WARRIORS PORTAL

CAUTIVO

Warriors®

"Security that makes difference"

PORTAL CAUTIVO

Es una solución de seguridad que permite el control y administración de usuarios a las redes públicas y privadas. Esta solución se utiliza habitualmente para la gestión de del acceso de invitados en redes wifi abiertas que se encuentran en hoteles, hospitales, aeropuertos, restaurantes u oficinas corporativas. El acceso a Internet es restringido hasta que el usuario proporcione alguno de los métodos de accesos, como: correo electrónico, usuario - password, voucher o algún formulario que registre la información del usuario.

+ RED DE INVITADOS

+ ACCESO WI-FI PARA CLIENTES

+ DISPOSITIVOS NO CORPORATIVOS – BYOD (BRING YOUR OWN DEVICE)

PERSONALICE SU PÁGINA DE ACCESO

WDNG le ofrece un gestor de plantillas con lo cual podrá configurar su propia página de acceso. Al mismo tiempo ofrece funcionalidades adicionales como:

Redirección de URL
Página de inicio de sesión personalizada

ADMINISTRADOR DE ZONAS

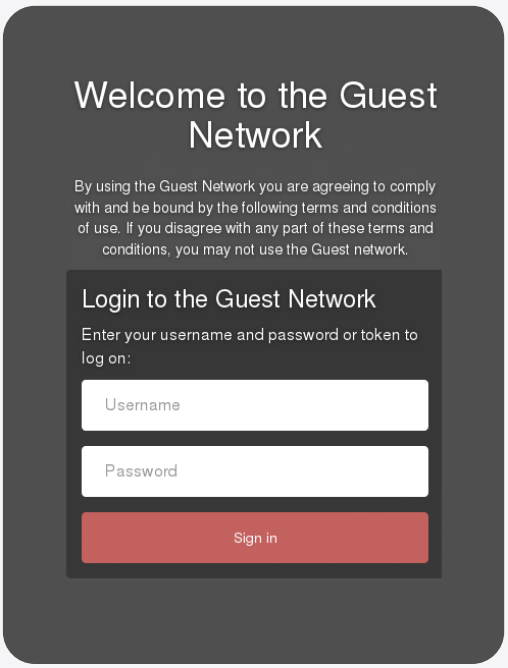
Se pueden configurar diferentes zonas en cada interfaz o varias interfaces pueden compartir una configuración de zona. Cada zona puede utilizar una plantilla de portal cautivo diferente o compartirla con otra zona.

ADMINISTRACIÓN MEDIANTE TICKETS

El Portal Cautivo cuenta con un sistema de creación de tickets que exporta los tickets a un archivo csv para utilizarlo con su aplicación favorita. La exportación le permite imprimir los comprobantes crear un folleto de buen aspecto con su logotipo y estilo de empresa

AUTENTICACIÓN

Autenticación segura a través de HTTPS o portal de sólo splash con redirección de URL a una página determinada se pueden utilizar diferentes fuentes para autenticar a un usuario en una zona:



- *LDAP [Active Directory]*
- *Radius*
- *Gestor de usuarios local*
- *Vauchers / Tickets*
- *Contraseña de un solo factor (2FA)*
- *Sin autenticación (sólo pantalla de inicio)*
- *Múltiple (una combinación de lo anterior)*

ADMINISTRACIÓN DE ANCHO DE BANDA

El optimizador de tráfico de red puede ser utilizado para:

+ *Balancear el ancho de banda y evitar un uso excesivo*
+ *Dar prioridad a protocolos o a hosts en específico*

PORTAL BYPASS

Direcciones MAC o direcciones IP puedes ser colocadas en listas blancas para realizar un bypass al portal cautivo

PERIODOS DE TIEMPO

La conexión puede terminar después de que el usuario haya estado inactivo durante un cierto tiempo (tiempo de espera inactivo) y/o forzar una desconexión cuando haya pasado un número de minutos, aunque el usuario siga activo la sesión (tiempo límite).

En caso de que un usuario se vuelva a conectar dentro del tiempo de espera y/o del tiempo de inactividad, no es necesario iniciar sesión y el usuario puede reanudar su sesión activa.

+ Redireccionamiento a página WEB definida por el cliente

+ Uso de diferentes motores de autenticación externos: Radius,

MySQL, LDAP

+ Excepciones MAC, IP, Dominio

+ Administración vía Web

KEY FEATURES

Tipos de autenticación
LDAP [Active Directory]
Radius
MySQL
Gestor de usuarios local
Vauchers / Tickets
Contraseña de un solo factor (2FA)
Sin autenticación (sólo pantalla de inicio)
Múltiple (una combinación de lo anterior)

TRAFFIC SHAPING

Limitador de tráfico
Priorización de Aplicaciones
Control de Consumo de ancho de banda

CONTROL ACCESO

Control de acceso por horario
ACL – Dispositivos permitidos
Conexiones concurrentes


Warriors®
"Security that makes difference"