí podremos configurar las reglas de la política de acción que seguirán los monitores, umbrales y alertas cada uno de los servidores de WhatsUp Gold implementados.

Por decisión propia del departamento técnico de Abenet Soluciones, las reglas de política de acción que hemos utilizado en los distintos servidores de WhatsUp Gold que hemos implementado son las siguientes:

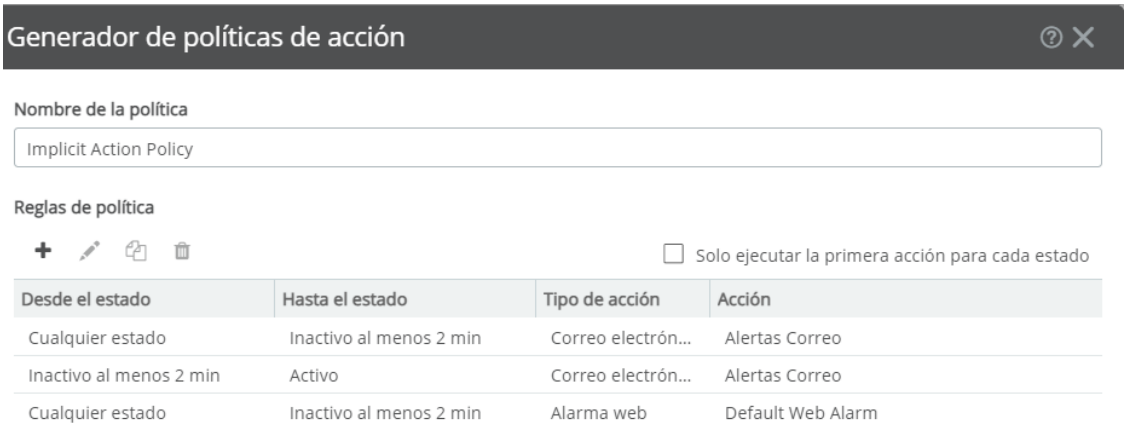

Ilustración 38: Generador de políticas de acción en WhatsUp Gold

Aquí podemos ver que:

1. En la primera acción se ejecutará como tipo de acción el correo electrónico mediante la acción de alertas de correo si los dispositivos del servidor de WhatsUp Gold sobre los que se aplica esta política de acción pasan de un estado inicial cualquiera a un estado final de ping inactivo al menos 2 minutos.
2. En la segunda acción se ejecutará como tipo de acción el correo electrónico mediante la acción de alertas de correo si los dispositivos del servidor de WhatsUp Gold sobre los que se aplica esta política de acción pasan de estar inactivos al menos 2 minutos a estar activos. Por tanto tendremos confirmación mediante mensaje de correo electrónico así tanto cuando queda inactivo el dispositivo como cuando vuelve a estar activo.

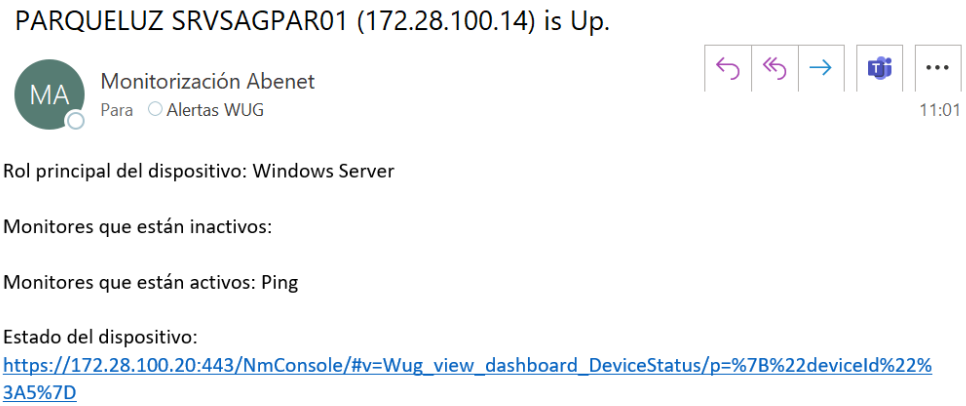

Ilustración 39: Notificación mediante correo de monitor inactivo en WhatsUp Gold

Aquí tenemos la notificación complementaria mediante mensaje de correo electrónico a la anterior mostrada en el punto 4.4.5 en la ilustración 37 donde vemos que recibimos una confirmación (debida a la implementación de la política de acción) de que el monitor de ping ha vuelto a estar activo en dicho servidor.

3. En la tercera acción se ejecutará como tipo de acción la alarma web (de la cual se puede cambiar el sonido por defecto que incorporan los servidores de WhatsUp Gold en caso de Alerta Web) mediante la acción de alarma web por configurada por defecto si los dispositivos del servidor de WhatsUp Gold sobre los que se aplica esta política de acción pasan de cualquier estado a estar inactivo al menos 2 minutos. Por tanto, si esto ocurre mientras nos encontramos en la versión web de WhatsUp Gold nos aparecerá en la parte superior derecha una alarma web notificándonos que dispositivo o dispositivos han quedado inactivos.

Ilustración 40: Alarma Web en WhatsUp Gold

5. Conclusiones y trabajo futuro

El objetivo principal de este TFG era implementar una serie de herramientas que nos permitan asegurar y monitorizar el estado de una red corporativa.

Tras la implementación del software podemos afirmar que se ha conseguido elevar en gran medida la seguridad de las redes corporativas en las que se han puesto en marcha las medidas de seguridad detalladas a lo largo de este trabajo.

Tanto la doble autenticación mediante inWebo como la monitorización mediante WhatsUp Gold han supuesto mejoras en cuanto al rendimiento y optimización de dichas redes corporativas elevando el nivel de seguridad de todos sus equipos y trabajadores y permitiendo anticiparse a problemas que puedan ocurrir.

También se ha conseguido una protección frente a ataques y fugas de información que puedan provocar personas que intenten comprometer la integridad y los intereses de dichas empresas.

Como trabajo futuro a realizar para cada una de las redes corporativas en las que se han implementado estas herramientas software destaco lo siguiente:

inWebo:

- Formación a los trabajadores para que sean capaces de detectar cuando tienen que registrar nuevas pantallas (cada vez que quieran registrar un navegador o aplicación nueva para cualquiera de los dispositivos implicados en la política de inWebo)
- Concienciación a los trabajadores de que el PIN que utilizan para acceder al portal de inWebo no puede estar guardado en sitios potencialmente vulnerables además de tener presente que no puede ser un patrón simple como 1111 o 1234 lo que no supondría un gran avance
- Formación a la hora de restablecer el PIN de acceso de cualquiera de los usuarios mediante el rol de Administrador.
- Concienciación de que este servicio tiene una licencia de tiempo finito, es decir, llegará el día en el que esta caduque y ninguno de los integrantes de la red corporativa podrá acceder al portal de inWebo lo que supondría una brecha de seguridad de nuevo. Por tanto se ha de saber cuando caduca dicha suscripción para poder renovarla con antelación y evitar problemas que revistan gravedad.

Keepass

- Formación completa de lo que supondría no seguir el protocolo de almacenamiento de archivos clave y las bases de datos lo que supondría que aunque todos los trabajadores de una empresa cumpliesen el guion a seguir y 1 no lo hiciese la brecha de seguridad sería la misma que si nadie hiciese nada ya que la base de datos de todos los usuarios quedaría expuesta igualmente.
- Concienciación del uso del generador automático de contraseñas a la hora de generar nuevas claves para cualquier servicio web o aplicación ya que no sirve de nada tener implementado este software si se siguen creando las mismas contraseñas o contraseñas con patrones semejantes porque si una de ellas queda expuesta, las otras también serán vulnerables.

WhatsUp Gold:

- Formación técnica profunda en cuanto al funcionamiento, la magnitud y potencia de esta herramienta a la hora de la monitorización de redes corporativas.
- Al igual que inWebo, tener presente que este servicio es de tiempo finito y por tanto llegará el día también en el que su suscripción caduque y por tanto no se pueda acceder al servidor Central de WhatsUp Gold y por tanto no se podrán monitorizar las redes corporativas desarrolladas. Por tanto se aconseja también anticipación para este software en cuanto a la caducidad de licencia del mismo.
- Es capital también el mantenimiento de los servidores ya que recientemente en Abenet hemos tenido un problema con algunos de los servidores de WhatsUp Gold implementados ya que debido a la última actualización acumulativa de Windows los servidores de WhatsUp Gold generaban problemas de acceso mediante errores internos que pocos días después solucionamos con la instalación en todos los servidores de la corrección que Windows sacó de dicha actualización. Por tanto es importante tener completamente actualizados los servidores de WhatsUp Gold para su correcto funcionamiento.

6. Bibliografía

https://www.inwebo.com/es/

https://www.myinwebo.com/console

https://aad.portal.azure.com/

https://www.myinwebo.com/welcome

https://www.capterra.es/software/172815/inwebo

https://docs.inwebo.com/

https://docs.inwebo.com/documentation/3331915779.html

https://docs.inwebo.com/documentation/Sophos-XG-SSL-VPN---inWebo-RADIUS-integration.3432841306.html

https://docs.inwebo.com/documentation/Microsoft-Azure-AD-connector.1536786455.html

https://portal.azure.com/

https://keepass.info/download.html

https://keepass.info/translations.html

https://www.youtube.com/watch?v=d3ooAPpS_i0&t=455s

https://www.youtube.com/watch?v=FHg-FNyv37Q

https://www.youtube.com/watch?v=rB-VqKJGHsg&t=1167s

https://www.youtube.com/watch?v=7Dg20hv7Vcg&t=818s

https://www.youtube.com/watch?v=cFUlJe4VXpg&t=879s

https://www.youtube.com/watch?v=XpkTNfQoVRE&t=241s

https://www.youtube.com/watch?v=4f2WS8n65l4&t=132s

https://www.whatsupgold.com/es

https://www.whatsupgold.com/es/monitoreo-de-aplicaciones

https://www.whatsupgold.com/es/testimonios

https://documentation.meraki.com/General_Administration/Monitoring_and_Reporting/SNMP_Overview_and_Configuration

http://oidref.com/1.3.6.1.4.1.6486.800.1.1.2.1

https://www.alcatelunleashed.com/viewtopic.php?t=26338

http://www.mibdepot.com/cgi-bin/vendor_index.cgi?r=alcatel

https://www.youtube.com/watch?v=mtt3-u4VdIA

https://www.youtube.com/watch?v=yfwl7xfsI_8

https://www.youtube.com/watch?v=hHr0ZwxMRZE