maristak
Durango Ikastetxea

IDEX

GRUPO 1

Eneko González,
Xabier Parra y
David Lobo.

Índice

Contenido

1. Introducción

Se ha solicitado un soporte para la implementación y la securizacion de la web que se desarrolló. La securización incluirá todo lo relativo a canales seguros y cifrados, así como la gestión y el control de los mecanismos de autenticación y autorización. Los datos de los cuales se van a tratar son delicados lo que conlleva que la securizacion debe de ser máxima para ello se implementará un SSO el cual utilizaremos para iniciar sesión en nuestra web.

Diseñar el modelo de Seguridad Perimetral para la empresa cliente y para ello se cuenta con un presupuesto de 25.000€.

Además del diseño, también se solicita:

1. Implantar una técnica de acceso remoto más segura y compleja para controlar el acceso desde fuera de la LAN.

2. Implantar un UTM en el que se configuren al menos dos zonas de seguridad y las reglas y políticas básicas.

2. Información Presupuesto

El cliente solicitó que se montara una red partiendo de un presupuesto de 25.000€, y que esta fuese lo más segura posible teniendo en cuenta una serie de factores, entre ellos uno era que en la red habría entre 600 y 700 equipos.
Al tratarse de un presupuesto quizás demasiado ajustado, se tuvieron que priorizar una serie de características por lo que se decidió implementar un firewall que aislará la red interna, permitiendo así filtrar el tráfico tanto entrante como saliente de la red del cliente.

Además del firewall se han utilizado dos router de la marca synology, 6 switches de capa 3, estos switches cuentan con espacios para discos duros para tener funciones de NAS, evitando así tener que invertir un dinero extra en un NAS dedicado.

Para aumentar la conectividad a la red, se han repartido por la empresa una serie de Access points, siendo estos un total de 5, que permitirá tener acceso a la red desde casi cualquier parte de la empresa.

Finalmente, los trabajadores tendrán acceso a los equipos, y en muchas ocasiones estos usuarios no tienen la educación necesaria como para hacer un uso seguro de los equipos por lo que se instalará un software de antivirus para evitar que tanto los equipos como la red estén expuestos al peligro.

Una de las recomendaciones por parte de DEX sería montar un servidor en la zona DMZ y en el configurar un sistema de honeypot, para así atraer a los atacantes a este servidor manteniendo seguros el resto de servidores que se encuentran en la red interna.

1. Objetivo

El objetivo ha sido la implementación y la securizacion del aplicativo que fue desarrollado anteriormente por nosotros. Dentro de este también se incluía la securizacion tanto de canales seguros y cifrados, así como la gestión y el control de los mecanismos de la autenticación y autorización.

Por otra parte, es necesario pensar en implementar un sistema de autenticación centralizada para gestión de identidades, integrado con todos los sistemas de la empresa que requieran hacer login para poder así utilizar el mecanismo Single Sign On (SSO) y gestionar la autorización conjunta de la siguiente manera: un Directorio Activo o LDAP mediante el cual se puedan identificar todos los sistemas. La solución por la que se opte deberá de estar securizada.

1.2. Objetivos de la seguridad perimetral informática

Los objetivos principales de la seguridad perimetral informática son:

– Soportar los ataques externos.
– Detectar e identificar los ataques recibidos y alertar acerca de ellos.
– Segmentar y securizar los sistemas y servicios en función de su superficie de ataque.
– Filtrar y bloquear el tráfico ilegítimo.

2. Modelo de seguridad perimetral

Plataformas de seguridad perimetral informática

Las 5 principales plataformas de seguridad perimetral informática son:

1.- Firewalls o cortafuegos

Son dispositivos a través de los cuales pasa el tráfico de la red y que aceptan o deniegan el tráfico en base a unas políticas o reglas de acceso. Pueden funcionar a distintos niveles, siendo los más extendidos:
– A nivel de red: permitiendo o denegando el tráfico en función de la IP de origen y de la IP de destino o a nivel de subredes (conjunto de IPs de origen y de IPs de destino).
– A nivel de aplicación: permitiendo o denegando el tráfico en función del protocolo utilizado en las comunicaciones (p. ej. DNS, NTP…).

2.- Sistemas de detección y/o prevención de intrusión (IDS/IPS)

Inspeccionan el tráfico de red en base a firmas de ataques conocidos o en base a comportamientos/patrones de tráfico anómalos para la detección y/o prevención de intrusiones.

3.- Honeypots

Son plataformas para la simulación de sistemas que intentan atraer los ataques para poder analizarlos, mejorar con esta información la seguridad de la organización y también evitar que se produzcan a los sistemas críticos de las organizaciones.

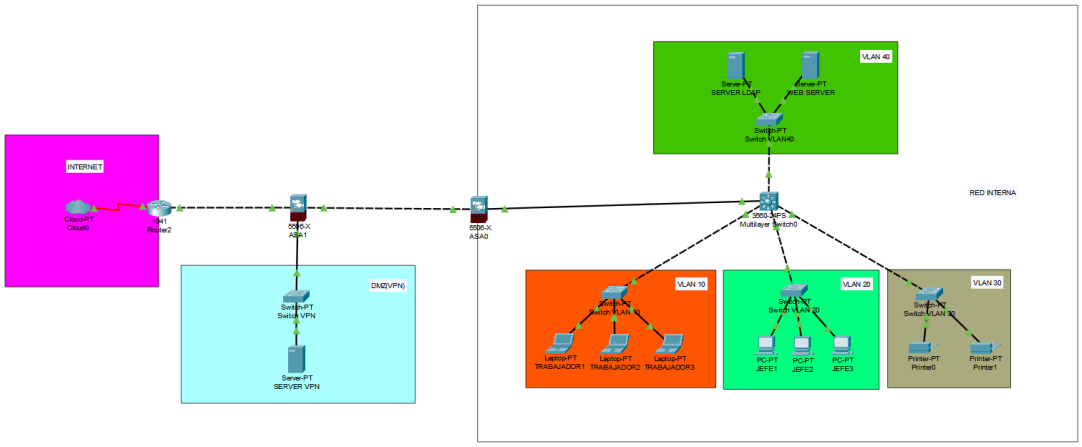
4.- Sistemas anti-DDoS

Sistemas que previenen o mitigan los ataques de denegación de servicio (DoS) o los ataques distribuidos de denegación de servicio (DDoS). Generalmente este tipo de sistemas necesitan un tiempo de aprendizaje para modelar cuál es el comportamiento normal o las tendencias en el tráfico de la red, estableciendo unas líneas base de los distintos volúmenes de tipos de tráfico… para que una vez se pongan en modo bloqueo, cuando se produzca un ataque y se detecten desviaciones de las líneas base, sean capaces de bloquear o mitigar dichos ataques evitando que el tráfico anómalo ingrese a la red.

5.- Pasarelas antivirus y antispam

Inspeccionan el correo electrónico de los servidores para filtrar aquellos que tienen contenido malicioso y evitar que entren a la red y lleguen a los destinatarios.
Los mecanismos de seguridad perimetral de red son elementos básicos de seguridad que mitigan el riesgo de sufrir incidentes de seguridad debidos a ataques DoS/DDoS, accesos no autorizados, infecciones por malware, etc. Cualquier organización debería implementar aquellos necesarios para mitigar el nivel de riesgo al que está expuesta su red y los sistemas que la forman.

Modelo



1.- Firewalls o cortafuegos:

Se ha decidido instalar dos firewalls, uno interno para filtrar cualquier tipo de paquete, la prevención de intrusiones, la monitorización de la capa de aplicaciones o la protección de malware todavía funcionen y otro externo para protegernos de cualquier ataque del exterior.

2.- Sistemas de detección y/o prevención de intrusión (IDS/IPS):

Se ha decidido instalar un sistema IDS que detectar accesos no autorizados a un ordenador o a una red, es decir, son sistemas que monitorizan el tráfico entrante y lo cotejan con una base de datos actualizada de firmas de ataque conocidas, también se ha implementado un IPS para proteger a los sistemas de ataques e intrusiones. Su actuación es preventiva. Estos sistemas llevan a cabo un análisis en tiempo real de las conexiones y los protocolos para determinar si se está produciendo o se va a producir un incidente, identificando ataques según patrones, anomalías o comportamientos sospechosos y permitiendo el control de acceso a la red, implementando políticas que se basan en el contenido del tráfico monitorizado, es decir, el IPS además de lanzar alarmas, puede descartar paquetes y desconectar conexiones.

Todo esto estará integrado en los firewalls así reduciremos la carga de dispositivos tanto por el número de dispositivos como por la parte económica.

3.- Honeypots:

Sería recomendable para aumentar la seguridad de la red, la instalación de un servidor que funcionara como honeypot intentando atraer a los atacantes para que así los ataque no fueran dirigidos a la red de la empresa. Este servidor estará situado en el área de la DMZ para así estar lo más aislado posible sin que esto suponga ningún peligro para la red interna.

4.- Sistemas anti-DDoS

Basándonos en la actualidad se ha implementado en el firewall una característica para evitar ataque DDOS ya que se está popularizando y eso conlleva tener la empresa parada durante horas o días ya que nos lanzarían peticiones hasta que nuestro firewall no pueda dar a basto y conseguirían ralentizar la red y en el peor de los casos tirarnos la.

5.- Pasarelas antivirus y antispam:

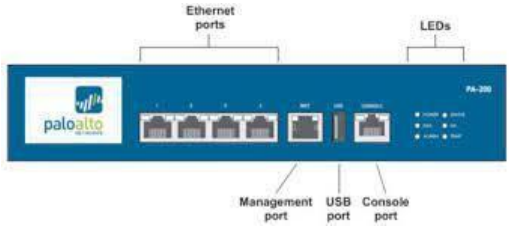
Al tratarse de equipos que están a disposición de usuarios que podrían no tener conocimientos avanzados de las prevenciones que deben tomar, se ha decidido implementar un servicio de antivirus que trate de disminuir al mínimo la posibilidad de que los equipos se vean infectados por la ejecución de algún archivo con código malicioso o un USB infectado, por ejemplo. Para ello se ha contratado ESET con la versión total security.

3. Firewall

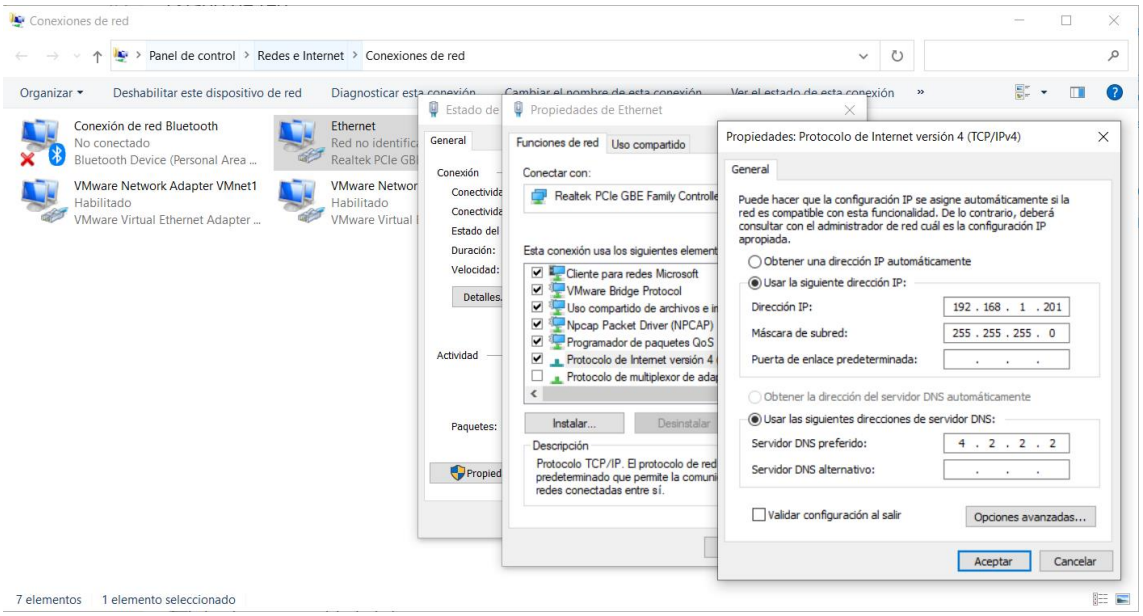
Configuración Firewall

Puesta en marcha

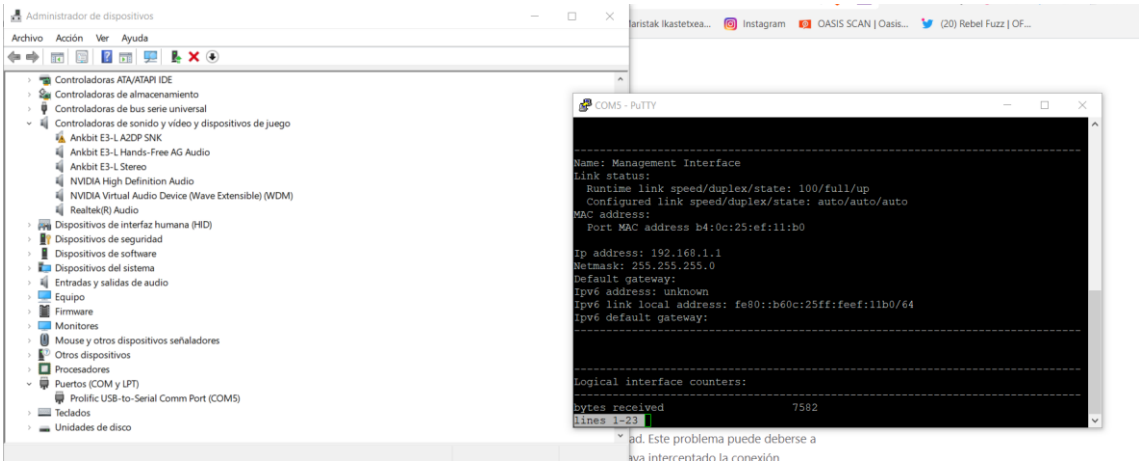
Lo primero que haremos será conectarnos al managment para ello necesitaremos un cable rj45 que conectaremos al puerto managment.



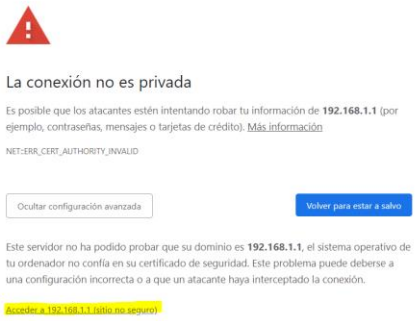
Después iremos a configurar la ip y nos pondremos en el rango del firewall, por defecto está en la 192.168.1.0/24.



Para comprobar en que ip esta nuestro firewall lo primero que haremos será acceder al administrador de dispositivos desplegaremos el apartado puertos y en este caso vemos que es el COM5, abriremos el PUTTY y lo configuraremos en el COM5, una vez conectados iniciaremos sesión y escribiremos el comando show interface managment, ya podremos apreciar la ip que se encuentra.



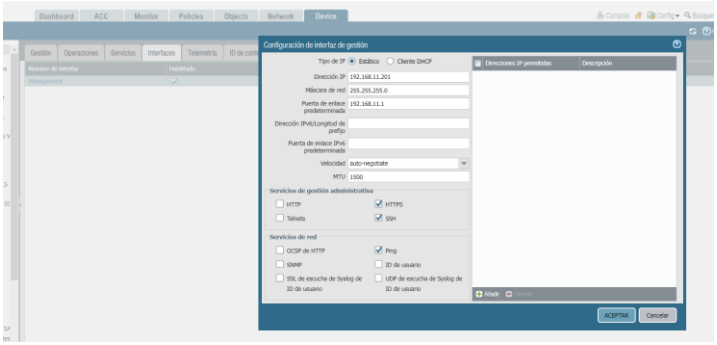
Ahora escribiremos esa ip en la barra de nuestro navegador siempre con https://



Iniciamos y ya tendriamos la configuracion básica.

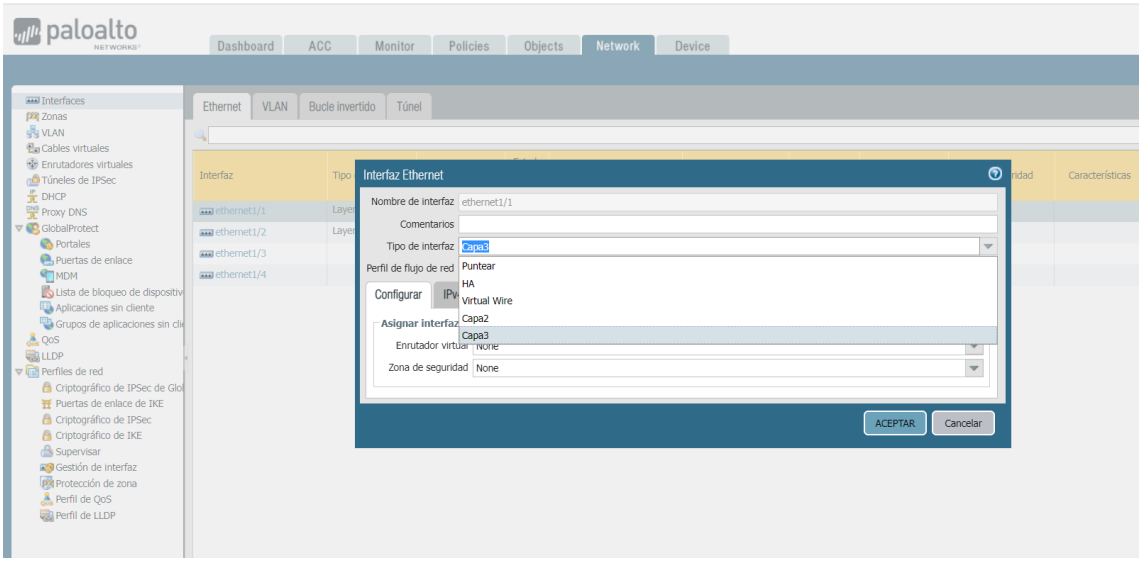
Cambiar ip por defecto

Iremos a device y clicaremos en la interfaz managment y lo configuraremos tal que así compilaremos cambiaremos la red para volvernos a conectar.

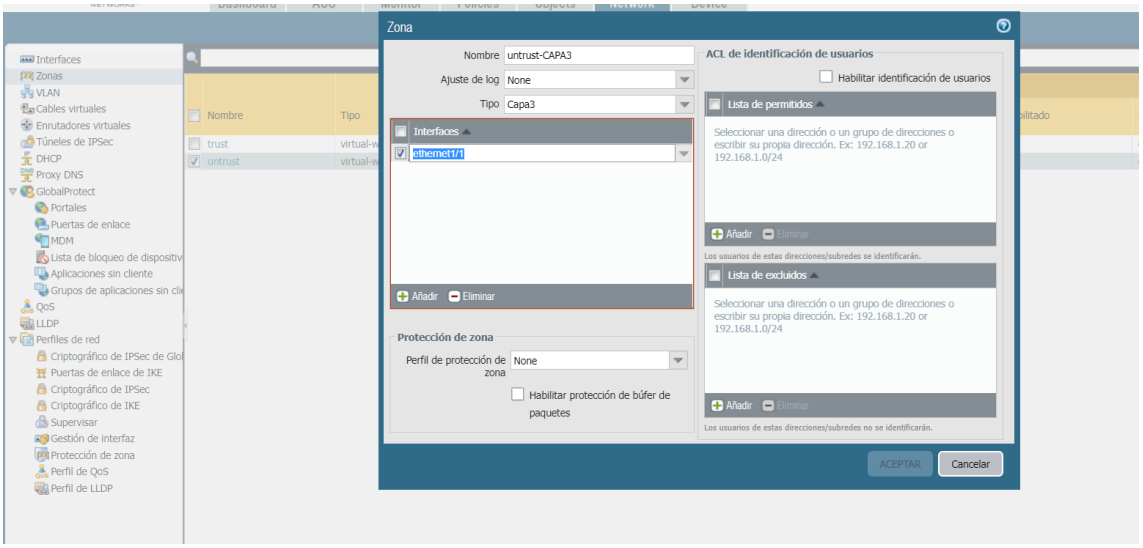


Configuración de Puertos+VLAN

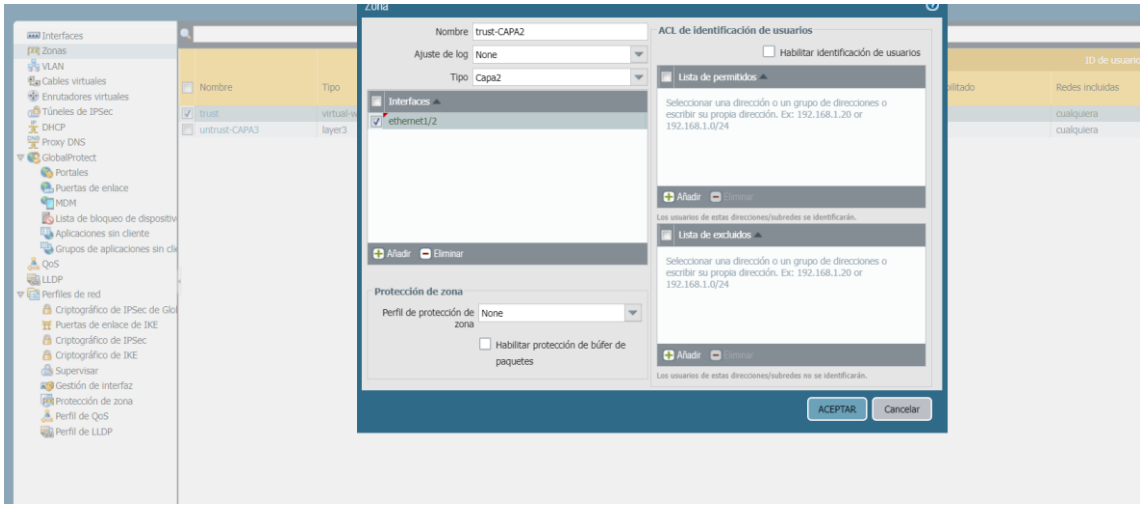
Lo primero que haremos será editar la configuración del puerto ethernet el cual va a salir hacia internet como va a salir hacia internet lo pondremos capa 3, también podemos aprovechar y poner el puerto que va a ir al switch capa 2.



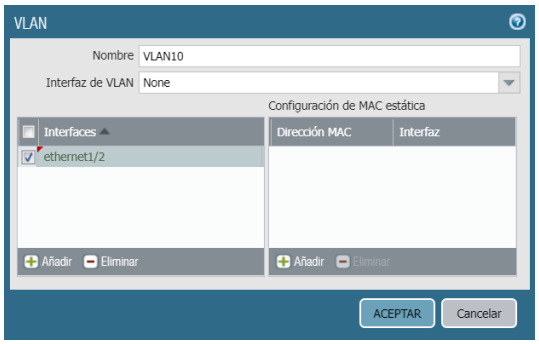
Ahora iremos a zonas y modificaremos la untrast y la configuraremos tal que así.



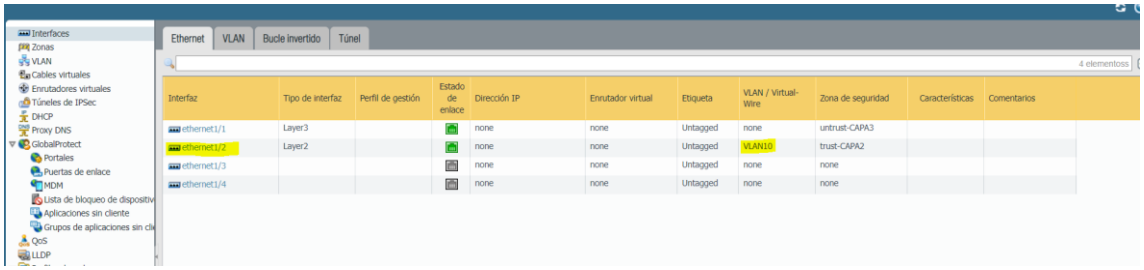
Haremos lo mismo con el trust, con su configuración particular claro, también crearemos un trust de capa3 para la vlan.



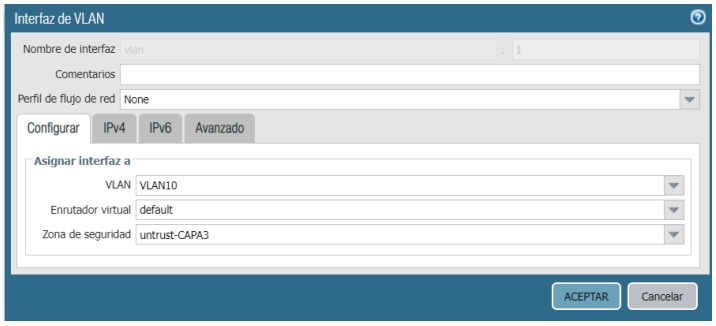
Ahora vamos a crear la VLAN para la LAN.



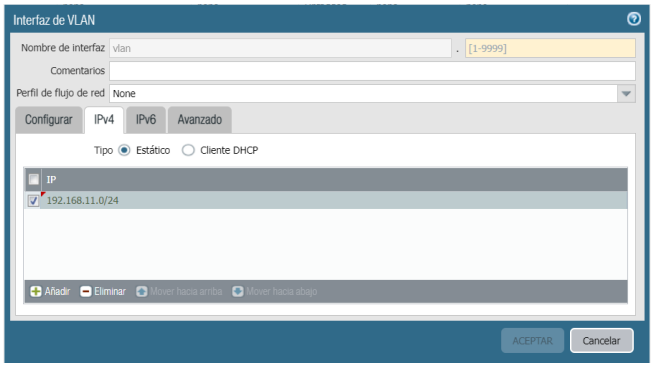
Se nos asignara automáticamente a nuestra interfaz.



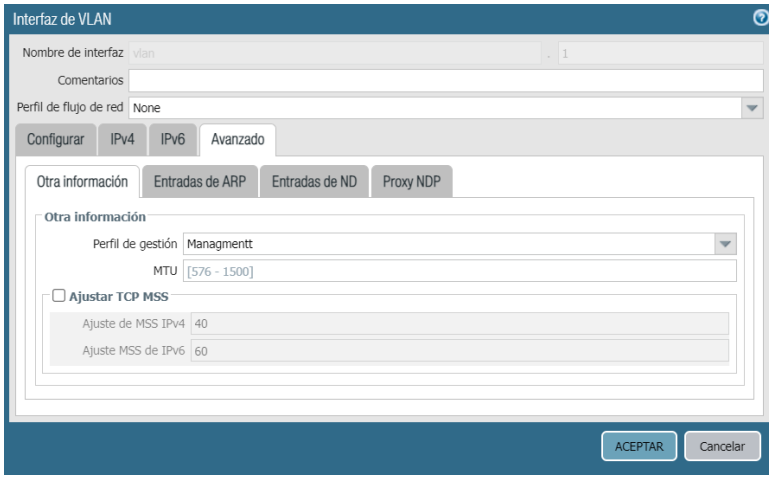
Vamos a crear un perfil de gestión el cual llamaremos managment y le daremos los permisos que aparecen.
Para que el managment tenga salida a internet tenemos que hacer una configuración iremos a Vlan en interfaces y crearemos una, asignándola a la Vlan 10, con el enrutador virtual por defecto y la zona de seguridad untras-CAPA3.



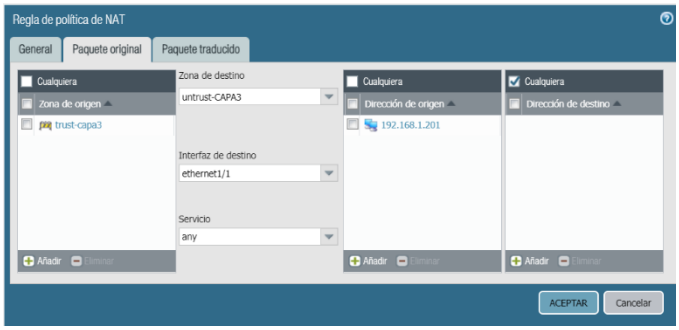
Iremos a ipv4 y asignaremos un rango



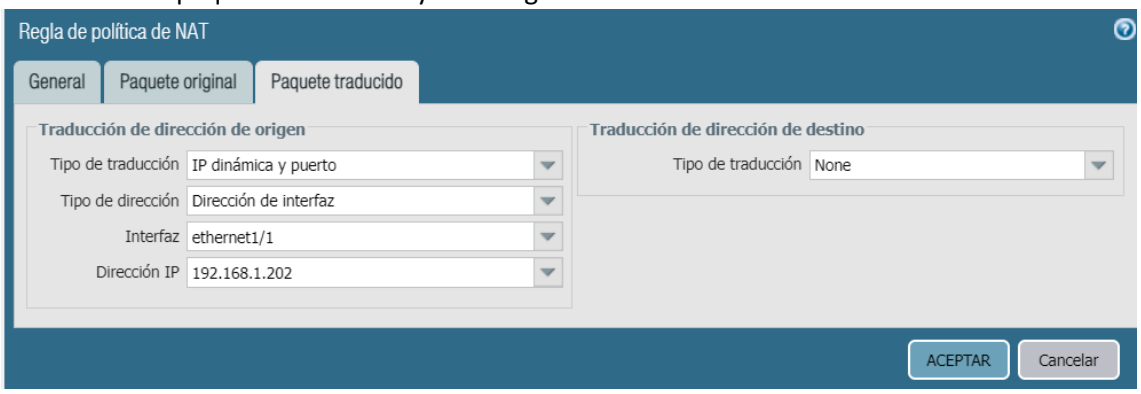
Después clicaremos en avanzado y escogeremos el perfil de gestión



Clicaremos en opciones y configuraremos la puerta de enlace la máscara de subred y el DNS
Por último vamos a configurar la salida hacia internet para ello iremos a polices y clicaremos en NAT, añadiremos una con esta configuración.

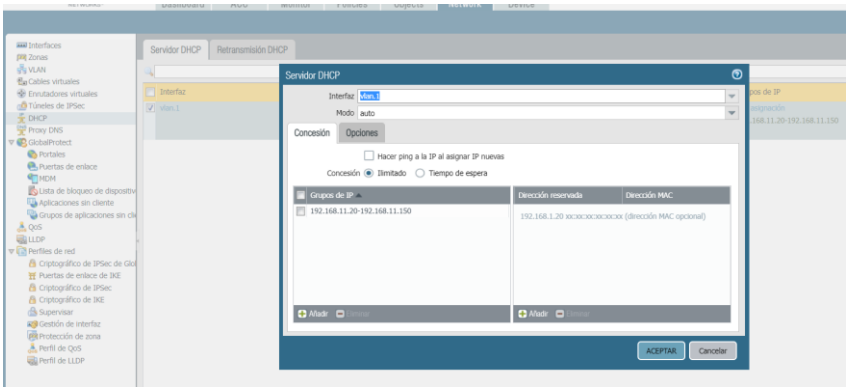


Clicaremos en paquete traducción y lo configuraremos.

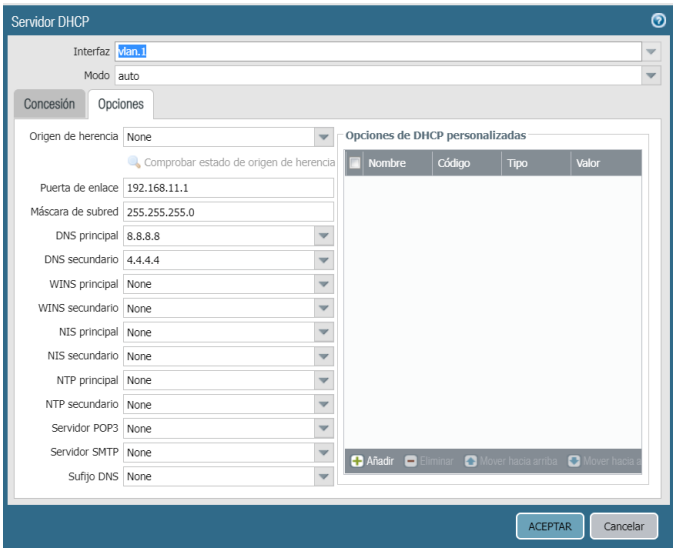


Configuración DHCP

Iremos a la pestaña DHCP y añadiremos uno nuevo y pondremos un rango direccionable.

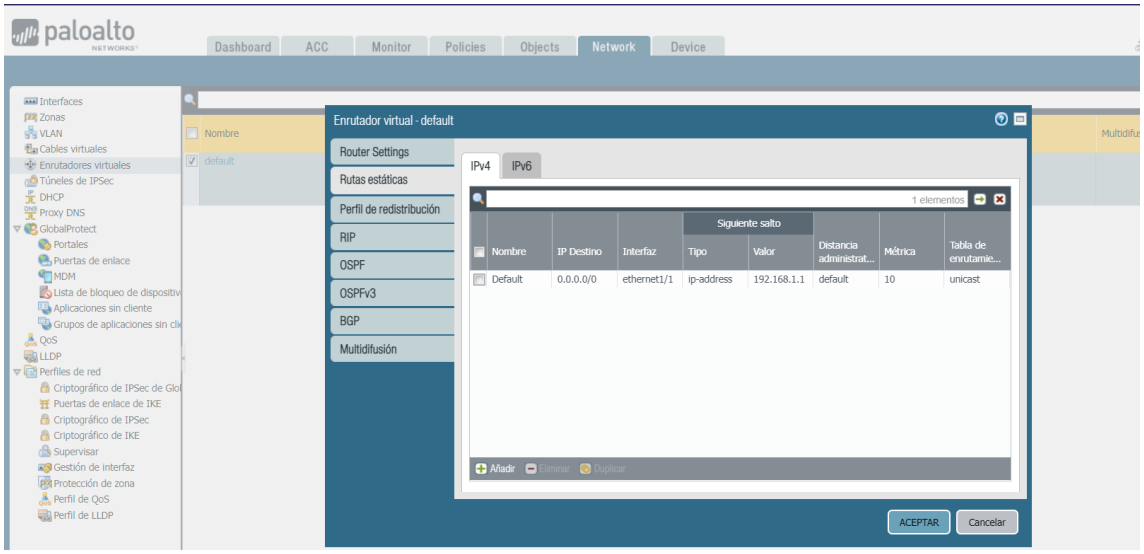


Después le daremos a opciones y lo configuraremos así.



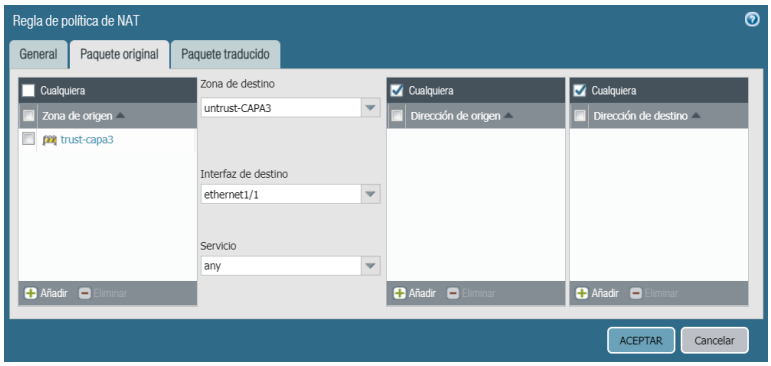
Enrutador Virtual

Iremos a network enrutador virtual y lo configuraremos de esta manera para que de acceso a cualquier petición.

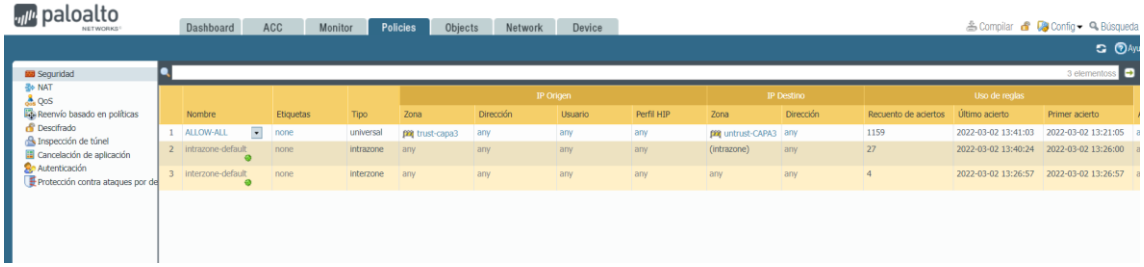


NAT

Vamos a pólices y configuramos en NAT esto.



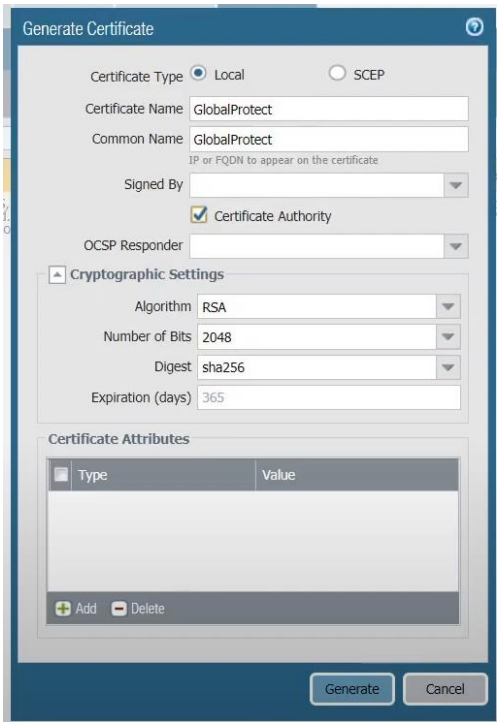
De momento configuraremos una acl para permitir todo.



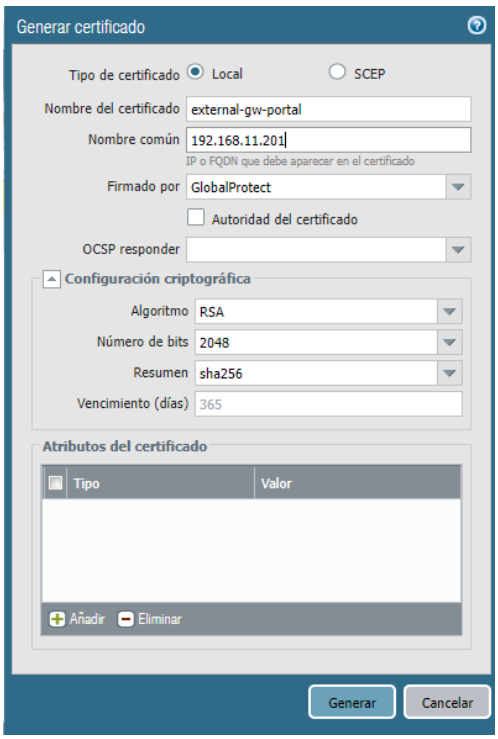
4. VPN

Configuración de la VPN.

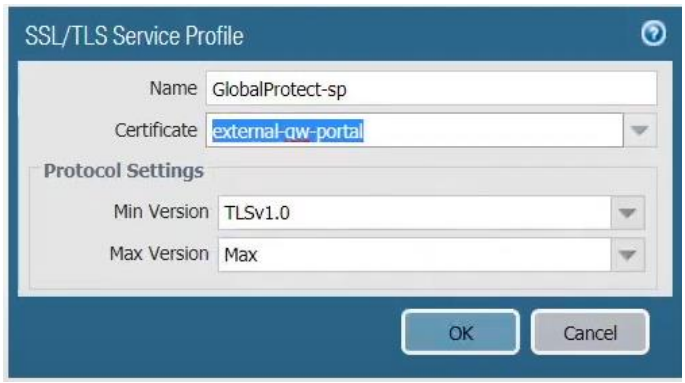
Para que los usuarios puedan trabajar de forma remota y que puedan acceder a la red cuando no están en la oficina para descargar documentos del NAS, por ejemplo.
Se ha pedido que se configure una VPN, en este caso lo que se ha hecho ha sido configurar el servicio que viene incluido con el propio firewall, de esta manera, se ha podido abaratar el costo de todo el presupuesto sacrificando en parte el rendimiento que ofrecería la VPN si hubiéramos dedicado un servidor para ello.
Dejando de lado lo anteriormente mencionado, se procederá a explicar las configuraciones que se han llevado a cabo para poder poner este servicio en funcionamiento.
Primero de todo habrá que establecer los certificados con los que la VPN funcionará, para ello, en el apartado de dispositivos, hay que entrar en el subapartado de certificados y ahí se añadirá uno nuevo, para ello, seleccionaremos que se tratará de un certificado de tipo local y este se creará con la configuración por defecto.



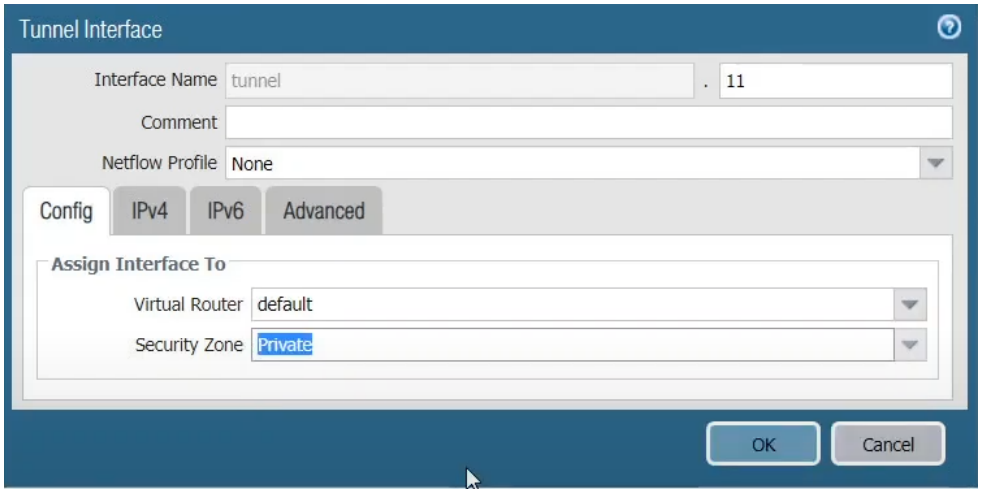
Una vez creado el certificado principal, crearemos el certificado para la puerta de enlace en el cual habrá que establecer como nombre común la IP de la puerta de enlace que se ha establecido anteriormente y que a su misma estará firmado por el certificado principal que se ha creado anteriormente.



A continuación, se procederá a configurar el servicio SSL/TSL, para ello en el mismo apartado que en el paso anterior, pero en este caso en el subapartado correspondiente se procederá a ello.
Para ello habrá que añadir un nuevo perfil del servicio en el cual se dará un nombre y elegirá un certificado que validará dicho servicio.



Uno de los pasos más importantes a la hora de configurar un servicio de VPN es la parte de los túneles, los cuales serán los encargados de permitir el acceso a la red desde “fuera”.
En este caso, en el apartado de Network se encontrará el subapartado de Tunnel que será en el que se va a llevar a cabo esta configuración.
Lo que habrá que hacer aquí será añadir un túnel nuevo al cual se le dará un nombre, un número que ira del 1-999 y se le asignará una IP.
Como router virtual se pondrá el default y la zona de seguridad será la privada en este caso.

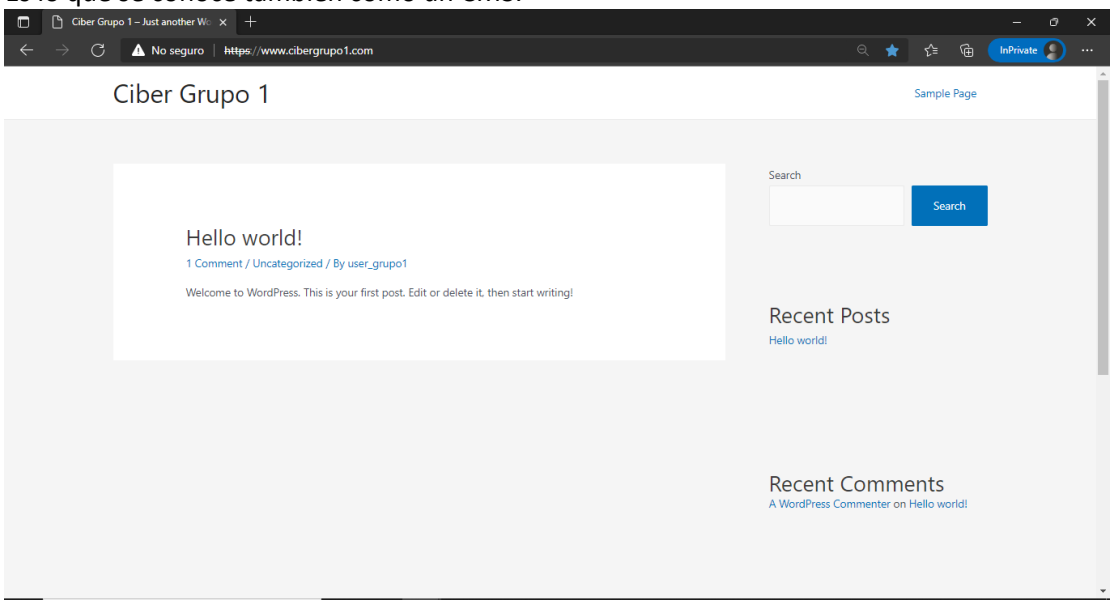


Finalmente, habrá que establecer una IP para que el host interno lo detecte, esto se hará desde el apartado de Network.
Además de ello se establecerá una puerta de enlace externa en forma de IP, y la región que estableceremos por defecto será Any permitiendo así que trabajadores que estén fuera de España puedan conectarse.
Una vez configurado todo lo anterior habrá que descargar los certificados en el ordenador cliente para que el cliente VPN funcione correctamente y una vez realizados todos los pasos anteriores, desde el portal de GlobalProtect se podrán descargar los agentes que harán que se pueda activar y desactivar la VPN.

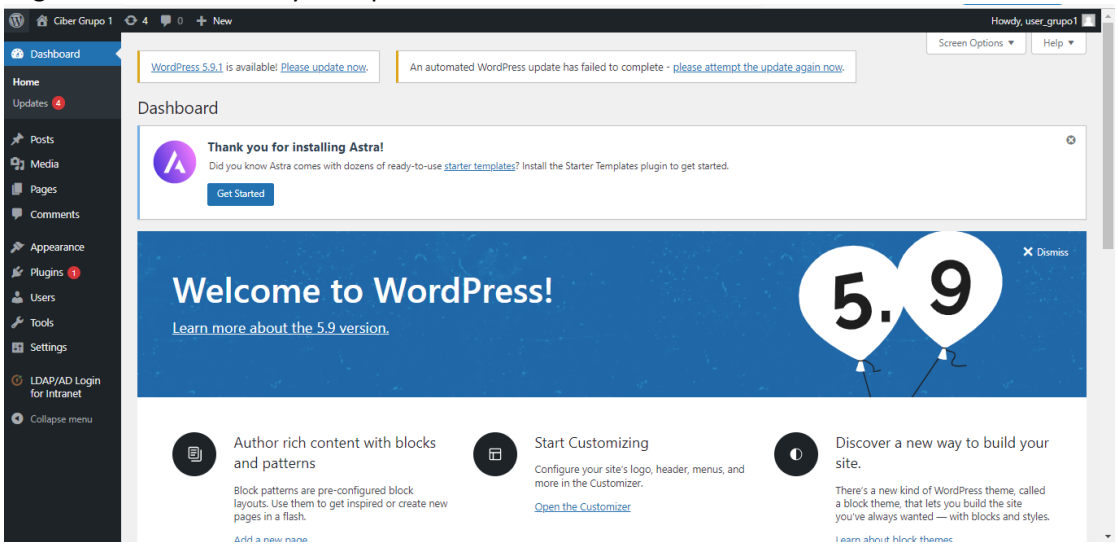
5. Servicios implementados

5.1. WordPress

Dicho de manera sencilla, WordPress es una aplicación, un programa, o como lo quieras llamar, que sirve para crear sitios web y publicar contenidos en estos sitios web.
Es lo que se conoce también como un CMS.



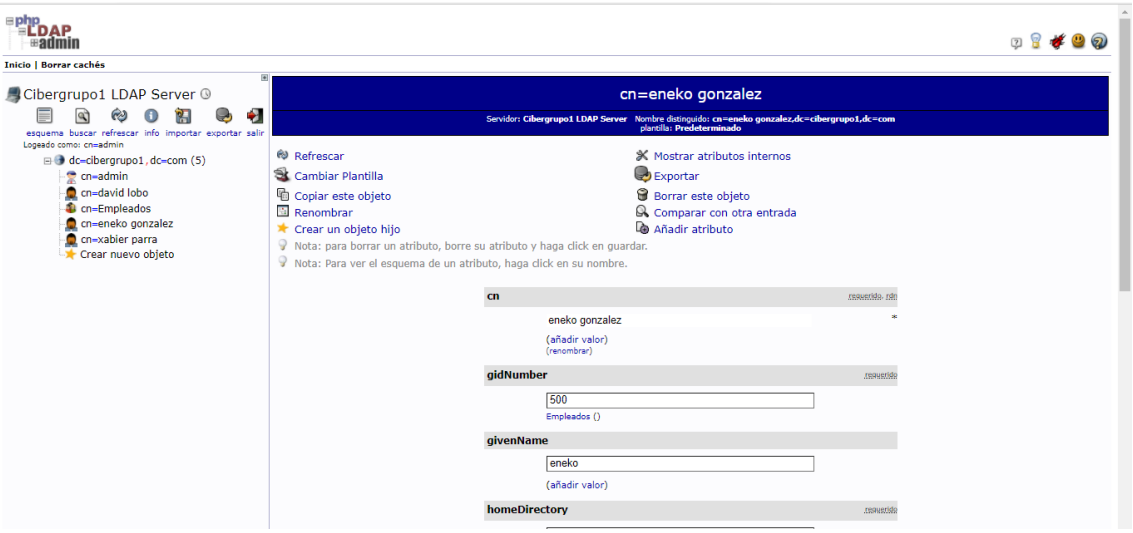
El gestor de contenidos y sus opciones.



5.2. LDAP

LDAP proporciona una forma de gestionar los usuarios y las pertenencias a grupos almacenados en Active Directory. LDAP es un protocolo que autentica y autoriza el acceso granular a los recursos de TI, y Active Directory es una base de datos de información de usuarios y grupos.

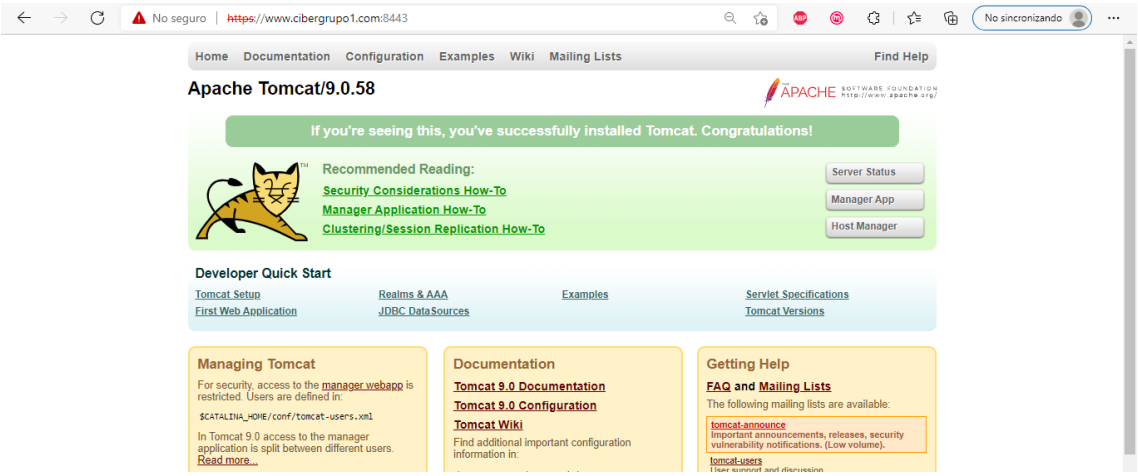
Una vez dentro te permite gestionar los usuarios y los grupos.



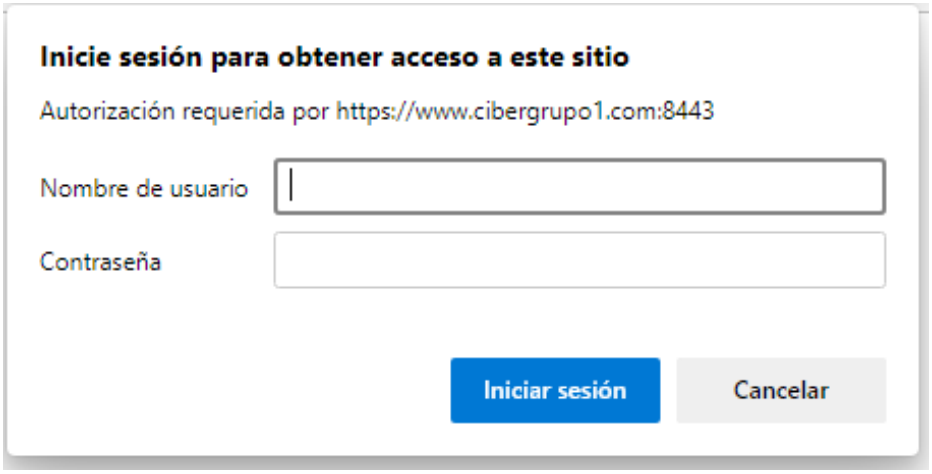
5.3. TOMCAT

Apache Tomcat (o, sencillamente, Tomcat) es un contenedor de servlets que se puede usar para compilar y ejecutar aplicaciones web realizadas en Java. Implementa y da soporte tanto a servlets como a páginas JSP (Java Server Pages) o Java Sockets.

Su página principal.



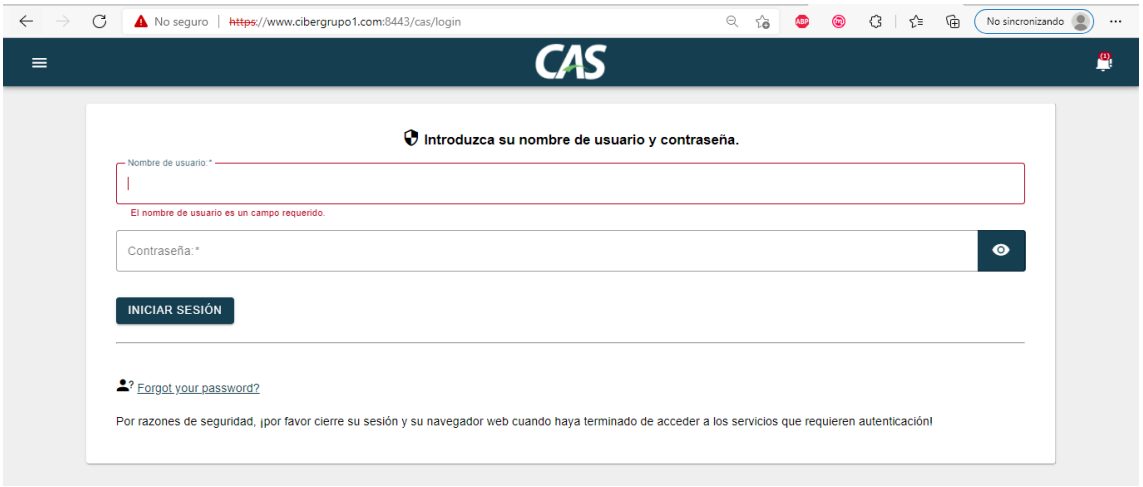
Cada página requiere de un login.



5.4. CAS

CAS (Central Authentication Service) es un protocolo mantenido actualmente por la Apereo Foundation. Se trata de un protocolo sencillo y bien documentado, para el que se encuentra gran cantidad de software publicado.

El Servicio de autenticación central es un protocolo de inicio de sesión único para la web. Su propósito es permitir que un usuario acceda a múltiples aplicaciones mientras proporciona sus credenciales solo una vez.



6. Instalación de los servicios

INSTALACION
SISTEMAS RETO 3.p

7. Conclusión

Uno de los factores a tener en cuenta a la hora de la valoración general del trabajo realizado por parte de DEX para la empresa Maristak, ha sido los problemas que han ido surgiendo a la hora de instalar varios servicios que han sido los causantes de que no hayamos conseguido satisfacer por completo los requerimientos del cliente.
En este caso, la parte del Single Sign On (SSO) no se ha podido finalizar la instalación, por lo que esta parte no estaría implementada por ahora, y se implementaría en un futuro si el cliente así lo desea.
Por otra parte, el resto de objetivos han sido cumplidos satisfactoriamente.