

Diseño de red y publicación de servicio web a Internet sin una IP homologada

Información del reporte:

Licencia Creative Commons



El contenido de los textos es responsabilidad de los autores y no refleja forzosamente el punto de vista de los dictaminadores, o de los miembros del Comité Editorial, o la postura del editor y la editorial de la publicación.

Para citar este reporte técnico:

Villarreal Brito, G. (2024). Diseño de red y publicación de servicio web a Internet sin una IP homologada. *Cuadernos Técnicos Universitarios de la DGTIC*, 2 (1), páginas (83 - 101).

<https://doi.org/10.22201/dgtic.ctud.2024.2.1.33>

Gustavo Villarreal Brito

Instituto de Ciencias del Mar y Limnología
Universidad Nacional Autónoma de México

gwillarreal@cmarl.unam.mx

ORCID: 0009-0006-9119-1122

Resumen

Se describe el análisis e implementación de una alternativa de solución que dio como resultado el diseño e implementación de una red que por medio de un enlace satelital sin IP fija y homologada se construye un túnel de VPN y NAT entre la Isla Contoy y la Unidad Académica de Sistemas Arrecifales de Puerto Morelos (UASA), logrando la conectividad para publicar un servicio web a Internet, y realizar tareas de administración remotamente, esto para el estudio de corrientes del lazo del canal de Yucatán. Esta implementación fue realizada en una isla sin energía eléctrica, infraestructura y presupuesto.

Palabras clave:

Enlace VPN, traducción de direcciones de red, redes, soluciones de TIC.

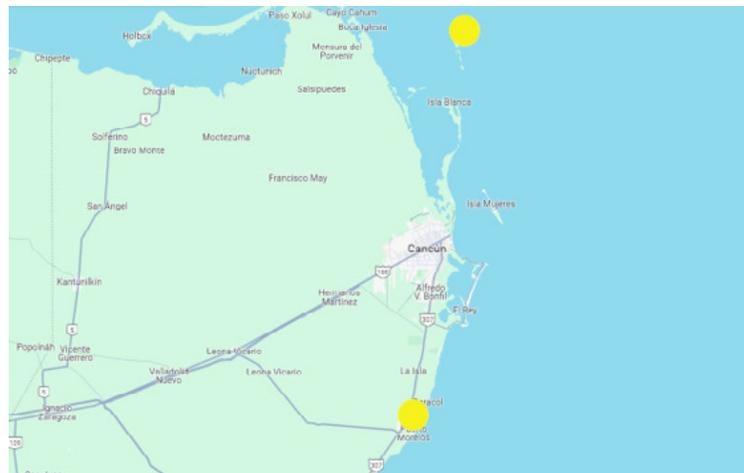
1. INTRODUCCIÓN

El Internet y el diseño de redes con el uso de redes privadas virtuales (VPN) y Traducción de direcciones de red (NAT), ha crecido en las últimas décadas, permitiendo dar soluciones para el intercambio de datos a distancia, conectando múltiples dispositivos en una red local con una sola dirección IP homologada¹. Estos diseños son útiles para limitar el uso de direcciones IP homologas, que son un recurso finito o por factibilidades técnicas donde no existe la posibilidad de tener una IP homologada fija.

El área de cómputo de la Unidad Académica de Sistemas Arrecifales del Instituto de Ciencias del Mar y Limnología de la UNAM colaboró con la implementación de una solución de redes para el intercambio de datos a distancia donde los interesados en el estudio de las corrientes del lazo en el canal de Yucatán pueden acceder desde cualquier parte del mundo.

Figura 1

Península de Yucatán



Nota. En el mapa se observan dos puntos amarillos que están ubicados en las coordenadas, 21.508712327889267, -86.81119818610304 referente a Isla Contoy y 20.86850736911935, -86.8675754220543 referente a la Unidad Académica de Sistemas Arrecifales con una distancia en línea recta de aproximadamente de 60 km

2. OBJETIVO

Se requiere publicar el servicio web² propio de la tecnología CODAR Ocean Sensor (CODAR Ocean Sensor, 2023) que se muestra en la figura 2, este servicio está almacenado en un equipo MAC mini que está físicamente en la Isla Contoy con una red privada; las características técnicas de este equipo de cómputo están descritas en el Anexo A. La solución debe ser basada en tecnología libre y con los recursos

1 Es la dirección IP pública asignada a un dispositivo de red por un proveedor de servicios de Internet, de acuerdo con el plan de asignación de direcciones IP (Instituto Federal de Telecomunicaciones, 2022).

2 Un servicio web es una aplicación que se puede acceder y utilizar a través de una red, como Internet. Los servicios web se utilizan para intercambiar datos y realizar tareas entre aplicaciones (Wikipedia, 2023).

económicos, tecnológicos y humanos existentes, se debe permitir la administración remota del servidor web y ver la página desde Internet.

Figura 2

Servicio web publicado en la ip 132.248.121.7:8240 con datos de las corrientes del lazo en el canal de Yucatán



Nota: Fuente: Salas de León D.A., Knap A.H., Glenn S., Monreal Jiménez R., Contreras Tereza V.K., Dimarco S.F., Dancer A.V., Escalante Mancera E., Gómez Realí M.A. (2023) Estudio de la Corriente de Lazo en el Canal de Yucatán mediante radares de alta frecuencia. Proyecto UNAM-TAMU iniciado en 2019, duración: por tiempo indefinido. Instituto de Ciencias del Mar y Limnología, Universidad Nacional Autónoma de México, Cd Mx – Puerto Morelos, Recuperado el 30 de noviembre de 2022 con autorización de los responsables

3. DESARROLLO TÉCNICO

3.1 METODOLOGÍA

Para dar una alternativa de solución en la publicación de servicios web a Internet sin una IP homologada fija se contemplan 3 puntos importantes.

- Definición del objetivo con los involucrados.
- Estudio de mercado.
- Definición de alternativas.

3.2 ANÁLISIS

Para la etapa de análisis, un punto importante fue visitar la Isla de Contoy, para obtener información de redes, infraestructura eléctrica y tecnológica, entre otros aspectos importantes.

Dentro del análisis de la Isla Contoy en el ámbito de tecnologías, se obtuvieron las siguientes premisas: cuenta con una antena satelital para el servicio de Internet; para mayor detalle de los datos de la red se puede consultar el Anexo B. Otro aspecto importante de la isla es que carece de una red de energía eléctrica y que sólo cuenta con 4 paneles solares con una capacidad de 200 a 250 watts³. El panorama se complementa con la presencia de un equipo Mac mini, personalizado y configurado para gestionar y operar antenas de alta frecuencia; por último, es esencial destacar la limitación de recursos económicos. Referente a la Unidad Académica, cuenta con un cuarto de telecomunicaciones y un servidor físico con software VMware para virtualizar sistemas operativos, los detalles técnicos del servidor se pueden observar en el Anexo C; la Unidad Académica cuenta con un enlace dedicado de 150 Mbps. Estas premisas resultan fundamentales para comprender el contexto y definir el diseño de la red e implementación de la solución.

3.3 ALTERNATIVAS DE SOLUCIÓN

De acuerdo con las premisas, requerimientos y el cumplimiento del objetivo de tener conectividad desde Internet hacia Isla Contoy se evaluaron y se englobaron 5 alternativas que se pueden consultar en el Anexo D, y que en la tabla 1 se resumen y se cuantifican sus propiedades y características. La cuantificación del valor 5 es la ponderación más alta, es decir cubre lo deseado o no tiene tanto impacto en las premisas, y acercarse o tener 0 es que no cumple los criterios o tiene un impacto mayor en las premisas planteadas. Los criterios evaluados que se muestran en la tabla 1 se pueden observar con mayor detalle en el Anexo E.

Tabla 1

Alternativas de solución

Criterios	Servicio satelital	Enlace de microondas	No-IP	Servidor Endian UTM	Cliente OpenVPN en Mac Mini
Cumple con el Objetivo	0	4	5	4	5
Tiempo de implementación	0	1	3	3	5
Costo de implementación	0	0	3	2	5
Consumo de energía eléctrica	0	2	5	3	5
Avituallamiento en isla Contoy	0	2	5	3	5

³ Es la unidad de medida de la potencia eléctrica en el Sistema Internacional de Unidades, que equivale a la producción de 1 julio por segundo (1J/s). El vatio o Watt mide la velocidad a la que puede transformarse la energía. (Real Academia Española.,2022).

Mantenimientos posteriores implementación	0	2	4	4	4
Maximizar los recursos existentes	0	2	5	3	5
Inscripciones y cuotas	0	2	3	3	5
Latencia	0	4	4	4	4
Continuidad en el servicio	0	3	5	5	5
Permisos y licencias Gubernamentales	0	2	5	5	5
Operación	0	3	5	5	5
Seguridad	0	4	4	5	5
Mayor control en políticas e independencia de ruteo.	0	4	4	5	5
Ponderación	0%	50%	86%	77%	97%

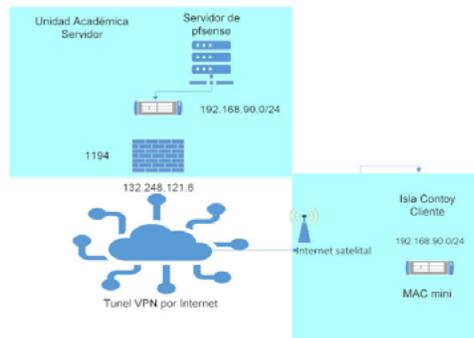
La alternativa de Cliente OpenVPN en Mac Mini es la mejor ponderada para cumplir con los objetivos de tener una conectividad hacia la Isla Contoy, pues se utiliza la infraestructura ya instalada, se tiene un mayor control y seguridad en la red, aunado a que no se requiere de costos periódicos o iniciales para su implementación.

3.4 DISEÑO DE LA RED

El diseño de red resultante es la interconexión de dos sitios remotos, ubicados en la península de Yucatán, entre la Unidad Académica de Sistemas Arrecifales y la Isla Contoy, con un enlace satelital y el cliente de VPN instalado en la isla. El cliente se conectará a la IP 132.248.121.6 por el puerto 1194 del servidor pfSense ubicado en la Unidad Académica; el diagrama conceptual de este diseño se puede observar en la figura 3.

Figura 3

Diseño conceptual del túnel de VPN

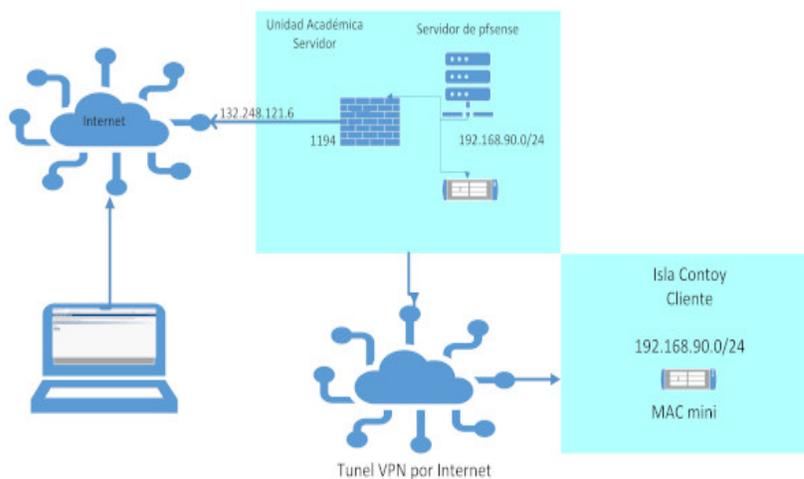


El cliente de Isla Contoy se conecta al servidor remoto de la UASA, donde el servidor le configura al cliente una IP del segmento 192.168.90.0/24 para que forme parte de la LAN interna de la Unidad Académica.

Una vez lograda la comunicación entre el cliente y servidor se genera un túnel en donde el cliente forma parte de la red LAN⁴, aún y estando físicamente en otro sitio. Configurando las políticas de firewall y NAT, se puede enrutar el tráfico de Internet desde la Unidad Académica hacia la Isla Contoy, el diagrama conceptual de este enrutamiento se muestra en la figura 4. El usuario hace la solicitud a la 132.248.121.6 del servidor de PfSense, este servidor acepta la petición y es trasladada hacia la ip del segmento interno 192.168.90.0/24, siendo totalmente transparente para el usuario final.

Figura 4

Diagrama conceptual de enrutamiento



Es importante considerar la latencia en los datos, que es inevitable en clientes o servidores de VPN, ya que se incrementa el número de saltos en la red, esto sumado a la latencia de 200 a 400 ms en enlaces satelitales de Internet; los datos comparativos de esta información se pueden observar en el Anexo F.

3.5 INSTALACIÓN Y CONFIGURACIÓN

El servidor de pfSense se instala en una máquina virtual del servidor físico existente. Para fines prácticos se muestran resumidos los pasos de las guías de instalación y configuración de pfSense (Netgate, 2023):

1. Instalación de pfSense. Para iniciar el proceso, es crucial contar con el archivo de imagen ISO de pfSense, descargable desde el sitio oficial. Tras la creación de una nueva máquina virtual en VMware, se configura el arranque desde el ISO de pfSense. La instalación inicia seleccionando "Install" y se guía al usuario a través de la configuración básica, incluyendo la asignación de interfaces de red WAN y LAN. Posteriormente, tras finalizar la instalación y retirar el medio de instalación, se accede

⁴ Una red de área local o LAN (por las siglas en inglés local area network) es una red de computadoras que permite la comunicación y el intercambio de datos entre diferentes dispositivos a nivel local, ya que está limitada a distancias cortas. (Wikipedia,2023).

a la interfaz web con la Ip previamente configurada para realizar la configuración inicial de pfSense. Algunas pantallas de configuración e inicio de la instalación se muestran en el Anexo G.

2. Configuración de interfaces de red. Este proceso implica la personalización de parámetros como la interfaz WAN, y otras configuraciones de red. Una vez completado, pfSense está listo para desplegar medidas de seguridad, reglas de firewall y funciones de red avanzadas en la infraestructura virtualizada; esta configuración también se presenta en el Anexo G.
3. Configuración del servidor de OpenVPN. Inicia con la habilitación del servicio OpenVPN y la creación de un certificado de servidor. Se establecen las configuraciones específicas del servidor, que incluye la selección del protocolo UDP o TCP; esto se puede observar en la figura 5.

Figura 5

Datos del servidor de OpenVPN

OpenVPN Servers			
Interface	Protocol / Port	Tunnel Network	Mode / Crypto
WAN	UDP / 1194 (TUN)	192.168.90.0/24	Mode: Remote Access (User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits

4. Configuración de usuarios de VPN. La creación y gestión de usuarios permite el control sobre el acceso remoto a la red. A través de la interfaz web de administración, se accede al apartado de usuarios, donde se puede añadir usuarios con credenciales y certificados.
5. Configuración de NAT. La configuración de NAT permitirá el enrutamiento del tráfico, facilitando la conexión de usuarios remotos a servicios internos; en este caso, el servicio interno está conectado por una VPN hacia la Isla Contoy, lo que para el usuario final es transparente. Los datos de configuración se pueden observar en la figura 6 de acuerdo al diseño que se mostró en la figura 4.

Figura 6

Regla de NAT para el servicio remoto

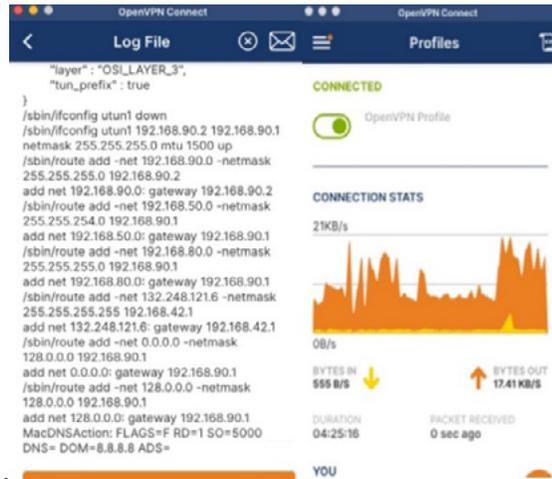
Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports
WAN	TCP/UDP	*	*	192.168.51.72/31	8240	192.168.90.2	8240

Nota: Se especifica la IP y puerto de donde está escuchando las peticiones de red, y el destino IP y puerto hacia donde se trasladará la petición recibida

6. Configuración de cliente. La instalación y configuración del cliente OpenVPN en macOS es un proceso donde se descarga e instala el cliente desde su sitio oficial, para lo cual es necesario tener el archivo de configuración (ovpn). El archivo usado en esta solución se puede observar en la tabla 4 del Anexo G. Una vez instalado y configurado se procede activar la conexión en donde se debe crear el túnel con las rutas necesarias y la aplicación marcará como conectado; en la figura 7 se presenta la pantalla de conexión.

Figura 7

Cliente de OpenVPN, conectado exitosamente



7. Pruebas y validaciones. Para validar y asegurar que la configuración esté funcionando correctamente, se pueden realizar diversas pruebas y validaciones:

- Apertura de la página deseada desde Internet.
- Ping desde el cliente hacia salida a Internet, como se muestra en la figura 8 del Anexo F.
- Monitoreo del tráfico.
- Revisión de bitácoras.
- Pruebas de ancho de banda como se muestra en la figura 7 del Anexo B.
- Trazar la ruta de los paquetes.
- Simulación de fallos.

Estas pruebas son necesarias para mitigar errores, y posibles fallas. La validación final es poder acceder a los datos desde cualquier lugar o de acuerdo con las especificaciones del usuario final.

4. CONCLUSIONES

La solución propuesta ha cubierto la necesidad de acceder a datos cruciales para las investigaciones de la UNAM, logrando este objetivo sin requerir una inversión significativa, respetando las premisas y restricciones establecidas. Si bien existe una latencia en los tiempos de respuesta debido a todas las capas por donde viajan los datos, esto no fue una restricción para cumplir con los objetivos planteados.

Esta opción destaca frente a otras alternativas que habrían implicado la conexión de hardware a la red eléctrica, la inversión de un cuarto de telecomunicaciones, la instalación de paneles solares, entre otros recursos. La elección de utilizar software libre y maximizar los recursos disponibles ha demostrado ser una alternativa eficaz para alcanzar los objetivos establecidos, asegurando así una solución eficiente

y económicamente viable, donde los interesados pueden consultar la información y realizar tareas de mantenimiento.

5. AGRADECIMIENTOS

Agradezco a los involucrados y responsables del proyecto de Estudio de la Corriente de Lazo en el Canal de Yucatán mediante radares de alta frecuencia. Proyecto UNAM-TAMU iniciado en 2019, duración: por tiempo indefinido. Instituto de Ciencias del Mar y Limnología, Universidad Nacional Autónoma de México, Cd Mx – Puerto Morelos. Salas de León D.A., Knap A.H., Glenn S., Monreal Jiménez R., Contreras Tereza V.K., Dimarco S.F., Dancer A.V., Escalante Mancera E., Gómez Reali M.A.

Agradezco también a Alfredo Landa Herrera y Fernando Negrete Soto por su asesoría y apoyo logístico.

6. REFERENCIAS

CODAR Ocean Sensor. (2023). CODAR Ocean Sensor. Versión 2023. CODAR Ocean Sensor. Estados Unidos. Recuperado de <https://www.codar.com/>. 22 de octubre de 2023.

HughesNet. (2024). [En línea]. Recuperado de <https://www.hughesnet.com/>. Recuperado el 20 de Octubre de 2024.

Instituto Federal de Telecomunicaciones. (2022). Reglamento de la Ley Federal de Telecomunicaciones y Radiodifusión. México, D.F.: IFT.

Netgate.(2023). *pfSense Installation Guide*. Recuperado de https://docs.netgate.com/pfSense/en/latest/install/download-installer-image.html?_gl=1*6smz33*_ga*MTYyOTk2NDM3MC4xNzAxMzU4NTAw*_ga_TM99KBGXCB*MTcwMTM1ODQ5OS4xLjEuMTcwMTM1ODUwNy41Mi4wLjA , Recuperado el 30 de noviembre de 2023

Real Academia Española. (2022). *Diccionario de la lengua española* (24.^a ed.). Madrid: España.

Wikipedia. (2023). Red de área local. Wikipedia, la enciclopedia libre. Recuperado de https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local: https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local, el 22 de octubre de 2023.

Wikipedia. (2023). Servicio web. Wikipedia, la enciclopedia libre. Recuperado de https://es.wikipedia.org/wiki/Servicio_web: https://es.wikipedia.org/wiki/Servicio_web, el 22 de septiembre de 2023.

ANEXO A

CARACTERÍSTICAS TÉCNICAS DEL EQUIPO MAC MINI

En la figura 8 se observa las características y versión del equipo Mac mini utilizado para la implementación de esta solución.

Figura 8

Equipo Mac Mini en Isla Contoy



Nota. El equipo Mac Mini (Late 2014) tiene el sistema operativo Mac Os High Sierra, versión 10.13.6 cuenta con un procesador Core i5 y 8 GB en RAM y un almacenamiento de 1.1 TB

ANEXO B

ESPECIFICACIONES DE LA RED EN ISLA CONTOY

La tabla 2 muestra la información de la red pública del enlace satelital, estos datos pueden variar ya que no son fijos.

Tabla 2

Especificaciones de la red WAN Isla Contoy enlace de 25 Mbps asíncrono

Parámetro	Valor
Tipo de WAN	DHCP
Dirección IP de WAN	100.70.22.57
Máscara de subred	255.255.255.248
Gateway	100.70.22.57
DNS	192.168.0.1
Dirección IPv6	fd0d:edc3:e12a:0:1:ff:fec7:887e

Nota: Es una IP variable y el proveedor no tiene el servicio de IP homologada. Se dan datos que pueden variar en el tiempo, pero son importantes para una perspectiva y entendimiento del artículo. Datos tomados en noviembre de 2023

En la tabla 3 se muestra el resumen de la red LAN de la Isla Contoy, con en el segmento de red que entrega el ruteador.

Tabla 3

Especificaciones de la red LAN Isla Contoy

Parámetro	Valor
Dirección IP	192.168.42.1
Máscara de subred	255.255.255.0

Nota: Es una IP privada. Se dan datos que pueden variar en el tiempo, pero son importantes para una perspectiva y entendimiento del artículo. Datos tomados en noviembre de 2023

La velocidad proporcionada por el proveedor es de 25Mbps asíncrono, y no se puede garantizar debido a que es un servicio satelital; en la figura 9 se muestra la velocidad obtenida el día 10 de noviembre de 2023.

Figura 9

Prueba de velocidad en Isla Contoy



Nota: Prueba de velocidad con la página speedtest.net. Datos tomados en noviembre de 2023

ANEXO C

El servidor físico utilizado para esta solución es el que se muestra en la tabla 4

Tabla 4

Servidor físico en la UASA

Propiedad	Características
Marca	Dell
Modelo	PowerEdge R330
CPU	4 CPUs x Intel(R) Xeon(R) CPU E3-1230 v6 @ 3.50GHz
Memoria	31.62 GB
IP	172.16.100.138

ANEXO D

ANÁLISIS DE MERCADO Y ESTUDIO DE ALTERNATIVAS DE SOLUCIÓN

En este anexo se muestran un resumen de las diferentes alternativas analizadas para definir la solución a implementar.

Alternativa 1: Servicio Satelital

La primera alternativa analizada fue obtener un nuevo servicio de IP fija homologada con el proveedor de Internet satelital Hughesnet. Esto no resultó factible debido a la arquitectura tipo satelital, ya que no permite tener una IP fija homologada, debido a que esta tecnología utiliza el protocolo DHCP (Protocolo de configuración dinámica de host, por sus siglas en inglés) (HughesNet, 2024); este protocolo asigna direcciones IP dinámicas a los dispositivos, sumado a que se ocupan varios satélites en órbita durante el día, a lo cual los enrutamientos cambian durante las horas. El proveedor de Internet de la Isla de Contoy se contrató mediante los procesos de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación.

Alternativa 2: Enlace de microondas

La distancia entre Isla Mujeres e Isla Contoy es de aproximadamente 10 kilómetros, por lo cual se analizó un enlace mediante tecnología de microondas con antenas parabólicas de 1.2 metros de diámetro, con un tiempo de implementación de 4 a 6 meses y un costo a 3 años +-10% de error, de 300 mil pesos, aunado a que se debe cumplir con todos los procedimientos internos de la UNAM y locales de la Isla Contoy e Isla Mujeres. También se requiere un consumo extra de 100 watts por los componentes que se requieren instalar, permisos gubernamentales de construcción y procesos internos de compras. Se requiere de mantenimientos periódicos y responsables en las islas para poder operar y restaurar servicios.

Esta alternativa tiene como desventaja las condiciones meteorológicas que pueden provocar intermitencias en el servicio, se dependen de varias capas en la red, tanto físicas como lógicas, también requiere de un mayor mantenimiento post implementación.

Alternativa 3: No -IP

Esta alternativa consiste en contratar un servicio de DNS dinámico, que permita asociar su dirección IP pública con un nombre, esto permite acceder a la red local desde cualquier parte; el tiempo de implementación es de 2 meses por procesos internos de contratación, el costo aproximado a 3 años +-10% de error, \$20,000 pesos; existen planes gratuitos, pero no incluyen o garantizan servicio sin interrupciones, puertos y clientes. No se requiere de nueva infraestructura.

Los siguientes puntos describen algunas desventajas al contratar un servicio No-IP:

- Alta probabilidad de bloqueo del servicio ya que estos servicios caen en listas negras.
- Poco control en el tráfico de la red y administración de servicios e IP.

Alternativa 4: Instalar servidor Endian UTM Mini

La alternativa de instalar un servidor de VPN conectado a OpenVPN Cloud en la Isla Contoy, mediante tecnologías como Endian o similares, para lograr la conectividad punto a punto, y hacer el túnel y NAT

hacia el servicio, implica un tiempo de implementación por compra y puesta en marcha de 2 a 3 meses, aunado a que se requiere de infraestructura y de energía eléctrica, mantenimiento y licenciamiento con un costo a 3 años de 700 mil pesos, con un margen de error de $\pm 10\%$, donde se debe tomar en cuenta el avituallamiento de la infraestructura que se requiere para su implementación.

Alternativa 5: Cliente OpenVPN en Mac Mini

Es una solución de firewall de código abierto que ofrece una amplia gama de funciones, incluida la VPN. La instalación de PfSense es relativamente sencilla tomando en cuenta que la Unidad Académica de Sistemas Arrecifales cuenta con un servidor físico para virtualizar servidores. Este serviría para crear el enlace de VPN y NAT para publicar el servicio web a Internet. El cliente de OpenVPN se instalará en la Mac Mini por lo que no representa un costo de nueva infraestructura de implementación, ni se requiere adquisición de nuevo hardware, licencia o recursos humanos. El tiempo de implementación es de 2 semanas y no se requiere adquirir o tener recursos económicos, humanos o de infraestructura.

ANEXO E

EVALUACIÓN DE ALTERNATIVAS

Los criterios que se usaron para elegir la mejor alternativa de acuerdo con las premisas y cumplimiento de los objetivos fueron los siguientes:

Cumple con el objetivo: Este criterio se refiere a la capacidad de la solución de satisfacer las necesidades específicas de los interesados.

Tiempo de implementación: Este criterio se refiere al tiempo que lleva implementar la solución: que la solución se pueda implementar en un tiempo corto, con todo el ciclo de proyecto como es el de análisis, diseño, desarrollo, cotizaciones, compras, instalaciones, pruebas y puesta en marcha.

Costo de implementación: Este criterio se refiere al costo de implementar la solución, y que de acuerdo con las necesidades planteadas, qué tan cercano está a cumplirse.

Consumo de energía eléctrica: Este criterio se refiere a si se requiere de un consumo de energía eléctrica para implementar la solución, considerando que no se cuenta de energía eléctrica extra en la Isla Contoy.

Avituallamiento en Isla Contoy: Este criterio se refiere a la capacidad de la solución para funcionar en la Isla Contoy con la infraestructura actual, o si se requiere de nueva inversión, como un cuarto de telecomunicaciones, aire acondicionado o cableado, entre otras propias de cada alternativa planteada.

Mantenimientos post implementación: Este criterio se refiere a la frecuencia con la que se necesita realizar mantenimientos en la solución.

Maximizar los recursos existentes: Este criterio se refiere a la capacidad de la solución para utilizar los recursos existentes de hardware, software, humanos y económicos.

Inscripciones y cuotas: Este criterio se refiere a cualquier costo adicional que se deba pagar por la solución.

Latencia: Este criterio se refiere al tiempo que tarda la señal en viajar desde el dispositivo del usuario hasta la red remota.

Continuidad en el servicio: Este criterio se refiere a la capacidad de la solución para proporcionar un servicio continuo.

Operación: Este criterio se refiere a la usabilidad con la que se operan y administran las soluciones. Si es necesario una operación dedicada o desatendida.

Seguridad: Este criterio se refiere a la capacidad de la solución para proteger su red y sus datos, si los datos viajarán por una red privada o comercial, si se comparte la VPN o es dedicada.

Mayor control en políticas e independencia de ruteo: Este criterio se refiere a la capacidad de la solución para controlar las políticas y el enrutamiento de la red.

ANEXO F

En este anexo se presentan pruebas para el desempeño de la red, en las diferentes modalidades; en la figura 10 se observa los tiempos cuando el cliente está conectado por satélite y por VPN.

Figura 10

Prueba de ping con enlace satelital y VPN

```
64 bytes from 8.8.8.8: icmp_seq=7 ttl=52 time=1278.416 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=52 time=1196.341 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=52 time=1195.566 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=52 time=694.779 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=52 time=1182.301 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=52 time=978.974 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=52 time=1568.454 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=52 time=852.966 s
64 bytes from 8.8.8.8: icmp_seq=15 ttl=52 time=1278.627 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=52 time=803.012 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=52 time=1044.960 ms
64 bytes from 8.8.8.8: icmp_seq=18 ttl=52 time=1174.157 ms
64 bytes from 8.8.8.8: icmp_seq=19 ttl=52 time=1159.120 ms
64 bytes from 8.8.8.8: icmp_seq=20 ttl=52 time=692.487 ms
64 bytes from 8.8.8.8: icmp_seq=21 ttl=52 time=702.857 ms
64 bytes from 8.8.8.8: icmp_seq=22 ttl=52 time=698.519 ms
64 bytes from 8.8.8.8: icmp_seq=23 ttl=52 time=696.549 ms
64 bytes from 8.8.8.8: icmp_seq=24 ttl=52 time=713.009 ms
64 bytes from 8.8.8.8: icmp_seq=25 ttl=52 time=746.462 ms
64 bytes from 8.8.8.8: icmp_seq=26 ttl=52 time=675.939 ms
64 bytes from 8.8.8.8: icmp_seq=27 ttl=52 time=741.726 ms
64 bytes from 8.8.8.8: icmp_seq=28 ttl=52 time=710.158 ms
64 bytes from 8.8.8.8: icmp_seq=29 ttl=52 time=687.456 ms
```

Nota: El promedio de 25 resultados es de 902,205 ms.

Figura 11

Prueba de ping con enlace satelital sin VPN

```
64 bytes from 8.8.8.8: icmp_seq=16 ttl=56 time=553.021 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=56 time=585.506 ms
64 bytes from 8.8.8.8: icmp_seq=18 ttl=56 time=546.851 ms
64 bytes from 8.8.8.8: icmp_seq=19 ttl=56 time=545.704 ms
64 bytes from 8.8.8.8: icmp_seq=20 ttl=56 time=544.160 ms
64 bytes from 8.8.8.8: icmp_seq=21 ttl=56 time=554.997 ms
64 bytes from 8.8.8.8: icmp_seq=22 ttl=56 time=533.928 ms
64 bytes from 8.8.8.8: icmp_seq=23 ttl=56 time=551.022 ms
64 bytes from 8.8.8.8: icmp_seq=24 ttl=56 time=567.249 ms
64 bytes from 8.8.8.8: icmp_seq=25 ttl=56 time=541.748 ms
64 bytes from 8.8.8.8: icmp_seq=26 ttl=56 time=562.076 ms
64 bytes from 8.8.8.8: icmp_seq=27 ttl=56 time=555.472 ms
64 bytes from 8.8.8.8: icmp_seq=28 ttl=56 time=544.493 ms
64 bytes from 8.8.8.8: icmp_seq=29 ttl=56 time=565.014 ms
64 bytes from 8.8.8.8: icmp_seq=30 ttl=56 time=542.756 ms
64 bytes from 8.8.8.8: icmp_seq=31 ttl=56 time=541.135 ms
64 bytes from 8.8.8.8: icmp_seq=32 ttl=56 time=553.296 ms
64 bytes from 8.8.8.8: icmp_seq=33 ttl=56 time=562.997 ms
64 bytes from 8.8.8.8: icmp_seq=34 ttl=56 time=541.065 ms
64 bytes from 8.8.8.8: icmp_seq=35 ttl=56 time=545.376 ms
64 bytes from 8.8.8.8: icmp_seq=36 ttl=56 time=561.957 ms
64 bytes from 8.8.8.8: icmp_seq=37 ttl=56 time=566.665 ms
64 bytes from 8.8.8.8: icmp_seq=38 ttl=56 time=570.725 ms
```

Nota: El promedio de 25 resultados es de 553,477 ms.

Figura 12

Prueba de ping con enlace dedicado en la Unidad Académica de Sistemas Arrecifales

```
Respuesta desde 8.8.8.8: bytes=32 tiempo=59ms TTL=55
Respuesta desde 8.8.8.8: bytes=32 tiempo=60ms TTL=55
Respuesta desde 8.8.8.8: bytes=32 tiempo=60ms TTL=55
Respuesta desde 8.8.8.8: bytes=32 tiempo=60ms TTL=55
Respuesta desde 8.8.8.8: bytes=32 tiempo=59ms TTL=55
Respuesta desde 8.8.8.8: bytes=32 tiempo=60ms TTL=55
Respuesta desde 8.8.8.8: bytes=2 tiempo=60ms TTL=55
Respuesta desde 8.8.8.8: bytes=32 tiempo=60ms TTL=55
Respuesta desde 8.8.8.8: bytes=32 tiempo=62ms TTL=55
Respuesta desde 8.8.8.8: bytes=32 tiempo=60ms TTL=55
Respuesta desde 8.8.8.8: bytes=32 tiempo=59ms TTL=55
Respuesta desde 8.8.8.8: bytes=32 tiempo=60ms TTL=55
```

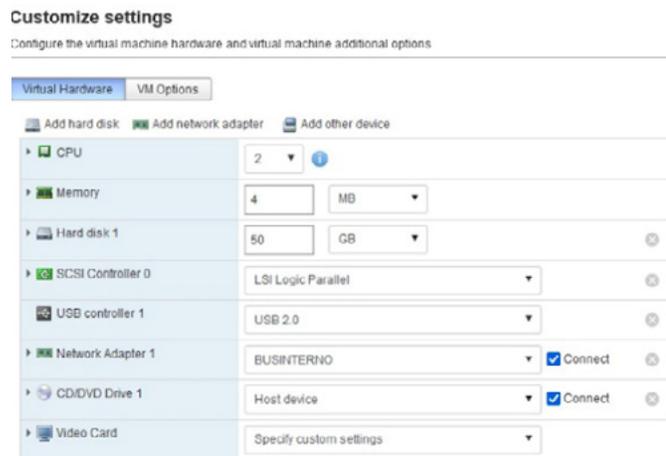
Nota: El promedio de 25 resultados es de 60 ms.

ANEXO G

Estas son algunas pantallas de configuración e inicio de la instalación del servidor PfSense:

Figura 13

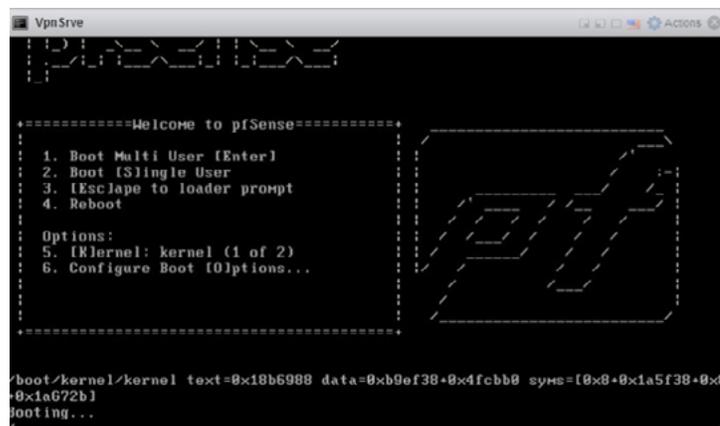
Configuración básica de servidor de PfSense



Nota: Se configuró con dos procesadores virtuales, 4 GB en RAM y 50 GB de almacenamiento

Figura 14

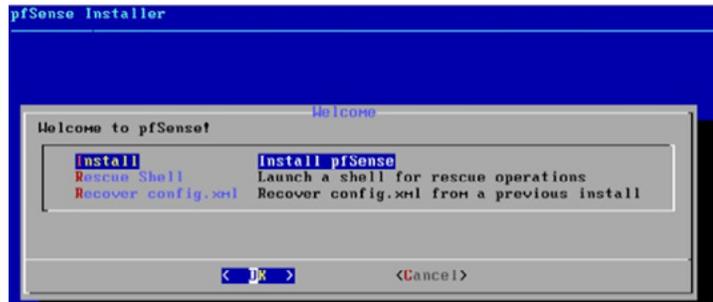
Inicio de la instalación del servidor PfSense



Nota: Al configurar el ISO en CD/DVD, éste iniciará automáticamente la instalación

Figura 15

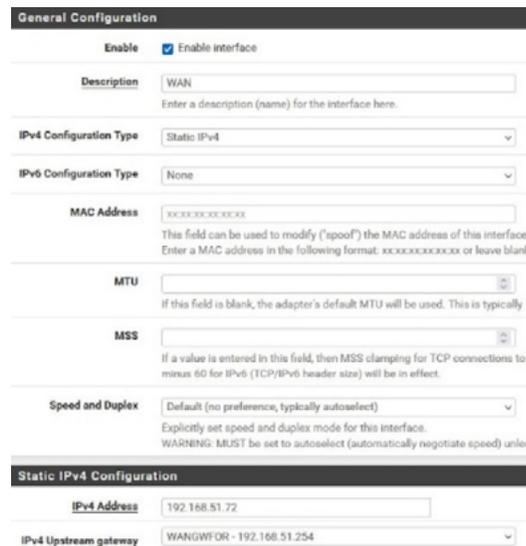
Instalación asistida del servidor PfSense



Nota: La instalación es asistida y se deberán seleccionar las opciones de acuerdo con la infraestructura y configuración deseada

Figura 16

Configuración de la red en PfSense



Nota: La configuración básica de la red WAN es establecer si es IPv4, la ip, mascara y puerta de enlace

La configuración del cliente es un tema importante que debe llevar la configuración de acuerdo con los parámetros que se configuraron en el servidor, ya que de lo contrario no se podrá crear el túnel entre los dos puntos. En la tabla 4 se presenta la configuración utilizada, personalizada y validada para su correcto funcionamiento.

Tabla 4

Configuración del cliente OpenVPN

```
#-- Config Auto Generated By pfSense for Viscosity --#
#viscosity startonopen false
#viscosity dhcp true
#viscosity dnssupport true
#viscosity name
dev tun
persist-tun
persist-key
data-ciphers AES-256-GCM:AES-128-GCM:CHACHA20-POLY1305:AES-256-CBC
data-ciphers-fallback AES-256-CBC
auth SHA256
tls-client
client
resolv-retry infinite
remote 132.248.121.6 1194 udp
nobind
auth-user-pass
remote-cert-tls server
explicit-exit-notify
push "route 192.168.20.0 255.255.254.0"
push "route 192.168.80.0 255.255.255.0"

<ca>
-----BEGIN CERTIFICATE-----
MIIEPzCCAyegAwIBAgIBADANBgkqhkiG9w0BAQsFADBzMRQwEgYDVQQDEwtpbnRl
cm5hbCIjYTELMakGA1UEAk1YMRQwEgYDVQQIEwtRdWlu
kc/
-----END CERTIFICATE-----
</ca>
setenv CLIENT_CERT 0
```

Nota: Los datos de seguridad como certificado e ip fueron modificados, ya que son datos sensibles de seguridad y en caso de usar esta configuración se deberán poner los propios

En la tabla 5 se explican los campos que son necesarios para lograr la comunicación con el servidor y generar el túnel.

Tabla 5

Explicación de los valores del archivo de configuración de OpenVPN

Parámetro	Descripción
dev tun	Crea una interfaz de túnel virtual para la transferencia de datos cifrados
persist-tun y persist-key	Conserva la configuración del túnel y las claves entre conexiones
data-ciphers	Especifica algoritmos de cifrado fuertes para la protección de datos
auth SHA256	Usa SHA256 para la autenticación e integridad de datos
tls-client	Habilita TLS para la comunicación segura con el servidor
client	Identifica esta configuración como un cliente
resolv-retry infinite	Sigue intentando la resolución de nombres indefinidamente
remote 132.248.121.6 1194 udp	Especifica la dirección IP, el puerto (1194) y el protocolo (UDP) del servidor
nobind	Evita el enlace a una dirección IP local específica
auth-user-pass	Requiere autenticación de nombre de usuario y contraseña
remote-cert-tls server	Verifica el certificado del servidor usando TLS
explicit-exit-notify	Notifica explícitamente al servidor cuando el cliente se desconecta
push "route 192.168.20.0 255.255.254.0" y push "route 192.168.80.0 255.255.255.0"	Agrega rutas a redes específicas a través del túnel VPN, para acceder a recursos en esas redes
Certificado	
<ca> sección	Contiene el certificado CA del servidor, usado para verificar la identidad del servidor
setenv CLIENT_CERT 0	Establece una variable de entorno, para uso interno de Viscosity