UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE:

INGENIERO EN ELECTRÓNICA DIGITAL Y TELECOMUNICACIONES

TEMA: DISEÑO E IMPLEMENTACIÓN DE CANALES DE COMUNICACIÓN SEGURAS ENTRE EL COMANDO GENERAL FAE Y LAS ESTACIONES REMOTAS.

AUTOR: WILLIAN HERNÁN TOAPANTA CAIZAGUANO

TUTOR: PhD. RENÉ ALBERTO CAÑETE BAJUELO

AÑO: 2015

INFORME FINAL DE RESULTADOS DEL PIC

CARRERA:	Electrónica Digital y Telecomunicaciones
AUTOR:	Willian Hernán Toapanta Caizaguano
TEMA DEL TT:	Diseño e Implementación de canales de comunicación seguras entre el Comando General FAE y las estaciones remotas
ARTICULACIÓN CON LA LÍNEA DE INVESTIGACIÓN INSTITUCIONAL:	Tecnología Aplicada a la Producción y la Sociedad
SUB-LÍNEA DE INVESTIGACIÓN INSTITUCIONAL:	Simulación, desarrollo y automatización de procesos industriales, empresariales y de la sociedad
ARTICULACIÓN CON EL PROYECTO DE INVESTIGACIÓN INSTITUCIONAL DEL ÁREA	
FECHA DE PRESENTACIÓN DEL INFORME FINAL:	Diciembre del 2015

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente proyecto está basado en el diseño e implementación de una Red Privada Virtual aplicada a la Fuerza Aérea Ecuatoriana, la cual tendrá comunicaciones con las estaciones remotas que están ubicadas geográficamente distantes.

Para el efecto se realizará la configuración de un equipo Firewall ASA 5505 la cual permitirá establecer un túnel para transmitir datos con criptografía entre dos estaciones remotas y así permitir que los usuarios puedan intercambiar datos, acceder a la INTRANET FAE (roles de pago, Hojas de vida personal, correo electrónico institucional, guía telefónica etc.)

Necesariamente se requiere instalar las aplicaciones VPN CLIENT y el Softphone en los equipos terminales para poder emular y entablar comunicaciones telefónicas a la Red MODE de las Fuerzas Armadas, a teléfonos convencionales y celulares con costos de llamadas locales, generando un ahorro significativo de recursos económicos al estado ecuatoriano.

DESCRIPTORES:

Red

Virtual

Comunicaciones

Seguridad

ABSTRACT

This project is based on the design and implementation of a Virtual Private Network throughout the Ecuadorian Air Force, which will have communications with the remote stations that are located geographically distant.

For the effect settings of a team which ASA 5505 Firewall will establish a tunnel to transmit data encryption between two remote stations, and allow users to exchange data, access the intranet FAE (roles payment will be made Leaves of personal, institutional e-mail, phone book etc.)

Necessarily it required to install applications and VPN CLIENT Softphone terminal equipment to emulate and engage the MODE telephone network of the Armed Forces, conventional cell phones with local calls, communications costs, generating significant savings of funds to Ecuadorian state.

WORDS:

Net

Virtual

Communications

Security

INTRODUCCIÓN

ANTECEDENTES

Una VPN (Virtual Private Network) o RPV, es una tecnología de red que permite una extensión de la red local sobre una red pública como el Internet. (García Alfaro, 2004, pág. 170)

En los últimos años las redes se han transformado en un elemento crítico para cualquier organización. Cada vez va en aumento, transmitiendo información calificada. Por lo tanto dichas redes deben cumplir con atributos tales como seguridad, alcance geográfico y ahorro en costos. (Gonzales, 2014)

En la actualidad las redes reducen los gastos y tiempo de las empresas, eso significa una gran ventaja para las organizaciones en especial aquellas que cuentan con oficinas remotas a varios kilómetros de distancia, a la vez estas redes despiertan la curiosidad de personas que se dedican a atacar los servidores para obtener información calificada. Por lo tanto la seguridad de redes es de gran importancia, y es por eso que se escucha hablar tanto de los firewalls. (García Alfaro, 2004, págs. 170-174)

Los datos que viajan a través de una RVP, parten del servidor dedicado y llegan a un firewall que hace la función de una pared para engañar a los intrusos de la red, después los datos llegan a la nube de internet en el cual se forma un túnel dedicado únicamente para nuestros datos a fin de que con una velocidad y ancho de banda garantizado lleguen al firewall remoto terminando en el usuario final. (Red privada virtual, 2014)

PROBLEMA INVESTIGADO

Debido a las frecuentes movilizaciones que tiene el personal militar por requerimientos institucionales en los diferentes sitios del país y hacia el exterior, existe la necesidad de comunicación con las diferentes unidades militares de manera segura para realizar coordinaciones laborales, así mismo se tiene la necesidad de mantenerse en contacto con sus respectivas familias, lo que resulta costoso la utilización de la telefonía celular y convencional.

Existen agregadurías militares ubicadas en diferentes países del mundo que requieren realizar coordinaciones y transmitir/recibir documentación calificada con los diferentes repartos de la Fuerza Aérea Ecuatoriana con seguridad criptográfica. Además tienen la necesidad de comunicarse con sus respectivas familias y esto genera elevados gastos económicos al presupuesto estatal y personal.

OBJETIVO GENERAL

Diseñar e implementar canales de comunicación seguros entre el Comando General de la Fuerza Aérea y las estaciones remotas, para generar ahorros de recursos económicos.

OBJETIVOS ESPECÍFICOS

- Seleccionar y realizar la configuración del equipo firewall para la habilitación del túnel VPN.
- Integrar la Intranet de la Fuerza Aérea con las estaciones remotas a través de una red virtual privada con seguridad encriptado.
- Integrar el sistema seguro de la red MODE de las Fuerzas Armadas con las estaciones remotas a través de la VPN.
- Realizar una prueba de campo demostrando el óptimo funcionamiento del sistema implementado.

FUNDAMENTACIÓN TEÓRICA Y METODOLÓGICA DEL PRODUCTO

RED PRIVADA VIRTUAL (VPN)

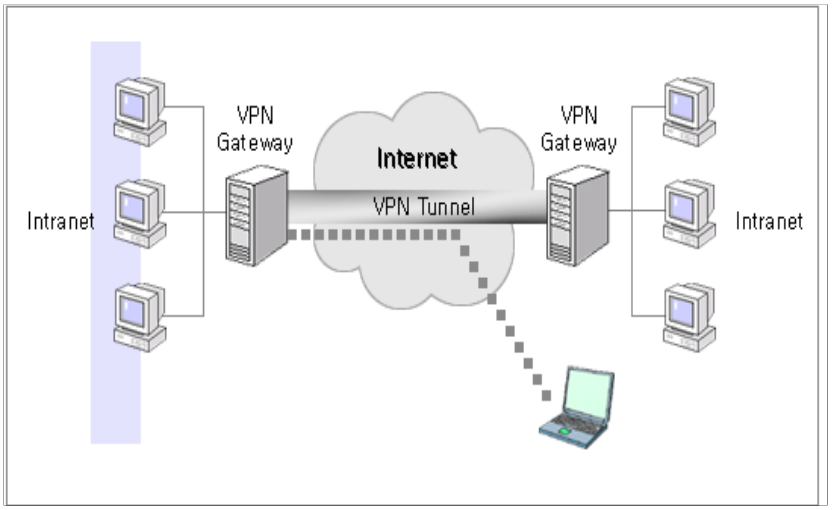

Figura 1: Esquema de una Red VPN
Fuente: (VPN, 2014)

Es la forma de compartir información entre un número determinado de usuarios que se encuentran en distintos lugares del planeta utilizando el Internet como medio de comunicación. La transmisión de los datos se realiza a través de la creación de túneles virtuales que aseguran la confidencialidad e integridad de los paquetes de datos a ser transportados. (Gonzales, 2014)

Este tipo de redes están implementadas con firewalls y Router´s para lograr la encriptación y autentificación, permitiendo el acceso remoto a los servicios de red. (Red privada virtual, 2014)

CARACTERÍSTICAS FUNCIONALES

Para que la Red Virtual proporcione la comunicación esperada, se debe contemplar varios aspectos de funcionamiento:

- Confidencialidad
  Por medio de la encriptación los datos que se transmiten por el canal solo pueden ser leídos por el transmisor y el receptor.
- Transparente a las aplicaciones
  No afectan el correcto funcionamiento de las aplicaciones.

- Integridad
  Los datos que llegan al receptor son exactamente los mismos que el emisor transmitió por la Red Virtual.
- Autentificación
  El receptor y emisor determinan de forma correcta sus identificaciones.
- Control de acceso
  Controla el acceso de los usuarios a los recursos no permitidos.
- Viabilidad
  Garantiza la conectividad del servicio en tiempo real. (Espallagas, Limonche, & Robles, 1995, págs. 422,423)

VENTAJAS

- Representa una solución en lo que se refiere a integridad, confidencialidad y seguridad de los datos.

- La Red Virtual dispone de una conexión de red con todas las características de la RVP que se accede, adquiriendo el usuario totalmente la condición de miembro de esa red, aplicando todas las condiciones de seguridad y permisos en un computador de esa red privada.

- Simplifica el crecimiento y la integración de una red, debido a que la Red Virtual facilita una solución escalable y flexible.

- Minimiza el costo de administración y soporte de la red, ayudando a incrementar la producción en la administración y soporte de la red. (Firewall Cisco, 2014)

DESVENTAJAS

- Complejidad en el tráfico de datos produciendo efectos indeseados al cambiar la numeración asignada al usuario RPV y que puede solicitar cambios en las configuraciones de programas o aplicaciones (servidor de correo, proxy, permisos basados en IP).
- Al realizar la encapsulación y encriptación de los paquetes de datos la VPN tiene mayor carga en la red, lo que origina que las conexiones tengan mayor lentitud.
- Se deben establecer las políticas de seguridad y de acceso de manera primordial. (Firewall Cisco, 2014)

ELEMENTOS PRINCIPALES DE UNA VPN

CLIENTE VPN

(Gonzales, 2014) “Es el usuario final que tiene una conexión virtual con un servidor VPN a través de una red pública de manera segura”.

VPN SERVER

Permite conectarse con otros servidores VPN ubicándose como Gateway en la salida de la red, generando túneles de comunicación con usuarios remotos proporcionando una conexión segura entre las redes. (Gonzales, 2014)

CONEXIÓN VPN

(Cisco ASA, 2014) Es la transmisión de datos de un lugar a otro de manera encriptada.

TÚNEL

(VPN, 2014) “Porción de la conexión en la cual se encapsulan sus datos”.

RED DE TRÁNSITO

(Cisco ASA, 2014) “La red pública que se cruzan los datos encapsulados, generalmente el internet”.

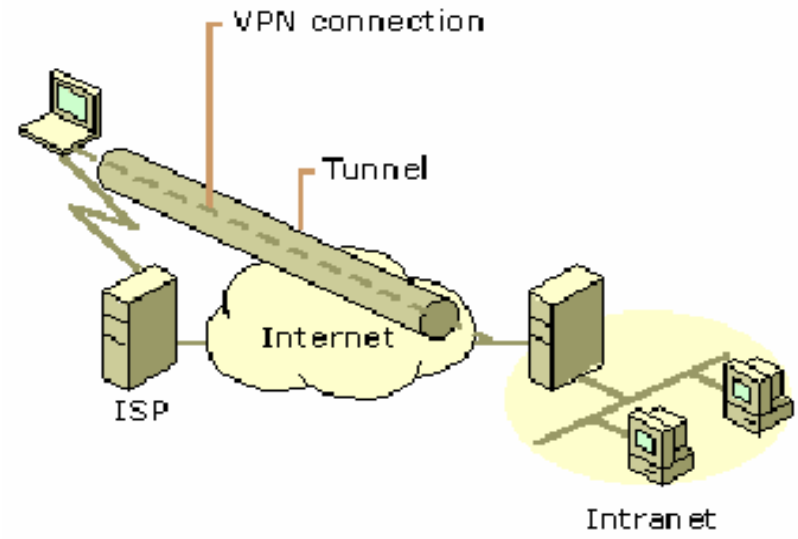

Figura 2: Elementos de una VPN
Fuente: (Cisco ASA, 2014)

REQUERIMIENTOS BÁSICOS DE LAS VPN´S

Al implementar la solución de red remota, la Fuerza Aérea logrará el acceso controlado a la información y a los recursos de la institución. La solución permitirá la libertad para que los usuarios remotos se conecten fácilmente a los recursos de la Intranet de la Fuerza Aérea. Así como las agregadurías se conecten entre sí para compartir recursos e información, garantizando la integridad y la privacidad de los paquetes que viajan a través del Internet, presentando los siguientes requerimientos:

ADMINISTRACIÓN DE DIRECCIÓN.

(Gonzales, 2014) Asignación de direcciones a clientes de la red privada, asegurándose de que se mantengan las direcciones privadas.

AUTENTICACIÓN DE USUARIO.

Verificar la identidad y permitir el acceso a la VPN a usuarios autorizados, proporcionado registros contables y de auditoria para mostrar quien y a que información accedió y cuando lo hizo. (Gonzales, 2014)

ADMINISTRACIÓN DE CLAVES.

(Gonzales, 2014) Generar y renovar las claves de encriptación para el cliente y el servidor.

ENCRIPTACIÓN DE DATOS.

(Gonzales, 2014) Los datos que viajan por el túnel a través de una red pública pueden ser leídos únicamente por clientes autorizados de la red.

ESCENARIOS MÁS COMUNES DE VPN´s

VPN´s Y ACCESO REMOTO

Se utiliza una conexión dial-up del cliente al RAS (servicio de acceso remoto) vía módems, considerando el ancho de banda apropiado a fin de que la conexión tenga sentido, usualmente los ISP no bloquean los protocolos que se usan; el administrador configura toda la infraestructura para garantizar la seguridad, de modo que el usuario remoto “disca” al número IP del servidor virtual, entrando a la etapa de autenticación y autorización (user-name y password) del enlace VPN. (Enciclopedia, 2013, pág. 339)

SITE-TO-SITE VPN

Enlaza las redes LAN entre diferentes ubicaciones geográficas, de ésta manera remplaza las costosas líneas dedicadas, empleando un enlace de red virtual a través de la red pública. Con este enlace deben autenticarse los servidores RVP entre sí, sin requerir autenticación de usuarios. (FAE, 2014)

Al establecer la conexión RVP, uno de los servidores asume el rol de cliente para iniciar una conexión con otro servidor de red virtual. (Vivanco , 2013)

TOPOLOGÍAS

Las topologías VPN se crean de acuerdo a las necesidades de la organización o se adaptan a la configuración de red existente; estas topologías se definen a través de acceso remoto como puede ser una laptop accediendo a un servidor LAN, conexión entre dos LAN a través de la Intranet y Extranet. (wikipedia, 2015)

TOPOLOGÍA DE VPN UTILIZANDO ACCESO REMOTO

Es el más usado y común en la topología. Aparece con la necesidad de un cliente externo quiere conectarse a la red interna de su empresa. Para esto se requiere que la organización tenga un firewall instalado con los software´s necesarios para implementar una red virtual y el cliente debe tener instalado un software con criptografía compatible con el firewall. (García Alfaro, 2004, pág. 174)

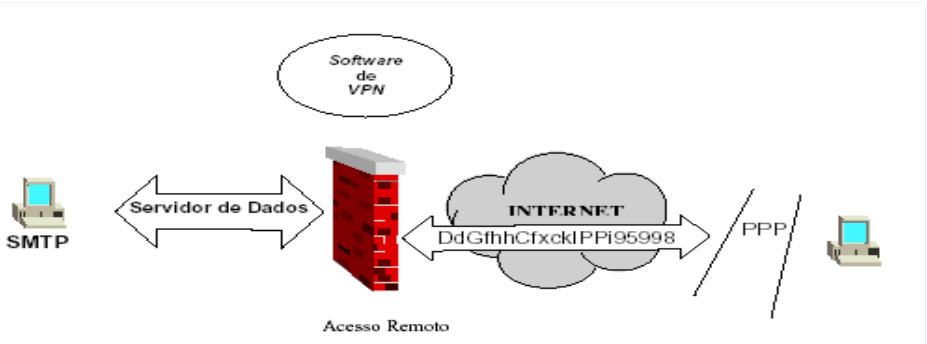

Figura 3: VPN de acceso remoto
Fuente: (Cisco ASA, 2014)

TOPOLOGÍA DE RVP SITE-TO-SITE

Esta topología es usada cuando se requiere comunicar dos redes LAN separadas geográficamente. En su configuración pueden usar software de RVP diferentes, pero deben usar en la criptografía el mismo algoritmo, configurados para cuando existan enlaces entre firewall, este tiene que ser criptografiado. (Cisco ASA, 2014)

ANÁLISIS DE PROTOCOLOS

Los fundamentos de una VPN son:

La criptografía.- se utiliza para garantizar la autentificación, confidencialidad e integridad de las conexiones siendo la base para la seguridad de las redes. (García Alfaro, 2004, pág. 104)

El tunelamiento.- es el encapsulamiento y transmisión de los datos sobre una red WAN entre dos puntos distintos.

En el mercado existen varios protocolos que proporcionan este servicio, que difieren entre sí dependiendo del nivel del modelo ISO/OSI. (Firewall Cisco, 2014)

CARACTERÍSTICAS BÁSICAS DE UN ANÁLISIS DE SEGURIDAD

Las características básicas de un análisis de seguridad de los protocolos utilizados para acceso remoto VPN en plataformas Linux o Windows son las siguientes:

PROTOCOLO DE TÚNEL PUNTO A PUNTO (PPTP)

El protocolo de las siglas Point to Point Tunneling Protocol, provee una red privada virtual entre usuarios remotos y servidores de red.
Encapsula data gramas de red en data gramas del protocolo de internet, siendo tratados como cualquier paquete IP. (Mason, 2002)

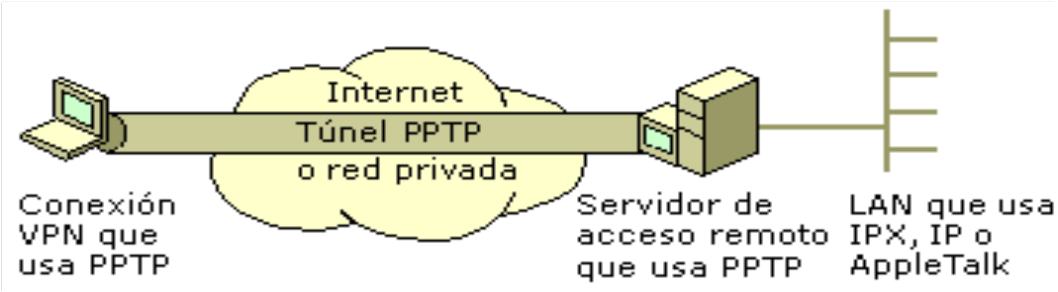

Figura 4: Diagrama del Protocolo PPTP
Fuente: (Red privada virtual, 2014)

PROTOCOLO DE SEGURIDAD DE INTERNET

IP-Sec es un estándar de la Internet Engineering Task Force (IETF), provee servicios de seguridad como autenticación, integridad, control de acceso y confidencialidad. Está implementado en la capa de Red. (García Alfaro, 2004, pág. 113)

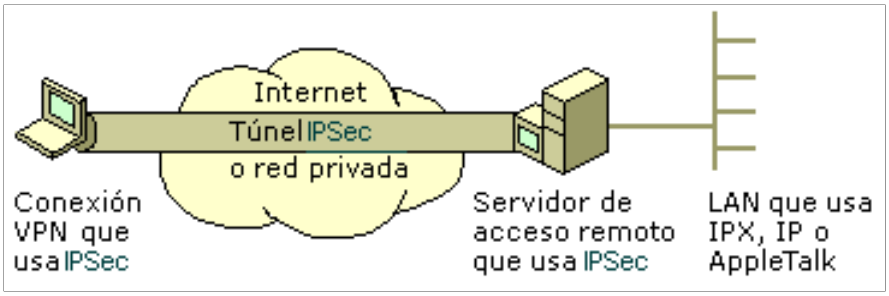

Figura 5: Diagrama del Protocolo IP-Sec
Fuente: (Cisco ASA, 2014)

Proporciona un mecanismo estándar, robusto y con posibilidades de expansión, para proveer seguridad a los protocolos IP y de capas superiores. (Red privada virtual, 2014)

FUNCIONAMIENTO DE IP-SEC

IP-Sec tiene dos modos de funcionamiento: el de transporte y el de túnel, en modo transporte protege la carga útil IP (capa de transporte), en modo túnel se protegen paquetes del protocolo de internet (capa de red) e implementando tres combinaciones: AH (Authentication Header, autenticación del origen de los datos) en modo transporte y túnel, ESP (Encapsulating Security Payload, confidencialidad*)* en modo transporte, ESP en modo túnel. (García Alfaro, 2004, págs. 105-108)

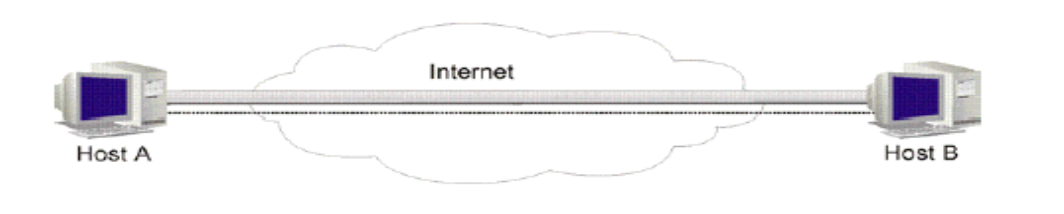

Figura 6: Modos de funcionamiento de IPSec
Fuente: (Espallagas, Limonche, & Robles, 1995)

El modo transporte se utiliza a nivel de hosts. ESP y AH en este modo intercepta los paquetes originarios de la capa de transporte a la de red aplicando la seguridad configurada. El esquema de IP-Sec en modo transporte, si la política de seguridad dice que los paquetes deben ser encriptados, se utiliza ESP en modo transporte, si solo se requiere autenticación, se utiliza AH en modo transporte. (García Alfaro, 2004, págs. 109-110)

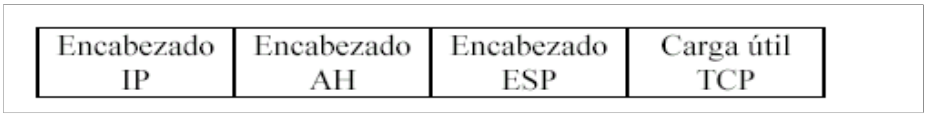

Figura 7: Cabeceras de IP-Sec
Fuente: (Cisco ASA, 2014)

El modo túnel se usa cuando la seguridad es aplicada a una red virtual, o cuando el paquete necesita ser asegurado de un punto hacia otro ubicados geográficamente distantes. El flujo de tráfico es entre host A y B, e IP-Sec se emplea con una agrupación de seguridad entre RB y RA, o también una agrupación de seguridad entre A y RB. (García Alfaro, 2004, págs. 115-117)

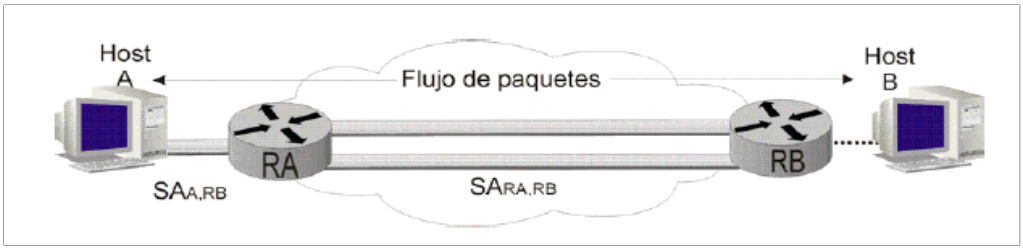

Figura 8: Flujo de paquetes
Fuente: (Enciclopedia, 2013)

PAQUETE DE ENCRIPTACIÓN IP

CAPAS Y CIFRADO DE RED

Existen varios sitios en donde la encriptación se puede montar internamente de una infraestructura de red, correspondiente a los protocolos de las distintas capas.

NIVEL DE RED: Los paquetes que recorren en la red son encriptados y su motor de encriptación está junto al driver que tx/rx los paquetes. La implementación se encuentra en CIPE.(Crypto IP encapsulación). (García Alfaro, 2004, pág. 110)

.

NIVEL DE APLICACIÓN: Las aplicaciones contienen su propio motor de cifrado y cifran los datos ellos mismos. Un ejemplo es PGP (Pretty Good Privacy) que cifra correo. El encriptado de nivel bajo está implementado con CIPE, tiene la ventaja de ser hecho para trabajar de forma transparente, sin afectación a la aplicación software.
La encriptación de bajo nivel posee la desventaja de no proteger contra los intrusos de niveles más altos, como son los bug exploit, troyanos, dentro del software del sistema pillos "sniffers" en los dispositivos terminales. (Textoscientíficos, 2010).

DIAGNÓSTICO DEL PROBLEMA Y DESCRIPCIÓN DEL PROCESO INVESTIGATIVO

PROBLEMA PRINCIPAL

La Fuerza Aérea dispone de Agregadurías Militares en diferentes países del mundo, las cuales realizan comunicaciones e intercambio de información frecuentemente entre los distintos sitios de administración. Estas acciones presentan un grave problema debido a que mencionada información se transmite con un nivel bajo de seguridad, lo que se expone a pérdida de información calificada.

Además representa un elevado costo en las tarifas telefónicas con costos internacionales que muestran tanto en la Comandancia General FAE como en las Agregadurías Militares.

EXPLICACIÓN DE LOS OBJETIVOS PLANTEADOS

En los últimos años las redes de datos se han convertido en un factor crítico para todo tipo de organizaciones, las redes transmiten información calificada. Por lo tanto dichos canales de transmisión deben cumplir con atributos tales como alcance a grandes distancias, seguridad y ahorro en costos.

Las redes reducen los gastos y tiempo de las empresas, eso significa una gran ventaja para la Fuerza Aérea ya que cuenta con Agregadurías Militares en diferentes países del mundo. Estas redes despiertan la acción de personas dedicadas a atacar los servidores, computadores para obtener todo tipo de información confidencial.

El objetivo principal de este diseño de red es que la voz y los datos que viajan a través de una RVP parten del servidor dedicado y llegan a un firewall que hace la función de una pared para engañar a los intrusos de la red, después los datos llegan al internet generando un túnel dedicado únicamente para mencionados datos, a fin de que estos con una velocidad y ancho de banda garantizado lleguen a un firewall remoto y culmine en el servidor final.

SEGURIDAD

Navegar en la red y compartir información a través de Wi-Fi público o privado, es muy arriesgado porque hay agujeros de seguridad entre el dispositivo y los sitios web que accede.

Los nombres de usuario y contraseñas que se utilizan para acceder a sus cuentas bancarias, cuentas de redes sociales y otras cuentas confidenciales pueden ser interceptados y robados por hackers. (García Alfaro, 2004, págs. 119-120)

El túnel privado ofrece una sólida autenticación y cifrado entre el teléfono móvil, tableta o computadora y cualquier contenido que usted acceda a proteger sus comunicaciones a través de Internet.

PROTECCIÓN

Los hackers apuntan a sitios web legítimos para alterar e inyectar código malicioso. Visitar estos sitios le expone a robo de su inicio de sesión y contraseñas.

Revelan su dirección IP pública y los Ciber-Delincuentes tienen la oportunidad para lanzar ataques maliciosos contra su dirección IP a fin de traer a su red y dar de baja el servicio.

El túnel privado oculta su dirección IP pública y protege su red contra este tipo de ataques. Está integrado con Open DNS y otras tecnologías anti-malware que mejoran su experiencia de navegación por la web y prohíben el acceso a páginas web maliciosas. (García Alfaro, 2004, págs. 121-123)

ACCESIBILIDAD

La accesibilidad a cualquier contenido de la web debería ser el derecho de todo ser humano en todo el mundo sin importar el lugar donde vivan.

Existen muchos países que han impuesto políticas para bloquear a sus ciudadanos de los derechos básicos para acceder al contenido web específicamente en Internet. China y algunos países de Oriente Medio se encuentran entre los países que bloquean Facebook, Twitter y otros recursos.
El túnel privado ofrece métodos avanzados para eludir las restricciones de proveer acceso a cualquier contenido de la web, sin importar su ubicación. (García Alfaro, 2004, págs. 124-125)

HIPÓTESIS

La implementación de la red de datos con tecnología VPN permitirá la comunicación de voz y datos entre las estaciones remotas y la Comandancia General FAE de manera segura y económica.

VARIABLE INDEPENDIENTE

Red de datos con tecnología VPN

VARIABLES DEPENDIENTES

Comunicaciones entre estaciones remotas.
Comunicaciones seguras
Comunicaciones económicas

DESCRIPCIÓN DE LA TEORÍA EN LA QUE SE FUNDAMENTA EL PROYECTO

Para el diseño de una red de datos a través de tecnología VPN, y poder establecer comunicaciones de voz y datos entre la Comandancia General FAE y las estaciones remotas que nacen de una necesidad institucional, se toma la teoría de redes virtuales privadas y telefonía IP.

METODOLOGÍA

El presente proyecto está basado en un requerimiento institucional, ya que se requiere un tipo de comunicaciones a nivel mundial que sean de manera segura y económica, por tal motivo se utiliza como método investigativo la técnica de la encuesta que contiene 5 preguntas relacionadas al tema de proyecto, aplicadas a miembros de la FAE que mantienen frecuentes movilizaciones a nivel nacional e internacional.
Luego se realiza la tabulación y graficación de los resultados que se visualizan en este capítulo con el propósito de interpretar los datos de la encuesta y verificar la hipótesis sobre la implementación de la red de datos con tecnología VPN con el objeto de efectuar una clase demostrativa de enlace a través de un túnel de internet.

LA ENCUESTA

POBLACIÓN Y MUESTRA

La muestra es el conjunto de elementos de un colectivo que se selecciona para obtener de ellos información, que posteriormente servirá para validar la hipótesis.
La fórmula utilizada para el cálculo de la muestra de la encuesta utilizada, es la más utilizada: (Palacios, Guía de proyectos I, 2007, págs. 8-9)

$$n = \frac{K^2 * p * q * N}{\left(e^2(N-1)\right) + K^2 * p * q}$$

Dónde:
N = es el universo, que para el proyecto lo constituyen 7000 usuarios que se proyectarán como usuarios de la red VPN.

K = constante de nivel de confianza de 1.96
e = Máximo error admisible (3%) 0.03
p = es la variabilidad positiva (50% $>$ 0.25) 80%
q = es la variabilidad negativa (50% $<$ 0.16) 20%
n = es el tamaño de la muestra

El tamaño de la muestra con estos datos arroja como resultado 166
Con este cálculo se realiza la encuesta a 150 usuarios, entre personal de Oficiales y Aerotécnicos de la Fuerza Aérea Ecuatoriana (FAE, 2014)
A continuación se analizan las respuestas obtenidas:

FORMATO DE INSTRUMENTOS APLICADOS

1. ¿Conoce otra manera de comunicarse a nivel mundial aparte de la telefonía convencional o celular? Si su respuesta es afirmativa indique cuáles son:

SI	
NO	

……

2. ¿Le gustaría que en la transmisión/recepción de datos se realice de manera, segura y confiable?

SI	
NO	

3. ¿Le gustaría que sus llamadas telefónicas a larga distancia nacional o internacional no tengan costo económico?

SI	
NO	

4. ¿Ha utilizado enlaces VPN?

SI	
NO	

5. ¿Sería de su aceptación la utilización de telefonía IP con tecnología VPN considerando los beneficios mostrados anteriormente?

SI	
NO	

TABULACIÓN Y ANÁLISIS DE RESULTADOS

1.- ¿Conoce otra manera de comunicarse a nivel mundial aparte de la telefonía convencional o celular? Si su respuesta es afirmativa indique cuáles son

Tabla No 1	**Número de Encuestados**	**SI**	**NO**
Total	150	10	140
Porcentaje	100%	7%	93%

Tabla 1: Tabulación pregunta 1 encuesta
Elaborado por: El Autor

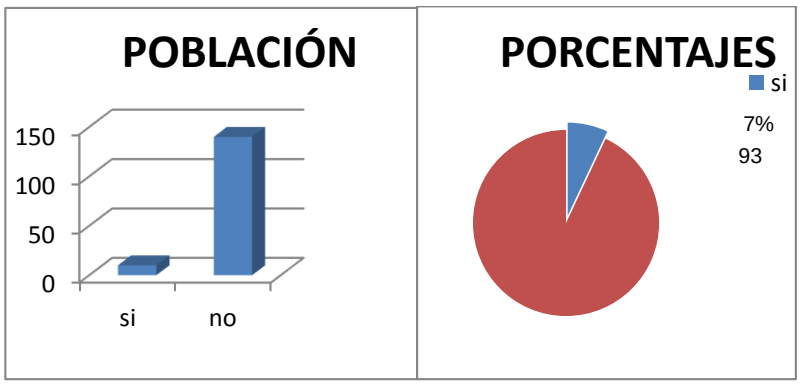

Figura 9: Gráfico de frecuencias 1
Elaborado por: El Autor

Análisis pregunta 1:

De 150 personas encuestados que equivalen al 100%, 140 de ellos equivalen al 93%, contestaron que no conocen otra manera de comunicarse a nivel mundial aparte de la telefonía convencional o celular, mientras que 10 personas que equivale al 7% dijo que sí. Por lo cual se concluye que la mayoría de personas desconocen otros tipos de comunicaciones.

2.- ¿Le gustaría que en la transmisión/recepción de datos se realice de manera rápida, segura y confiable?

Tabla No 2	Número de Encuestados	SI	NO
Total	150	150	0
Porcentaje	100%	100%	0%

Tabla 2: Tabulación pregunta 2 encuesta
Elaborado por: El Autor

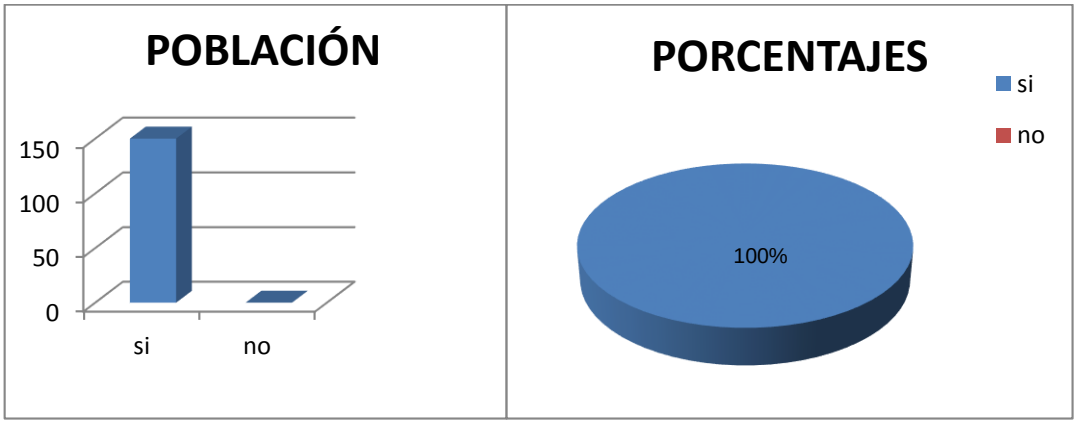

Figura 10: Gráfico de frecuencias 2
Elaborado por: El Autor

Análisis pregunta 2:

De 150 personas encuestadas que equivalen al 100 %, a todos ellos les gustarían que en la transmisión/recepción de datos se realice de manera rápida, segura y confiable.

3.- ¿Le gustaría que sus llamadas telefónicas a larga distancia nacional o internacional no tengan costo económico?

Tabla No 3	Número de Encuestados	SI	NO
Total	150	150	0
Porcentaje	100%	100%	0%

Tabla 3: Tabulación pregunta 3 encuesta
Elaborado por: El Autor

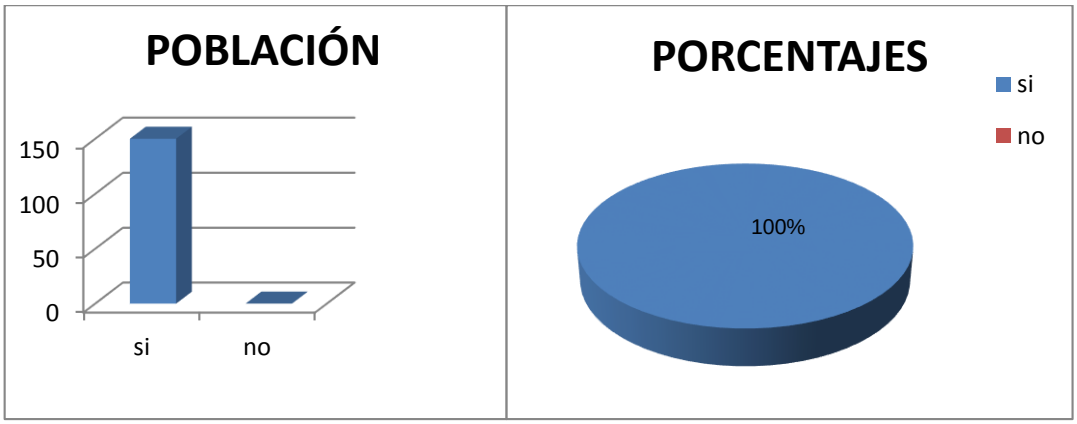

Figura 11: Gráfico de frecuencias 3
Elaborado por: El Autor

Análisis pregunta 3:

De 150 personas encuestadas que equivalen al 100 %, todos definieron que les gustarían que sus llamadas telefónicas a larga distancia nacional o internacional no tengan costo económico.

4.- ¿Ha utilizado enlace VPN?

Tabla No 4	Número de Encuestados	SI	NO
Total	150	1	149
Porcentaje	100%	1,5%	98,5%

Tabla 4: Tabulación pregunta 4 encuesta
Elaborado por: El Autor

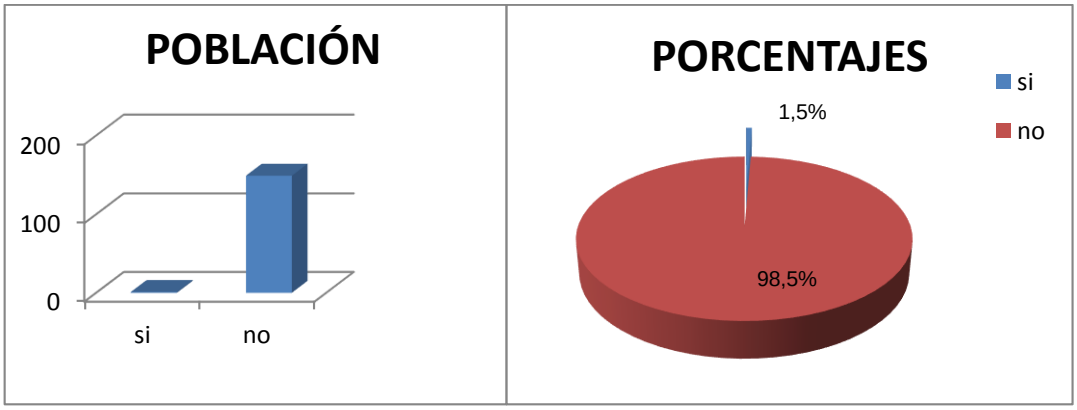

Figura 12: Gráfico de frecuencias 4
Elaborado por: El Autor

Análisis pregunta 4:

De 150 personas encuestadas que equivalen al 100 %, 1 de ellos contestó que si había utilizado enlace VPN, mientras que 149 personas que equivalen al 98,5% no lo han hecho.

5.- ¿Sería de su aceptación la utilización de telefonía Voz sobre IP con tecnología VPN considerando los beneficios mostrados anteriormente?

Tabla No 5	Número de Encuestados	SI	NO
Total	150	150	0
Porcentaje	100%	100%	0%

Tabla 5: Tabulación pregunta 5 encuesta
Elaborado por: El Autor

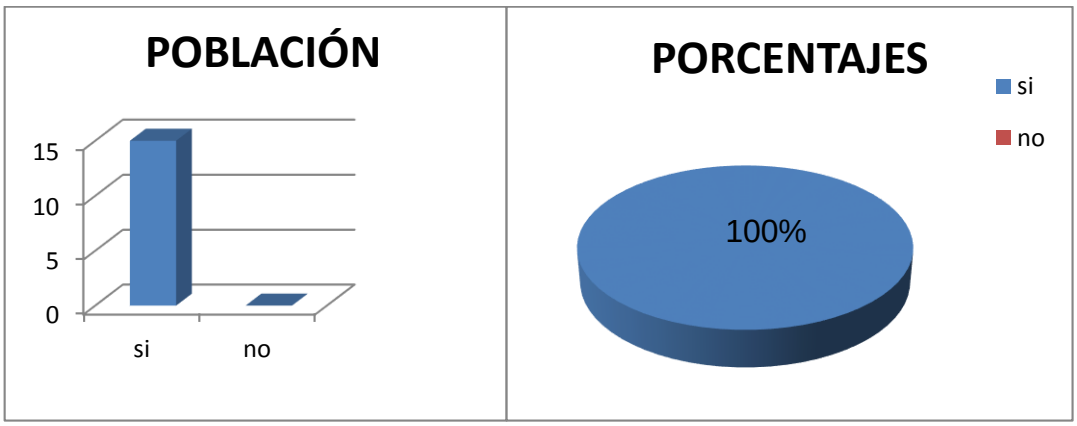

Figura 13: Gráfico de frecuencias 5
Elaborado por: El Autor

Análisis pregunta 5:

De 150 personas encuestados que equivalen al 100 %, todos contestaron que si sería de su aceptación la utilización de telefonía Voz sobre IP con tecnología VPN.

ANÁLISIS INTEGRAL

De acuerdo a la encuesta realizada que consta de 5 preguntas de tipo cerrado relacionadas directamente con el proyecto planteado, se concluye que existe una respuesta favorable ya que el porcentaje de respuestas positivas fue del 98,3%, por lo tanto la realización del enlace de comunicaciones a través de VPN es factible.

Para la realización de este proyecto se aplica los conocimientos adquiridos en asignaturas como Redes de datos y Telefonía.

RESULTADOS ESPERADOS

La implementación de una red de datos VPN nos permite conectar redes físicamente entre la Comandancia General de la Fuerza Aérea Ecuatoriana y las estaciones remotas ubicadas en distintas partes del mundo con seguridad encriptado.

Con el uso de ésta tecnología se logra realizar llamadas telefónicas entre los usuarios de la red y cualquier operadora que brinda servicio telefónico usando el túnel VPN.

PRESENTACIÓN Y DESCRIPCIÓN DEL PRODUCTO

DISEÑO DE LA RED VPN

Con una VPN un usuario remoto puede acceder a la red MODE de las Fuerzas Armadas del Ecuador a través del internet, formando un túnel seguro entre el pc del usuario y un servidor VPN de la institución.

Es un canal virtual, seguro con encriptación (seguridad) entre sitio remoto y sitio local.

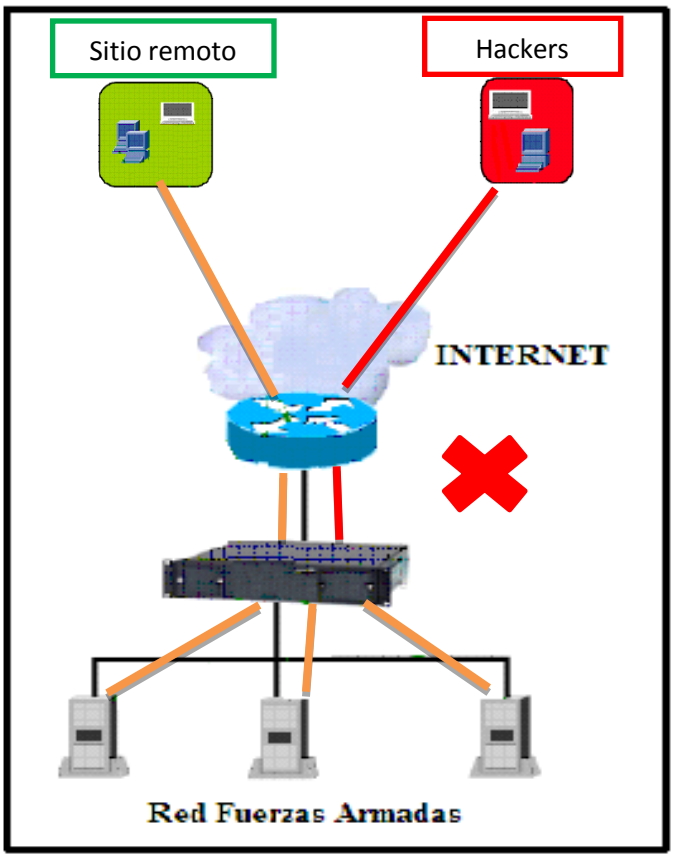

Figura 14: Red de integración VPN
Elaborado por: El Autor

Se forma un túnel virtual y seguro que permite extender geográficamente la conectividad entre un sitio ubicado en el Ecuador y un usuario ubicado en cualquier lugar del mundo (ejemplo Italia)

La conectividad de servicios (voz, datos) que presenta un sitio en una red LAN, se interconecta con un equipo ASA 5510 construyendo una especie de túnel en la nube de internet, solicitando una autenticación al sitio remoto que contiene un Firewall antes de llegar a la conectividad LAN del sitio remoto.

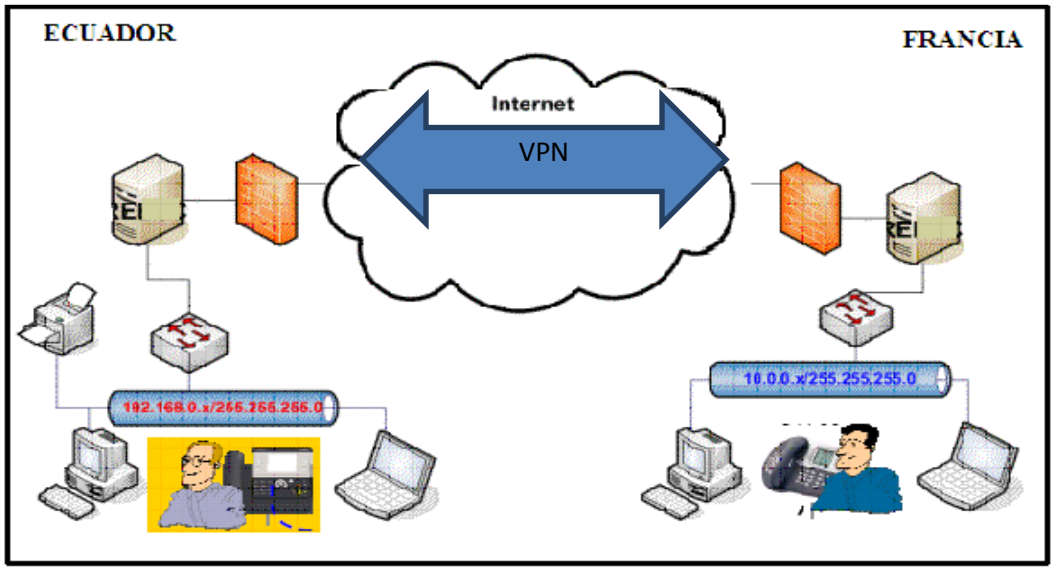

Figura 15: Red de integración VPN FAE
Elaborado por: El Autor

Para cada sitio remoto ubicado indistintamente del lugar geográfico en que encuentre se establece un túnel de conexión diferente

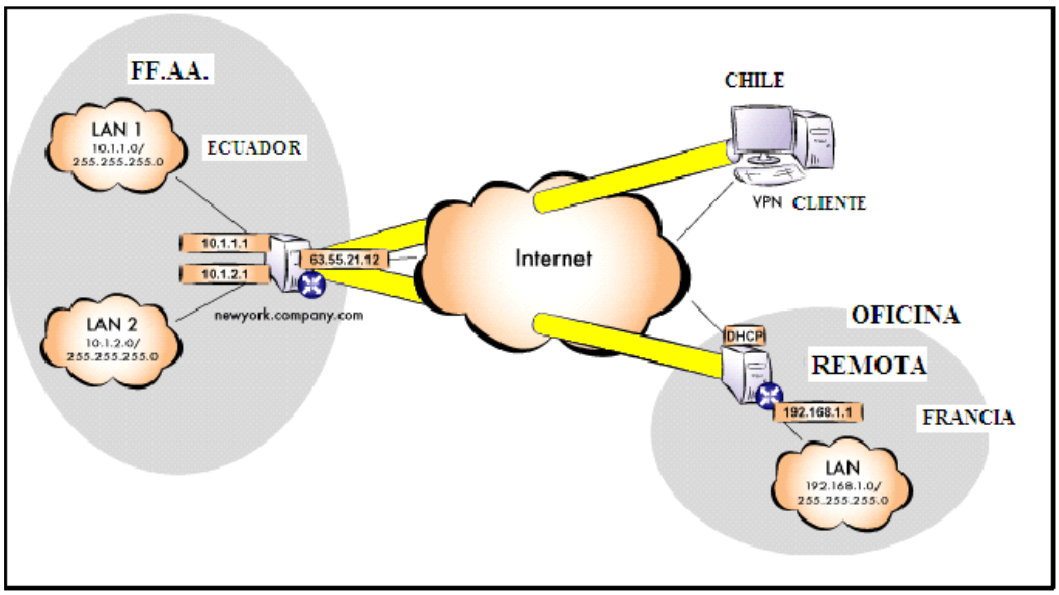

Figura 16: VPN con conexiones diferentes
Elaborado por: El Autor

Esquema de la red VPN a ser ubicadas en diferentes sitios a nivel mundial para integrarse a la red de Fuerzas Armadas.

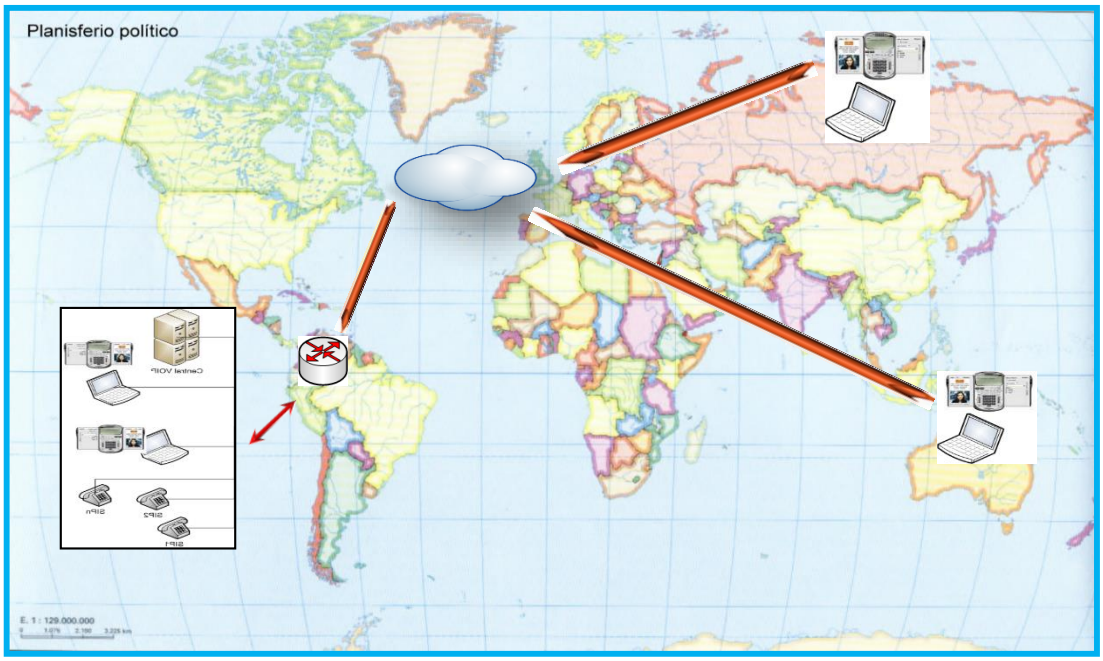

Figura 17: Esquema de la red mundial VPN
Elaborado por: El Autor

IMPLEMENTACIÓN

En el esquema se presenta los servicios de voz y datos a integrarse entre cada uno de los sitios remotos con sus respectivos equipos y aplicaciones necesarias para poder establecer una conexión VPN entre la nube de internet con seguridad encriptado y así poder cumplir con los objetivos planteados en este proyecto.

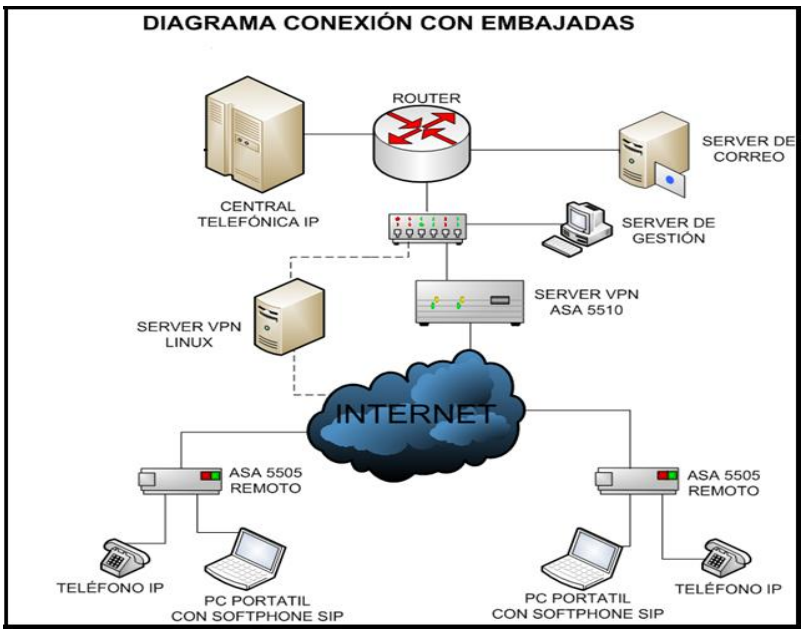

Figura 18: Diagrama de conexión con embajadas
Elaborado por: El Autor

TELÉFONO IP YEALINK SIP-T20P

Figura 19: Teléfono IP
Fuente: (Teléfonos SIP, 2014)

EQUIPO TERMINAL DE DATOS (ETD)

Para la implementación de la red VPN se requiere que el Equipo Terminal de Datos (computador) a utilizar, cumpla con los requerimientos básicos tales como:
Sistema Operativo: Windows XP, Windows 7, Windows 8
Memoria RAM: 512 Mb (mínimo)
Sistema: 32 bits, 64 bits
Procesador: 1.60 GHz. (Cisco ASA, 2014)

SERVIDOR DE CORREO

Uno de los requerimientos de los miembros de la Fuerza Aérea es poder ingresar al servidor del correo Institucional (intranet) a fin de poder transmitir/recibir información de carácter oficial así como también tener acceso a su información confidencial (roles de pago, orden del día, ordenes generales, hoja de vida etc.) del usuario que se encuentra geográficamente distante de su oficina habitual (lugar remoto). (FAE, 2014)

CENTRAL TELEFÓNICA

La Fuerza Aérea dispone de una central telefónica con tecnología digital y tecnología IP, que tiene una gran capacidad de soporte para usuarios finales, con la red virtual se logrará integrar los usuarios remotos a la red telefónica de la FAE y así cumplir con el objetivo planteado en este proyecto. (FAE, 2014)

EQUIPO VPN ASA 5505

Figura 20: Equipo ASA 5505
Fuente: (Firewall Cisco, 2014)

Descripción del producto	Cisco ASA 5505 Firewall Edition
Tipo de dispositivo	Dispositivo de seguridad
RAM instalada (máx.)	256 MB
Memoria flash instalada (máx.)	64 MB Flash
Cantidad de puertos	Switch de 8 puertos 10/100 con 2 puertos power sobre Ethernet.
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Alimentación	CA 120/230 V (50/60 Hz)
Tecnología de conectividad	Cableado
Rendimiento	Capacidad del cortafuegos : 300 Mbps Capacidad de la VPN : 25 Mbps
Capacidad	Peers VPN IP-Sec : 100 Interfaces virtuales (VLAN) : 20
Cantidad de túneles VPN	10 túneles
Algoritmo de cifrado	Triple DES, AES
Cumplimiento de normas	CE, certificado FCC Clase A, CISPR 22 Class A, EN 60950, EN 61000-3-2, UL 1950,VCCI Class A ITE, IEC 60950, EN 61000-3-3, CSA 22.2 No. 950, EN55022 Class A, ACA TS001, AS/NZS 3260, FCC Part 15

Tabla 6: Características del equipo ASA 5505
FUENTE: (ESPECIFICACIONES TÉCNICAS, 2015)

EQUIPO VPN ASA 5510

Figura 21: Equipo ASA 5510
Fuente: (Firewall Cisco, 2014)

Descripción del producto	Cisco ASA 5510 Firewall Edition
Tipo de dispositivo	Dispositivo de seguridad
Dimensiones (A x P x A)	44.5 cm x 33.5 cm x 4.4 cm
RAM instalada (máx.)	256 MB
Memoria flash instalada (máx.)	64 MB Flash
Cantidad de puertos	3
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Características	Protección firewall, asistencia técnica VPN, soporte VLAN
Alimentación	CA 120/230 V (50/60 Hz)
Cantidad de módulos instalados	0 (1)
Factor de forma	Montable en bastidor
Tecnología de conectividad	Cableado
Rendimiento	Capacidad del cortafuegos : 300 Mbps Capacidad de la VPN : 170 Mbps
Capacidad	Peers VPN IP-Sec : 250 Interfaces virtuales (VLAN) : 50
Cantidad de túneles VPN	50 túneles
Algoritmo de cifrado	DES, Triple DES, AES
Total ranuras de expansión (libres)	1 (1) x Ranura de expansión Interfaces 3 x red - Ethernet 10-Base-T/100-Base-TX - RJ-45 1 x gestión - Ethernet 10-Base-T/100-Base-TX - RJ-45 1 x gestión - consola - RJ-45 1 x serial - auxiliar - RJ-45 2 x Hi-Speed USB - 4 PIN USB tipo A
Cumplimiento de normas	CE, certificado FCC Clase A, CISPR 22 Class A, EN 60950, EN 61000-3-2, UL 1950,VCCI Class A ITE, IEC 60950, EN 61000-3-3, CSA 22.2 No. 950, EN55022 Class A,ACA TS001, AS/NZS 3260, FCC Part 15

Tabla 7: Características del equipo ASA 5510
Fuente: (Especificaciones Técnicas, 2015)

LISTA DE COMANDOS BÁSICOS A UTILIZAR EN LOS EQUIPOS ASA

Configure terminal
Copy runnyng-config startup-config.
Enable
Exit
Interface (interfaz)
Nameif
Ping
Reload
Setup
Show dhcpd state
Show flash
Show interface ip brief
Show nameif
Show running-config
Show version
Write erase

INICIALIZACIÓN DEL DISPOSITIVO ASA 5510

a) Acceder a la CLI del equipo Cisco ASA desde el terminal
b) Borrar la configuración por defecto del dispositivo con el comando write erase
c) Reiniciar el dispositivo (reload), y no guardar la configuración luego ingresar enter.
d) Al arrancar el dispositivo, mostrará en la pantalla la invitación a configurarlo utilizando un dialogo interactivo de configuración setup. Se interrumpe el dialogo interactivo respondiendo no. Aparecerá el prompt del modo EXEC usuario.
e) Utilizar el comando enable. Si pide una clave ingresar enter.
f) Verificar la configuración activa del dispositivo con el comando show running-config. (Cisco ASA, 2014)

ELIMINAR EL ARCHIVO DE CONFIGURACIÓN

a) ciscoasa#clear configure all (elimina la configuración activa y reinicia el equipo con una configuración vacía).
b) ciscoasa(config)#configure factory-default (restaura el dispositivo por defecto).

CONFIGURACIÓN DEL EQUIPO ASA 5510

La configuración básica del equipo ASA son tres interfaces conectadas a tres segmentos de red respectivos. El segmento de la red de internet está conectado con la interfaz del Ethernet 0/0 y etiquetado como output con nivel de seguridad 0. La red interna se conecta con Ethernet 0/1 y etiquetado como input con nivel de seguridad 100. El segmento DMZ, donde se ubica el servidor web se conecta con Ethernet 0/2 y se etiqueta como DMZ con nivel de seguridad 50.

La configuración de la interfaz y las direcciones IP:

```
Ciscoasa(config)#interface Ethernet0/0
 asa(config-if)#nameif outside
 asa(config-if)#ip address 192.160.100.100 255.255.0.0
 asa(config-if)#no shutdown
 asa(config-if)#exit

Ciscoasa(config)#interface Ethernet0/1
 asa(config-if)#nameif inside
 asa(config-if)#security-level 50
 asa(config-if)#ip address 192.160.0.1 255.255.0.0
 asa(config-if)#no shutdown
 asa(config-if)#exit

Ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 192.160.100.1
```

Se observa que la interfaz interior del equipo ASA está fijada con la dirección IP de 192.160.0.1, es el default gateway para los host internos. La interfaz externa ASA se configura con la dirección IP obtenida del ISP proveedor de servicio de internet. Si se utiliza el DHCP esto se proporciona de forma automática. La interfaz de la zona desmilitarizada se configura con la dirección IP de 192.160.1.1, y es el de fábrica gateway para los hosts en este segmento de la red desmilitarizada.

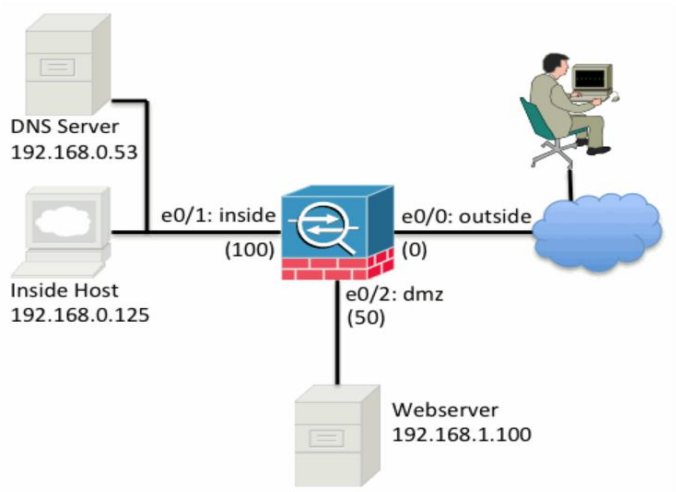

Figura 22: Funcionalidad del equipo ASA
Fuente: (Cisco ASA, 2014)

ADMINISTRACIÓN DEL EQUIPO ASA 5510

Para la administración del equipo ASA modelo 5510 a utilizarse en este proyecto; Una vez configurado el hardware del equipo, se accede desde el cliente de la interfaz INSIDE con la URL https: 192.160.0.1/admin, que es una dirección por defecto del ASA.

Se asigna un usuario con todos los permisos para la administración en modo privilegiado aplicando el siguiente comando:

Ciscoasa(config)# usuario admin clave admin privilege

Existen protocolos y aplicaciones estándar para la entrada en sistemas remotos tales como Telnet, Putty, en donde el administrador puede acceder al sistema desde cualquier equipo terminal.

Con éste equipo y de acuerdo a la configuración se tiene la capacidad de crear hasta 50 “Túneles” y enlazar un máximo de 250 usuarios VPN IP-sec.

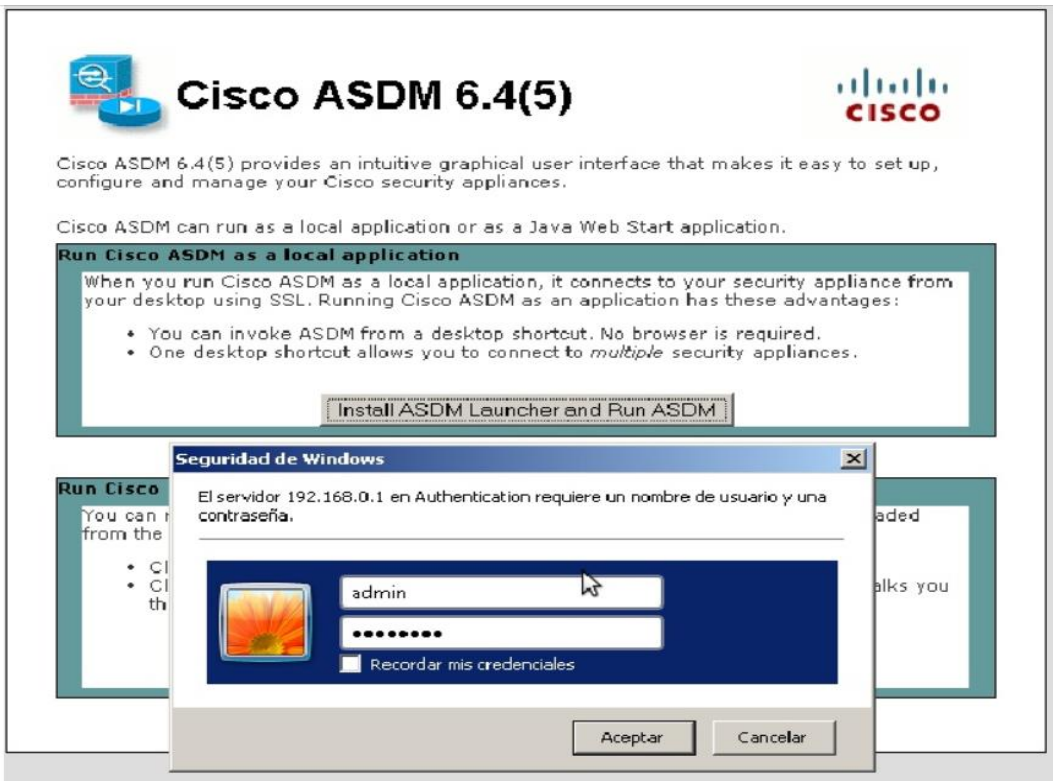

Figura 23: Administrador equipo ASA
Elaborado por: El Autor

En la ventana que aparece dar clic en “Install ASDM launcher and Run ASDM” en donde aparece una nueva ventana de dialogo “seguridad de Windows”, ingresar en user-name la palabra “admin” y la clave “admin” que vienen dado por defecto, y posterior dar clic en “aceptar”.

Figura 24: Configuración equipo ASA
Elaborado por: El Autor

Luego nos pedirá la dirección IP del Firewall ASA y de nuevo las credenciales de usuario.

Para proceder a cargar la interfaz gráfica de administración del firewall ASA y se presenta la siguiente pantalla:

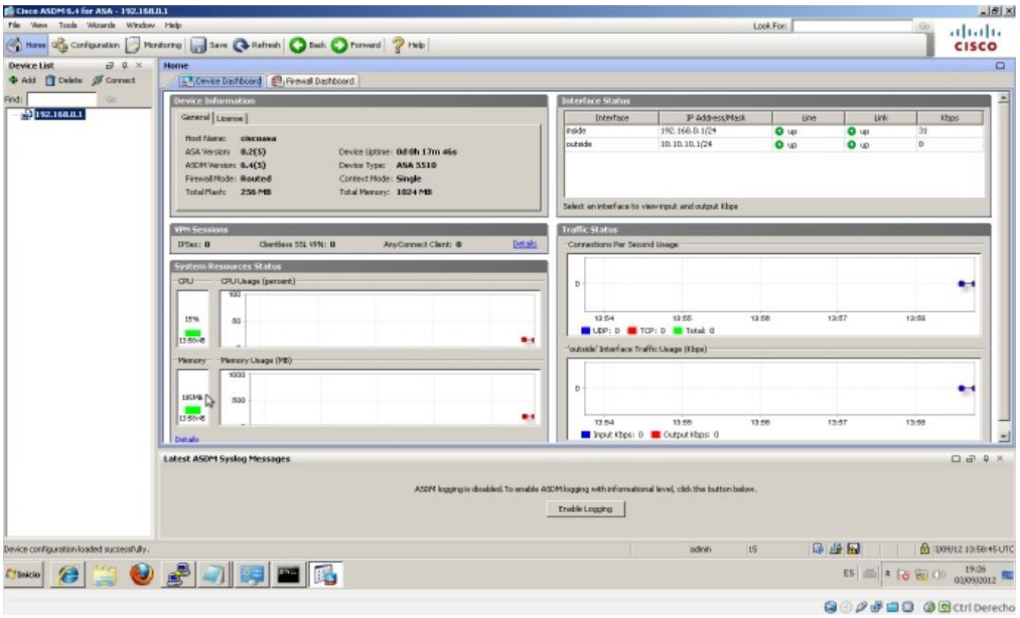

Figura 25: Interfaz Gráfica equipo ASA
Elaborado por: El Autor

Una vez que se encuentra cargado la aplicación se procede a iniciar el asistente de configuración de la VPN ubicando el cursor en la pestaña “wizards” donde se despliegan cinco ítems en el cual se selecciona “IP-sec VPN wizard…”

Figura 26: Configuración IP-sec equipo ASA
Elaborado por: El Autor

Este asistente se usa para configurar un nuevo túnel sitio a sitio VPN o un nuevo acceso a un punto remoto del túnel VPN. Un túnel con dos dispositivos ASA es llamado sitio a sitio y enlaza una comunicación bidireccional, uniendo dos redes LAN desde sitios distantes; El Remote Access utiliza un solo dispositivo ASA y este tipo de técnica enlaza una comunicación entre una red local con un dispositivo móvil, laptop ubicados en sitios distantes que tenga acceso a la ISP.

Se selecciona “Remote Access” y la interface del túnel VPN es “out-side” dando un visto en la habilitación del IP-sec, para continuar con el icono siguiente.

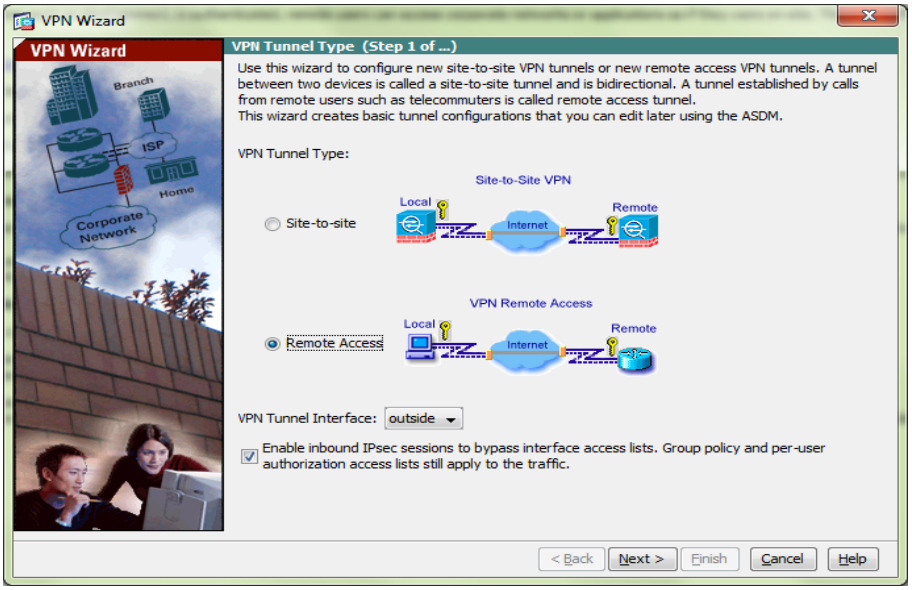

Figura 27: Config. Remote Acces equipo ASA
Elaborado por: El Autor

Aparece una ventana Remote Access Client, donde se puede seleccionar entre varios tipos de túneles VPN, se selecciona el Cisco VPN Client, reléase 3.x or higher para poder realizar la conexión con el dispositivo ASA 5510.

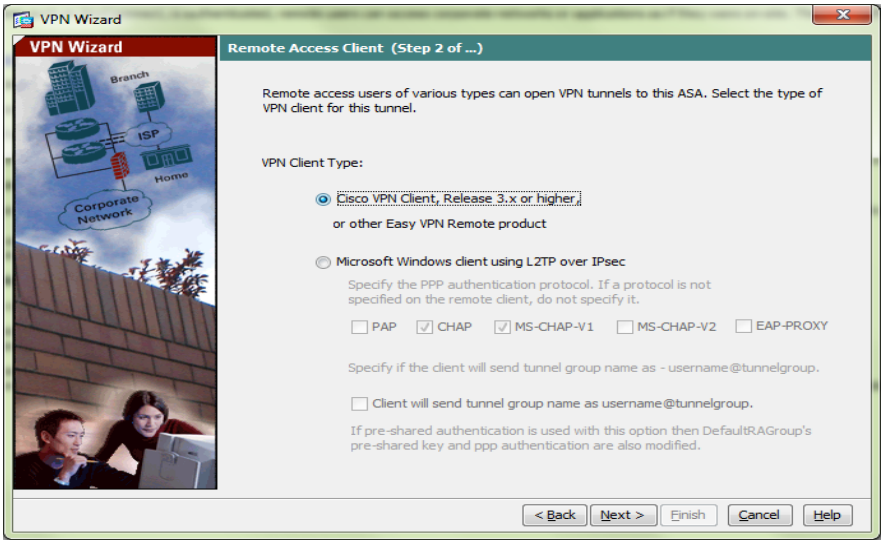

Figura 28: Config. VPN Client equipo ASA
Elaborado por: El Autor

MÉTODO DE AUTENTICACIÓN DEL CLIENTE VPN Y DESIGNACIÓN DEL GRUPO DEL TÚNEL

El equipo ASA 5510 permite que use el túnel en un grupo de acceso remoto basado en los parámetros de conexión común y la configuración de una clave común entre el sitio remoto y la estación LAN. En este caso la clave compartida se ha asignado 123456 y el nombre del grupo del túnel es prueba. Y continúa con la siguiente pestaña.

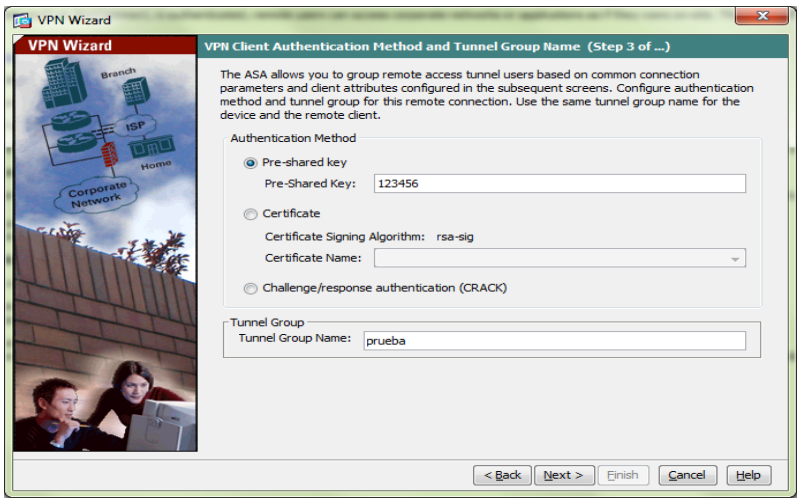

Figura 29: Nombre del Túnel y clave común
Elaborado por: El Autor

En este paso se adiciona una cuenta de usuario y las políticas de la VPN tales como, políticas de grupo, protocolos de túneles, filtros IP-v4, filtros IP-v6, y lo más importante selecciona el grupo VPN a pertenecer.

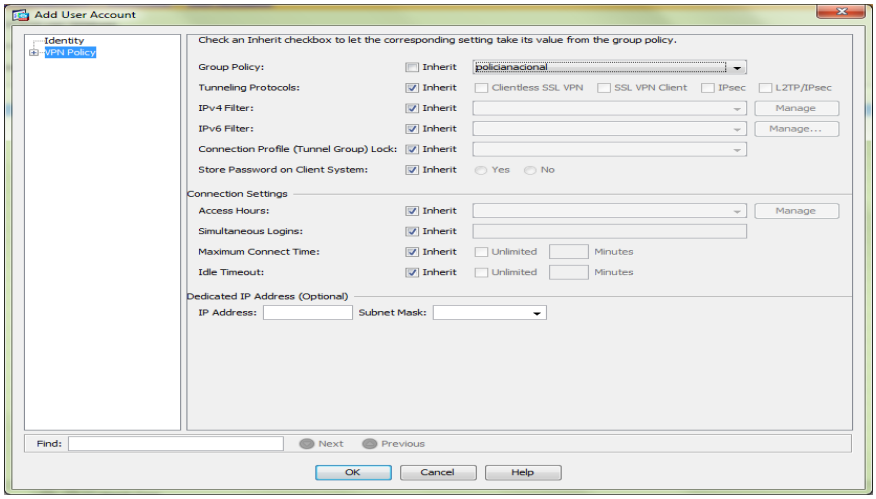

Figura 30: Config. Política del grupo VPN
Elaborado por: El Autor

Se concluye con la configuración del equipo ASA 5510 ingresados todos los parámetros en la base de datos del dispositivo, donde se observa el nombre de usuario creado, el nivel de privilegio, restricciones de acceso, el grupo de la VPN. Se encuentra listo para asignar usuarios VPN.

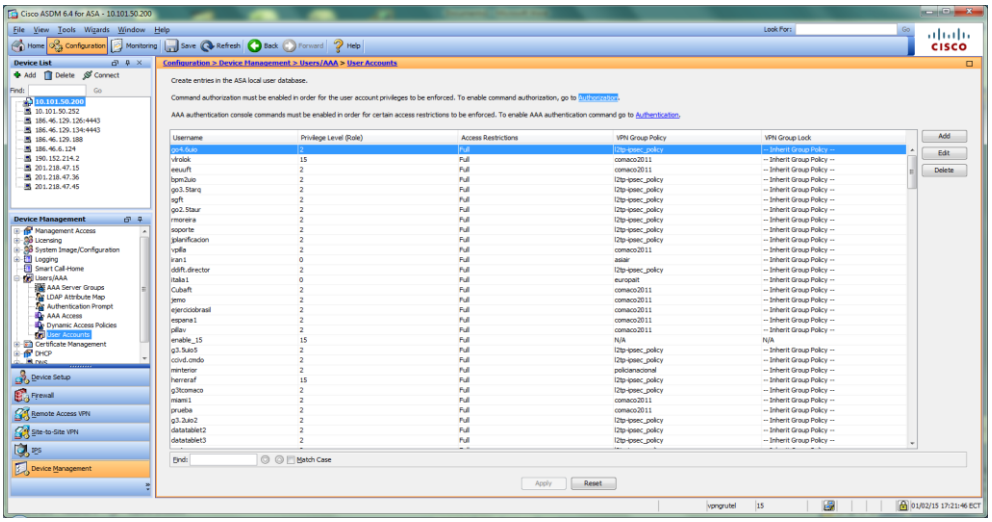

Figura 31: Conclusión de la Config. Equipo ASA
Elaborado por: El Autor

Se presenta la visualización del detalle de la conexión, se observa la dirección de IP pública y la dirección de la IP asignada con sus respectivos protocolos de encriptación, la duración del tiempo conectado y la cantidad de paquetes tanto transmitidos como enviados.

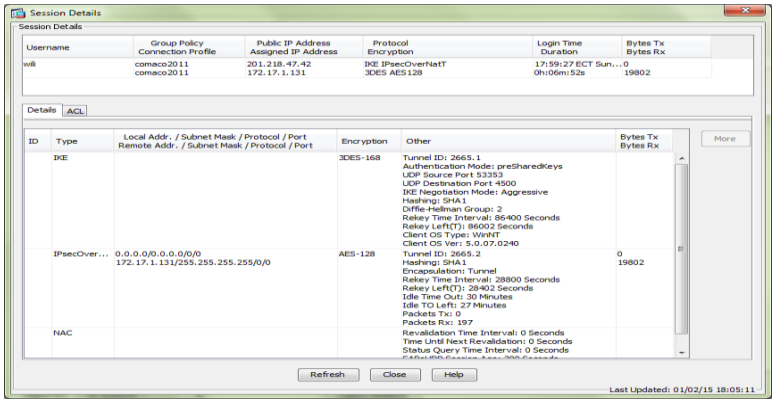

Figura 32: Detalle de la conexión VPN
Elaborado por: El Autor

A continuación se presenta la configuración y creación de las cuentas del usuario remoto, adicionando un nuevo usuario autenticándolo dentro de la base de datos del equipo ASA, en esta parte se crea un usuario y un password.

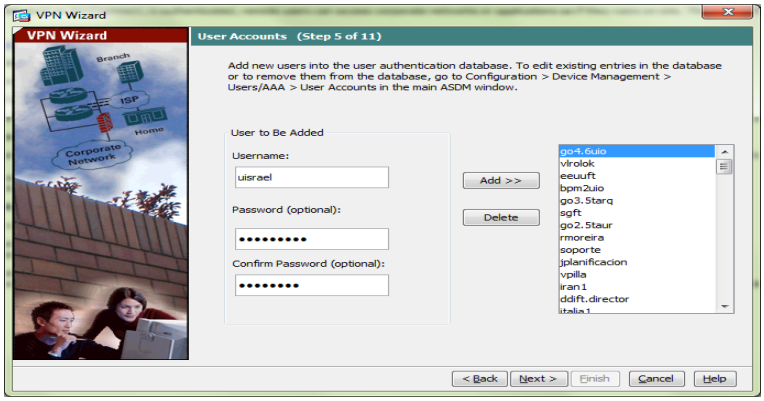

Figura 33: Config. De cuenta usuario remoto
Elaborado por: El Autor

Como se observa en este caso el grupo del túnel aparece como “prueba” y se procede a direccionar hacia los DNS de los servidores primarios y secundarios, además se requiere el nombre del dominio a enlazarse.

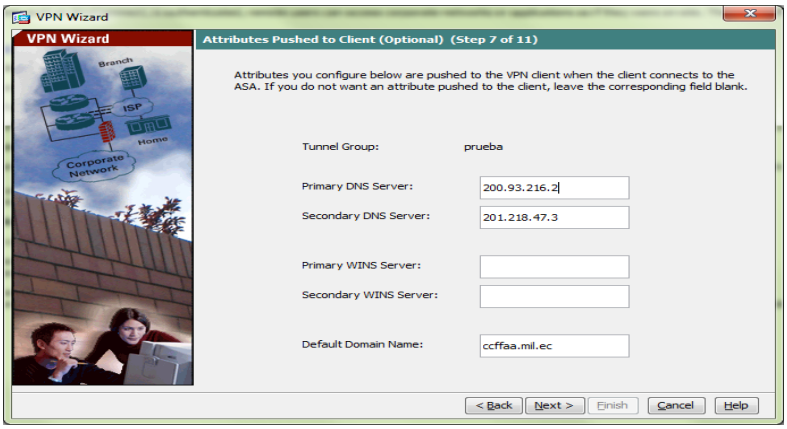

Figura 34: Direccionamiento de los DNS
Elaborado por: El Autor

La interface “Inside” permite direccionar la red LAN hacia la IP publica para lograr realizar el efecto enlace a través del túnel.

En esta parte de la configuración se puede habilitar un “Split Tunneling” para el usuario remoto que tiene como ventaja a más de tener la conexión VPN, permite mantener su conexión ISP.

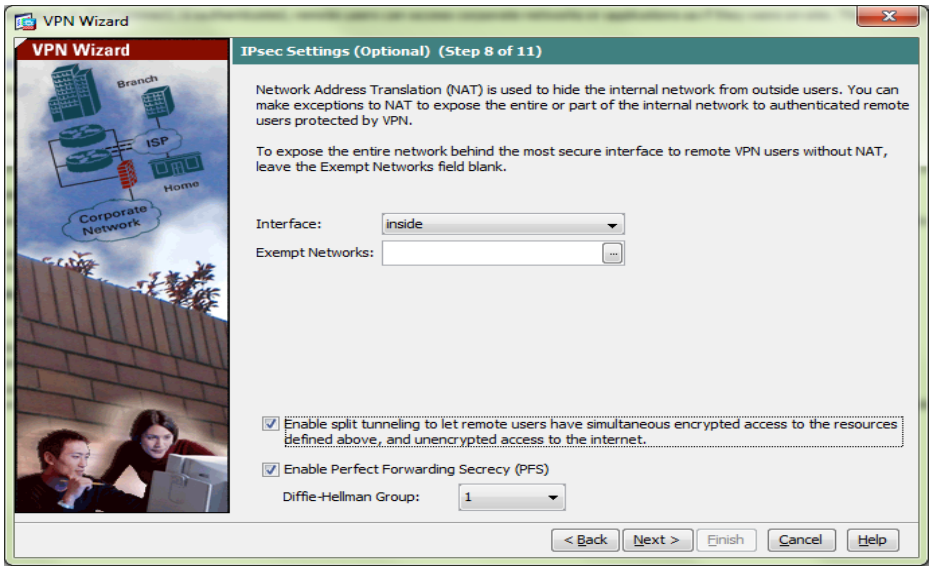

Figura 35: Config. Interface equipo ASA
Elaborado por: El Autor

Se ha creado la configuración de la red LAN con un equipo en el sitio remoto, aparece un resumen de la configuración realizada y almacenada en la base de datos del equipo ASA 55100. Para su correcto funcionamiento.

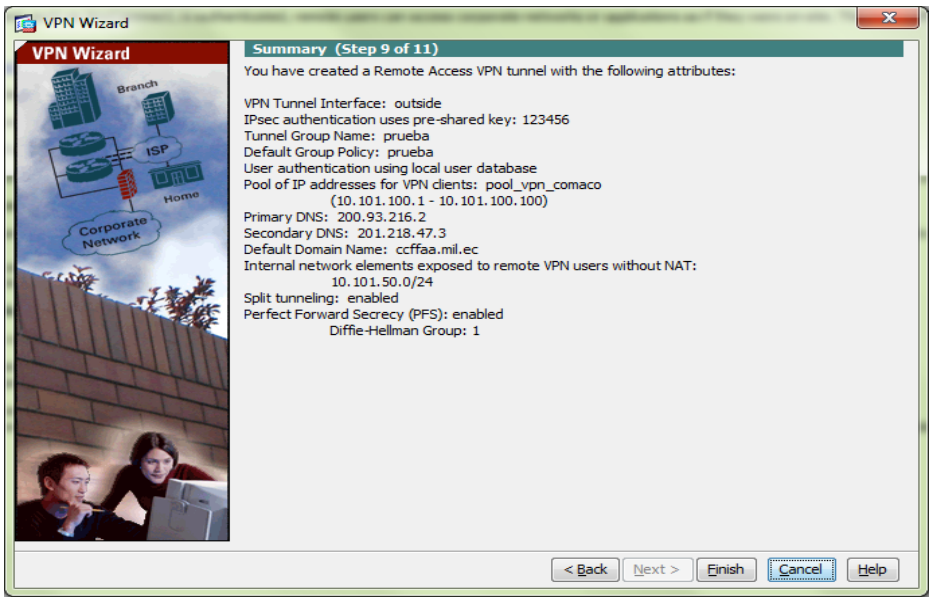

Figura 36: Resumen de Config. Realizada
Elaborado por: El Autor

Como ya se tiene configurado la aplicación Site-to-Remote en el equipo ASA, ahora se procede a instalar el software “VPN client” que existen versiones para 32 y 64 bits y esto permitirá la conexión entre el equipo remoto y la estacion LAN.

El proceso de la insatalacion es dando doble clic en el setup del aplicativo en la cual aparece el siguiente cuadro de dialogo:

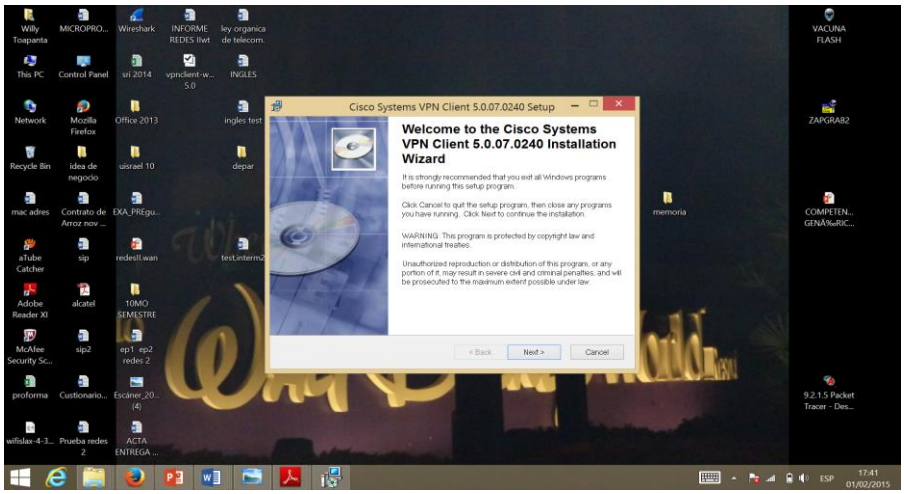

Figura 37: Instalación del software VPN Client
Elaborado por: El Autor

Se acepta las políticas del software a instalarse y se continúa con el proceso de instalación.

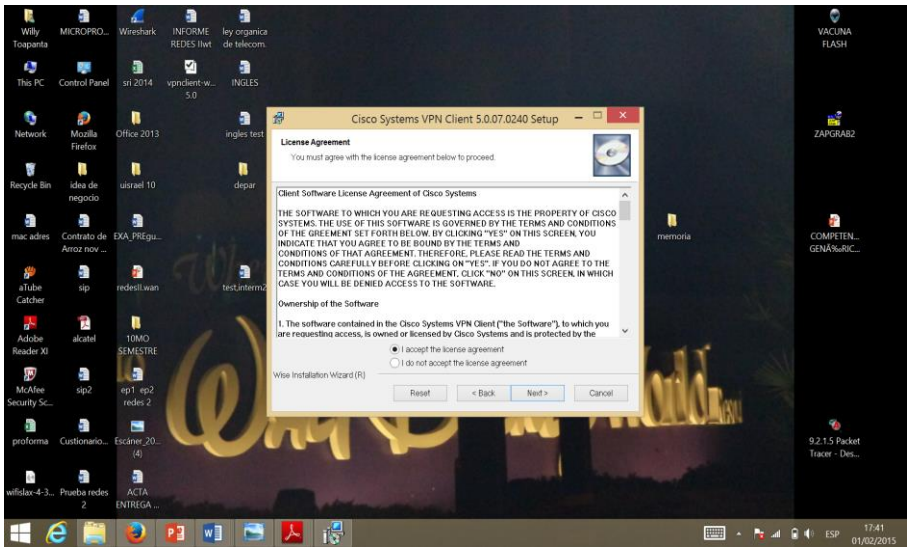

Figura 38: Políticas del sistema
Elaborado por: El Autor

En este paso se designa la ubicación de la aplicación a instalarse que por lo general se instala en el disco “C”

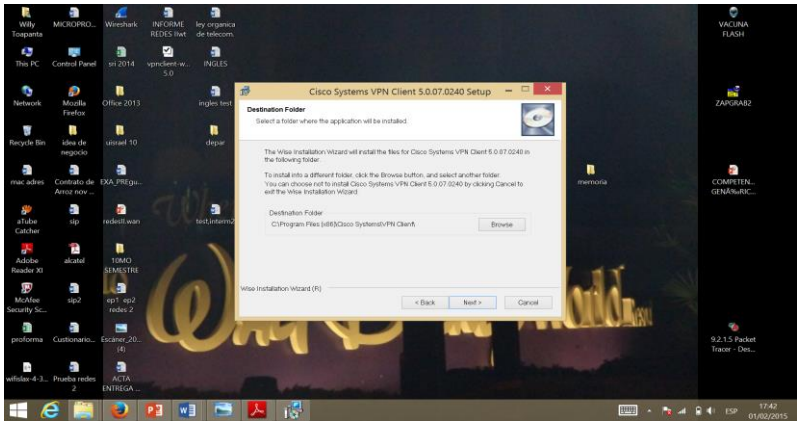

Figura 39: Destinación de la aplicación a instalarse
Elaborado por: El Autor

Una vez que acepta el proceso de insatalación del aplicativo comienza a instalarse en la computadora, se debe esperar unos pocos minutos para que concluya con la instalcion.

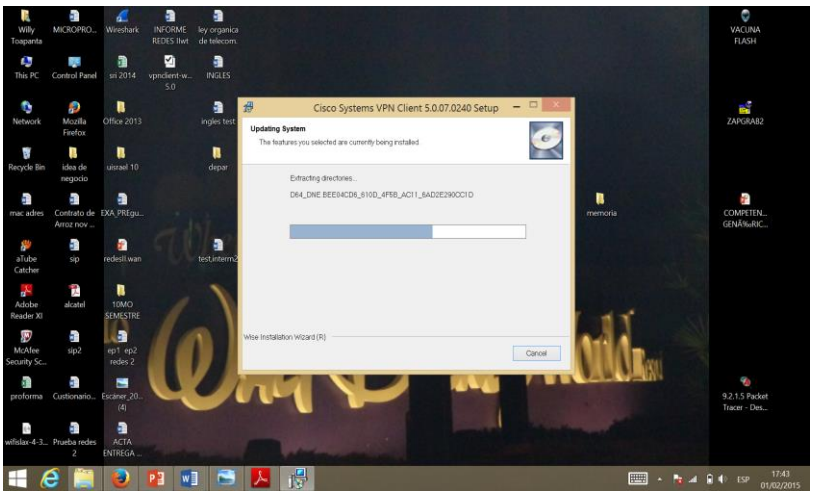

Figura 40: Progreso de instalación
Elaborado por: El Autor

La aplicación VPN Client ha sido correctamente instalada en el equipo remoto a utilizar.

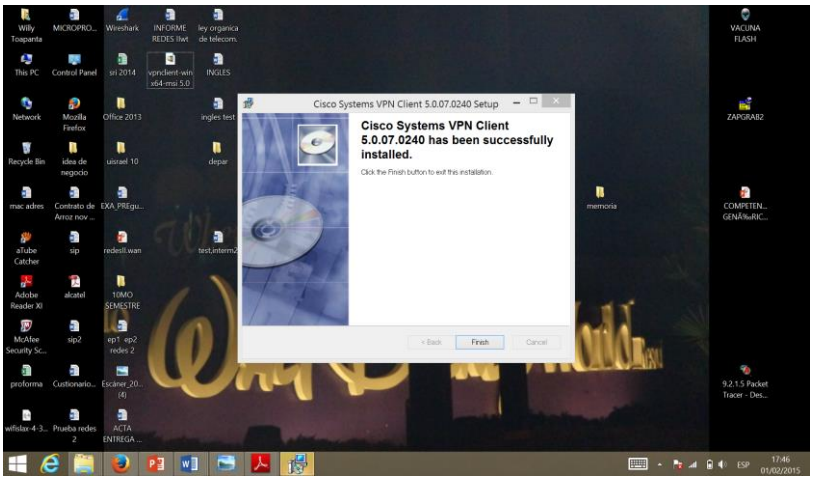

Figura 41: Aplicación correctamente instalada
Elaborado por: El Autor

Una vez instalada la aplicación VPN Client se observa el estado de la conexión que se encuentre desconectada, para el efecto el sistema pide la autenticación del usuario, ingresando la dirección del host (equipo ASA Out-Side) el nombre del grupo y la clave del direccionamiento a ejecutarse.

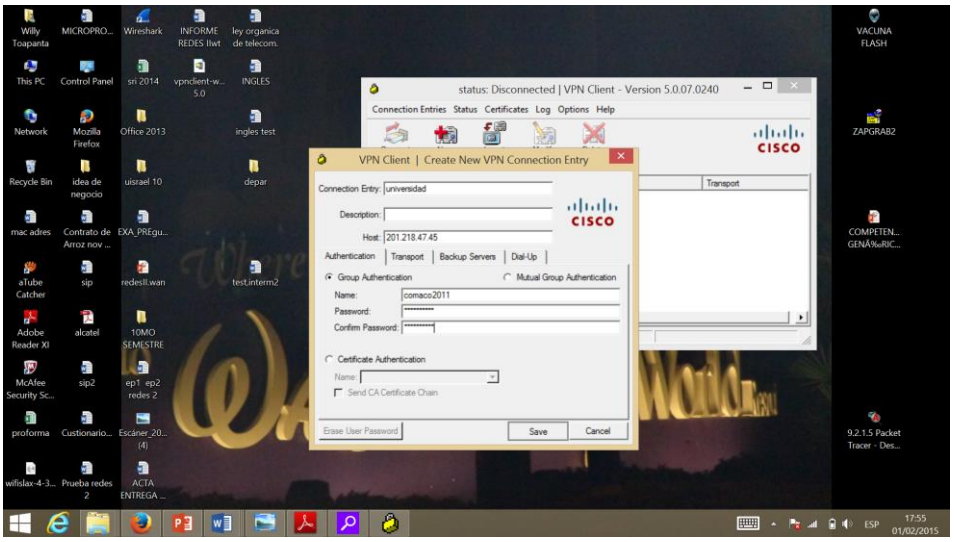

Figura 42: Autenticación del usuario
Elaborado por: El Autor

Hasta el momento el estado del enlace está desconectado, se requiere autenticar el usuario a la red RVP con el user-name y password del servidor, esto se puede visualizar también en la parte inferior derecha se encuentra un icono de un candado de color amarillo abierto.

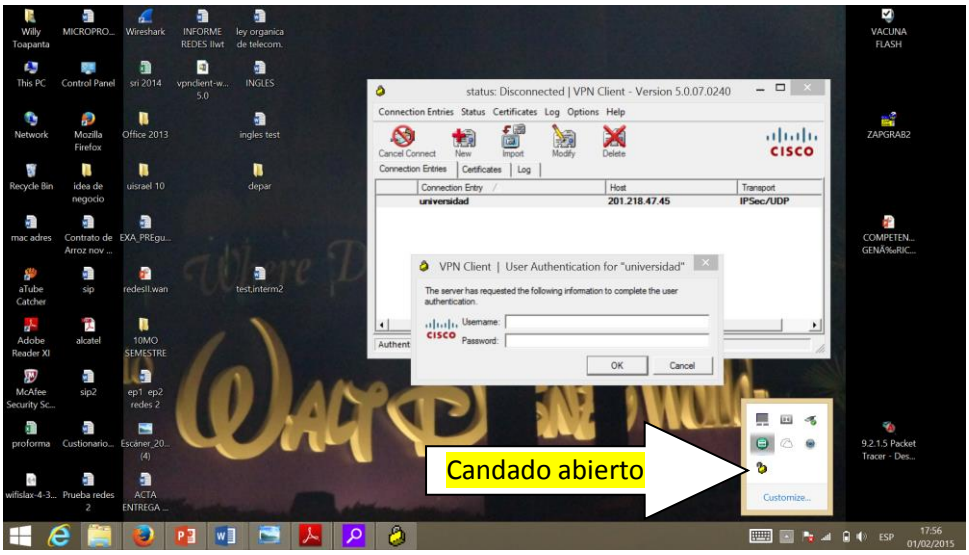

Figura 43: Ingreso User-name y Password
Elaborado por: El Autor

Una vez autenticado los dispositivos el candado amarillo se cierra, indicando que el túnel se encuentra activado.

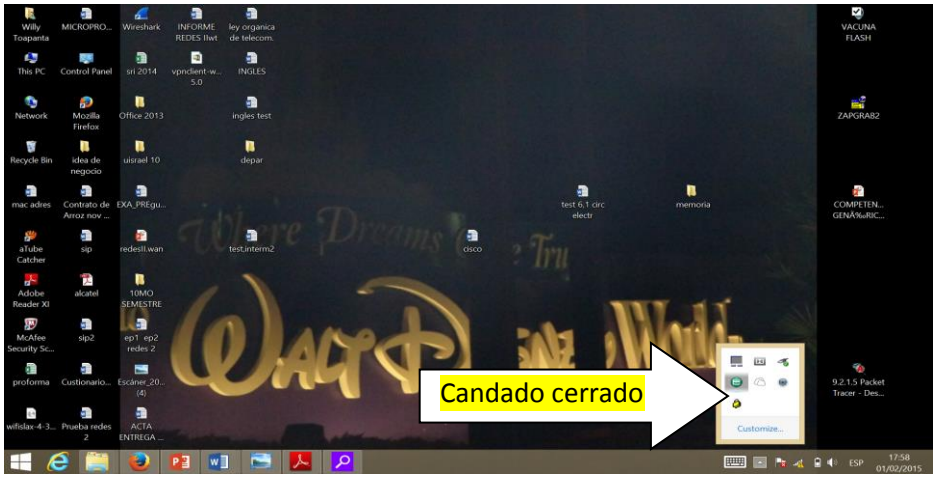

Figura 44: Activación del Túnel
Elaborado por: El Autor

Ingresando al sistema por medio del cmd.exe e indicando el comando “ip-config” se puede visualizar la dirección IP-v4 a la que ha sido asignado el equipo remoto junto con la máscara de subred y la dirección del Gateway.

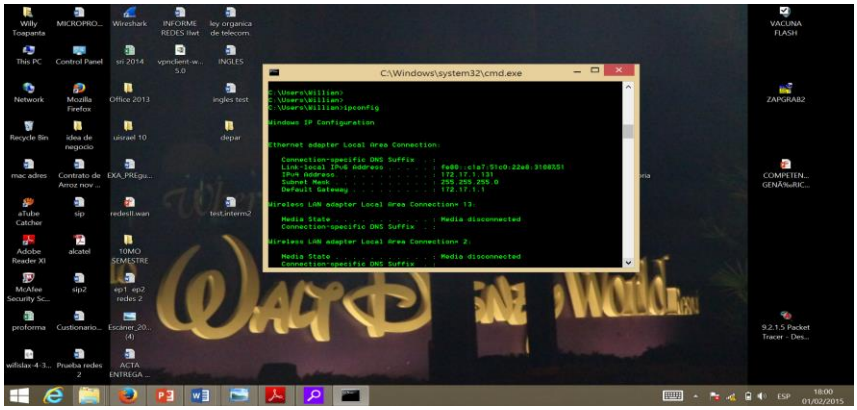

Figura 45: Comprobando enlace con Gateway
Elaborado por: El Autor

SOFTPHONE SIP

Vo-IP. Es la transmisión de Voz sobre un protocolo de Internet, es la manera más moderna de generar comunicación con la persona que se desee en cualquier parte del mundo evitando tener un contrato, factura u obligación por brindar servicio de comunicacion. Se consigue gracias a los servicios actuales de Vo-ip, utilizando una plataforma de internet desde un computador, Un Wi-fi o Router portátil que se conecta a su enlace de Internet al cual se conecta un teléfono fijo (aparato) para realizar sus llamadas.

Ahora se necesita tener un teléfono IP o una aplicación que emule el teléfono convencional y se logre mantener una comunicación telefónica a través del enlace VPN.

Esta aplicación utilizada es el software X-Lite que se instala en el equipo remoto del enlace VPN.

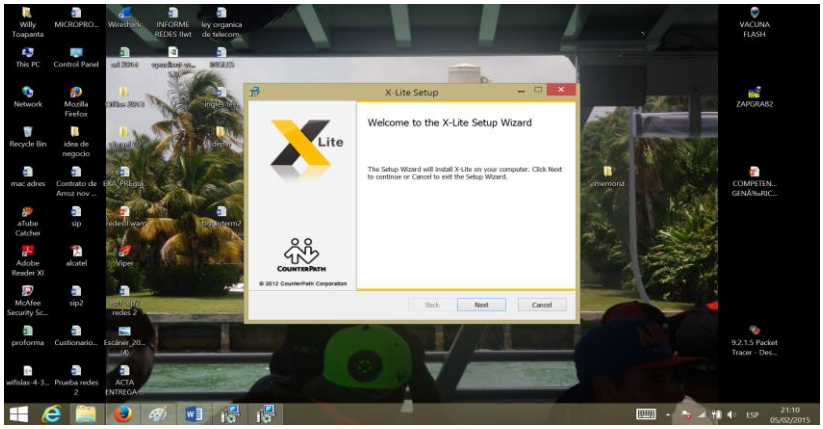

Figura 46: Instalación Softphone
Elaborado por: El Autor

Una vez que la aplicación está ejecutándose requiere que se acepten las políticas de instalación del software X-lite del usuario final, para continuar con el proceso de instalación.

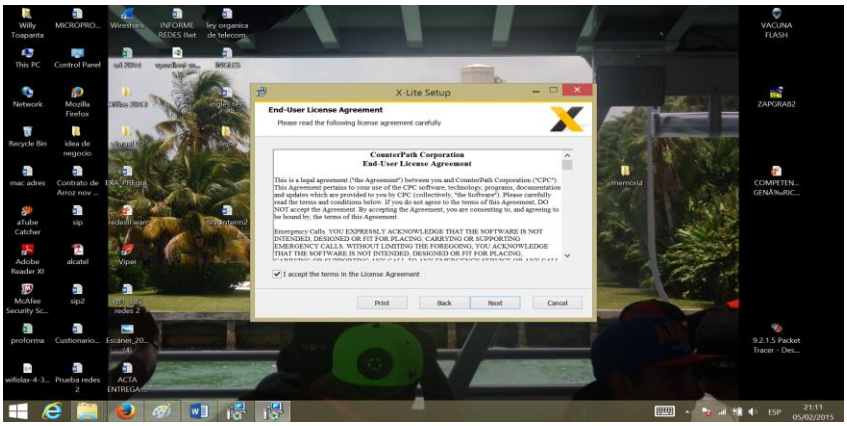

Figura 47: Aceptación de las políticas X-lite
Elaborado por: El Autor

En este paso se designa la ubicación de la aplicación a instalarse que por lo general se instala en el disco “C:\Program Files\” luego se presiona el icono “next”.

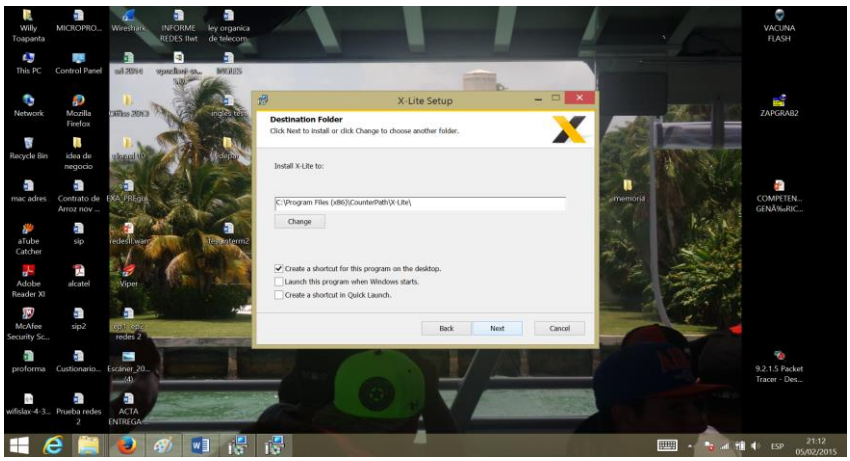

Figura 48: Ubicación del software X-lite
Elaborado por: El Autor

Una vez configurado el destino de la ubicación del software, se encuentra listo para la instalación del X-lite dando un clic en “Install” para empezar la instalación, puede dar un clic en “Back” para regresar y hacer cambios en la configuración de destino o clic en “Cancel” para abandonar y salir de la instalación.

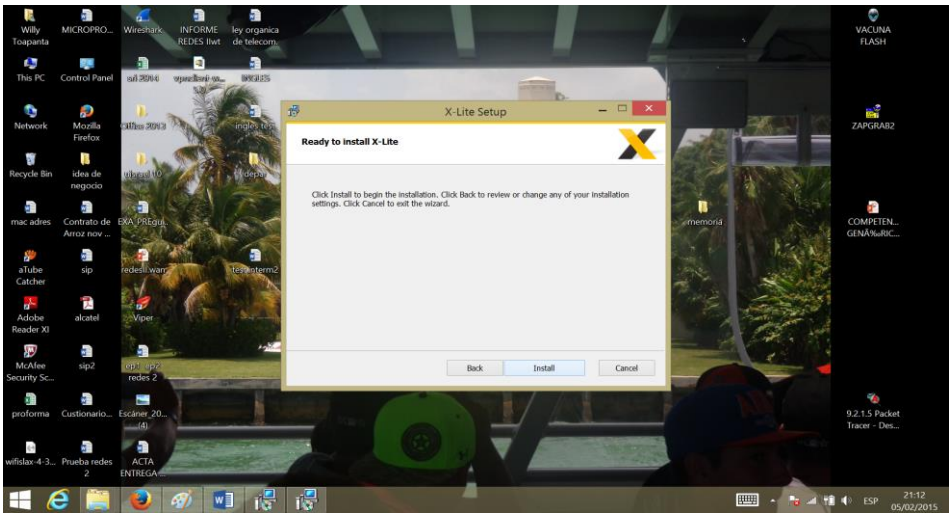

Figura 49: Listo para instalar X-lite
Elaborado por: El Autor

Una vez que acepta el proceso de instalación del aplicativo, comienza a instalarse en la computadora, se debe esperar unos pocos minutos para que concluya con la instalacion.

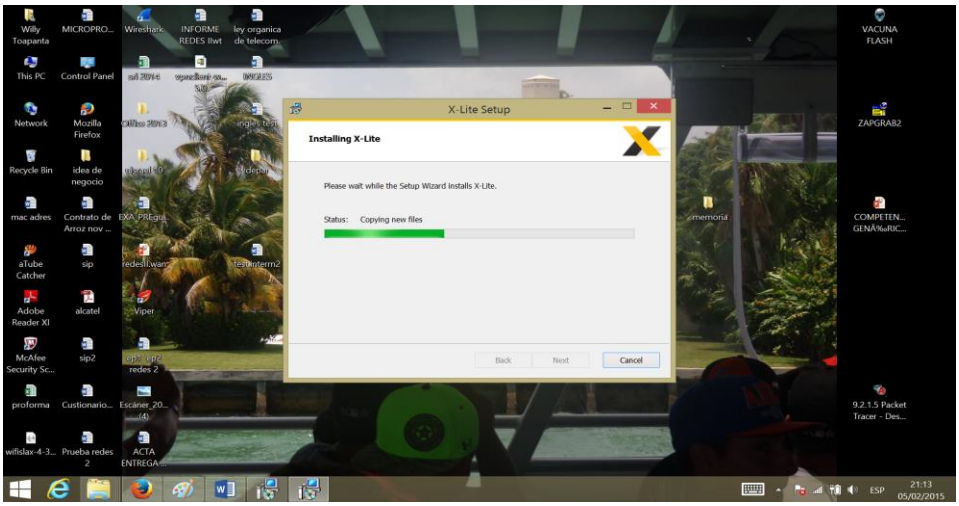

Figura 50: Proceso de instalación del software X-lite
Elaborado por: El Autor

Luego de correr el aplicativo, aparece una pantalla que le indica que el software X-lite ha sido instalado exitosamente en la computadora y así poder realizar una comunicación Vo-IP a través de un túnel con seguridad encriptado. Se recomienda reiniciar el computador para que la aplicación desarrolle correctamente.

CONCLUSIONES

La selección del firewall ASA 5505 de Cisco, es el equipo ideal para efectuar el enlace de Red Virtual Privada, cumpliendo las normas que requiere la IEEE, logrando realizar comunicaciones con seguridad criptográfica entre la Comandancia General de la Fuerza Aérea y las Agregadurías Militares que se encuentran ubicadas geográficamente distantes.

La instalación y configuración de aplicaciones VPN client y Softphone Zoiper en los equipos informáticos terminales, son herramientas necesarias de comunicación entre estaciones remotas, logrando emular un teléfono convencional desde el computador.

La integración de la Red Virtual Privada con la red MODE (voz y datos) de las Fuerzas Armadas del Ecuador, es fundamental con el fin de aprovechar su gran infraestructura para poder ingresar a la Intranet FAE y a la Central Telefónica de las Fuerzas Armadas desde una estación remota.

Se comprobó el enlace de comunicación VPN mediante pruebas de campo, entre dos estaciones remotas, logrando integrar a la red de voz y datos de las Fuerzas Armadas del Ecuador de manera segura.

RECOMENDACIONES

Mantener un buen ancho de banda para la óptima transmisión de datos en la nube de internet a través de los equipos firewall ASA.

Contar con licencias necesarias de las aplicaciones que se requieren para la conexión del enlace VPN.

Socializar este tipo de tecnología a empresas que desconocen del sistema y así poder mejorar sus medios de comunicación, implementando y mejorando los servicios que presenta las VPN.

Cuando una empresa requiera de altas velocidades de comunicación no se recomienda la instalación de una VPN, porque no obtendrá buenos resultados en transmisión/recepción debido al proceso de encapsulamiento y encriptación de la información que realiza la tecnología.

BIBLIOGRAFÍA

Cisco ASA, 5. (27 de diciembre de 2014). *Cisco*. Obtenido de www.cisco.com/web/LA/soluciones/la/vpn/index.html

Enciclopedia, e. (2013). Colombia: Larousse.

Espallagas, J., Limonche, F., & Robles, P. (1995). *El libro del teléfono.* España: Progensa.

Especificaciones Técnicas, A. (28 de enero de 2015). *ASA 5510*. Obtenido de http://es.scribd.com/doc/95704345/Especificaciones-Tecnicas-Firewall-Cisco-ASA-5510#scribd

FAE, M. (Septiembre de 2014). Comunicaciones VPN. (W. Toapanta, Entrevistador)

Firewall Cisco, A. (2014). *ASA 5510*. Obtenido de http://es.scribd.com/doc/95704345/Especificaciones-Tecnicas-Firewall-Cisco-ASA-5510#scribd

García Alfaro, J. (2004). *Ataques Contra Redes TCP/IP* (primera ed.). Barcelona, España: Eureca media. Recuperado el 12 de Febrero de 2015

Gonzales, G. (19 de diciembre de 2014). *Redes Virtuales Privadas*. Obtenido de http://blogthinkbig.com/que-es-un-vpn/

Mason, A. G. (2002). *Cisco secure Virtual Private Network*. Obtenido de http://www.cisco.com/web/LA/soluciones/la/vpn/index.html

Palacios, M. (2007). Guía de proyectos I. En P. Magdalena, *Guía de proyectos I* (págs. 23-28). Quito.

Red privada virtual. (20 de noviembre de 2014). *Red Privada Virtual*. Obtenido de http://es.wikipedia.org/wiki/Red_privada_virtual

Technologies, F. n. (2013). *Callcular la muestra correcta.* San Luis, California, EE.UU.: Feedback.

Teléfonos SIP. (2014). *Teléfonos SIP*. Obtenido de http://www.yealink.com/

Textoscientíficos. (03 de 11 de 2010). *Textoscientíficos*. Obtenido de http://www.textoscientificos.com/redes/redes-virtuales

Toapanta, W. (2014).

Vivanco , M. P. (octubre de 2013). *academia.edu*. Obtenido de http://www.academia.edu/417570/Desarrollo_de_una_Virtual_Private_Network_VPN_para_la_interconexi%C3%B3n_de_una_empresa_con_sucursales_en_provincias

VPN. (29 de abril de 2014). *Virtual Private Network*. Obtenido de http://www.uv.es/siuv/cas/anuncios/xarxa/vpn.wiki

wikipedia. (11 de febrero de 2015). *wikipedia*. Obtenido de http://es.wikipedia.org/w/index.php?title=Red_privada_virtual&action=history

Yealink. (2014). *yealink.com*. Obtenido de http://www.yealink.com/

ANEXOS

ANÁLISIS DE COSTOS DEL PROYECTO

Se considera un número indeterminado de estaciones remotas a implementarse por tratarse de información calificada.

CANT.	EQUIPO	DESCRIPCIÓN	COSTO
01	ASA 5510	Es un equipo cisco utilizado para configurar como Servidor de VPN con capacidad para 250 conexiones	3.000
15	ASA 5505	Serán instalados en los sitios remotos y configurados como clientes remotos.	15.000
01	SERVIDOR VPN	Es una aplicación bajo Linux, se utilizará como back-up del ASA 5510	1.000
01	ROUTER	Integrará la Central telefónica IP con la RED de Internet y Datos.	3.000
01	SWITCH	Segmenta VLAN´s en el Nodo Central.	2.000
15	LICENCIAS SIP	Se utilizará con equipos telefónicos IP y Softphone libre que serán instalados en Pc Portátiles.	1.500
15	TELÉFONOS IP	Equipos fijos que irán en las Agregadurías.	3.000
TOTAL			28.500

ANÁLISIS DE COSTO/BENEFICIO CON DOS AGREGADURÍAS.

Las cantidades indicadas están relacionadas con un consumo promedio mensual por cada Agregaduría.

ORIGEN	DESTINO	NÚMERO LLAMADAS DIARIAS	PROMEDIO (MIN X LLAMADA)	COSTO LLAMADA (X MIN)	GASTO MENSUAL
USANDO TELEFONÍA TRADICIONAL (SITUACIÓN ACTUAL)					
Francia	Ecuador	8	3	0,75 usd	540
Chile	Ecuador	8	3	0,50 usd	360
USANDO VPN					
Francia	Ecuador	8	3	0,06 usd	44
Chile	Ecuador	8	3	0,04 usd	29
Ahorro anual Francia					5.952
Ahorro anual Chile					3.972

CONFIGURACIÓN NAT PARA PERMITIR QUE LOS HOSTS SALGAN A INTERNET

El primer paso a realizar es configurar las reglas NAT (network address translation) traducción de direcciones de red, que permiten los hosts en el interior y segmentos del dmz a conectar con Internet. Porque estos hosts están utilizando los IP Address privados, se necesita traducirlos algo que es routable en Internet. En este caso se traduce el direccionamiento de modo que parezcan la dirección IP de la interfaz exterior ASA. Si la IP externa cambia con frecuencia (quizás debido al DHCP) ésta es la manera más directa de configurar esto.

Para configurar la NAT, se necesita crear un objeto de red que represente la subred interior así como uno que represente la subred del dmz. En cada uno de estos objetos, se configura una regla nacional dinámica que contenga a estos clientes como el paso de sus interfaces respectivas a la interfaz exterior:

```
object network inside-subnet
 subnet 192.160.0.0 255.255.0.0
 nat (outside, inside) interface dinámica

object network dmz-subnet
 subnet 192.160.1.0 255.255.0.0
 nat (outside, dmz) interface dinámica
```

Se observa la configuración corriente en este momento, la definición del objeto está partida en dos partes de la salida. La primera parte indica solamente cuál está en el objeto (host/subred, dirección IP, etc.), mientras que la segunda sección muestra que regla NAT atada a ese objeto.

Cuando los hosts que corresponden con la travesía de 192.160.0.0/24 subredes de la interfaz interior a la interfaz exterior, se quieren traducirlos dinámicamente a la interfaz exterior.

CONFIGURACIÓN NAT PARA ACCEDER EL WEB SERVER DE INTERNET

Una vez que los hosts en las interfaces interiores y del dmz pueden salir a Internet, se necesita modificar la configuración de modo que los usuarios en Internet puedan acceder nuestro web server en el puerto TCP 80.

La configuración es de modo que la gente en Internet pueda conectar con otra dirección IP que el ISP proporcionó, una dirección IP adicional *poseemos*. Se utiliza la dirección 198.51.100.101. Con esta configuración, los usuarios en Internet podrán alcanzar el web server del dmz accediendo 198.51.100.101 en el puerto TCP 80.

Se utiliza el objeto NAT para esta tarea, y el ASA traducirá el puerto TCP 80 en el web server (192.160.1.100) para parecer 198.51.100.101 en el puerto TCP 80 en el exterior.

```
object network webserver-external-ip
 host 198.51.100.101

object network webserver
 host 192.160.1.100
 nat (outside, dmz) static webserver-external-ip service tcp www.
```

Cuando un host que corresponde con a la dirección IP 192.160.1.100 en los segmentos del dmz establece una conexión originada del puerto TCP 80 (WWW) y esa conexión sale la interfaz exterior, eso se traduce para ser el puerto TCP 80 (WWW) en la interfaz exterior y para traducir ese IP Address para ser 198.51.100.101
Cuando los hosts en el exterior establecen una conexión a 198.51.100.101 en el puerto 80 (WWW) del TCP de destino, el IP Address de destino se traduce para ser 192.160.1.100 y el puerto destino será el puerto TCP 80 (WWW) y le enviará el dmz

CONFIGURACIÓN ACL

Los ACL (access control list) lista de control de acceso, en el ASA permite reemplazar la conducta de seguridad predeterminada que es la siguiente:

- El tráfico que va de una interfaz de menor seguridad se niega al ir a una interfaz de mayor seguridad
- El tráfico que va de una interfaz de mayor seguridad se permite al ir a una interfaz de menor seguridad

Sin agregar ACL en la configuración, el tráfico trabaja de la siguiente manera:

- Los hosts en el interior con nivel de seguridad 100 pueden conectar con los hosts en el dmz con nivel de seguridad 50
- Los hosts en el interior con nivel de seguridad 100 pueden conectar con los hosts en el exterior con nivel de seguridad 0
- Los hosts en el dmz con nivel de seguridad 50 pueden conectar con los hosts en el exterior con nivel de seguridad 0.

Sin embargo, se niega el tráfico siguiente:

- Los hosts en el exterior con nivel de seguridad 0, no pueden conectar con los hosts en el interior con nivel de seguridad 100

- Los hosts en el exterior con nivel de seguridad 0, no pueden conectar con los hosts en el dmz con nivel de seguridad 50
- Los hosts en el dmz con nivel de seguridad 50, no pueden conectar con los hosts en el interior con nivel de seguridad 100.

Se necesita permitir explícitamente el tráfico, se debe utilizar el IP real del host en el ACL y no el IP traducido. Esto significa que la configuración necesita permitir el tráfico destinado a 192.160.1.100 y no con el tráfico destinado a 198.51.100.101 en el puerto 80.

Comandos de configuración:
access-list outside_acl extended. permite enlister un objeto del servidor web tcp.

access-group outside_acl in interface outside
En la configuración presentada se asume que hay servidor DNS en la red interna en la dirección IP 192.160.0.53 que los hosts en la necesidad del dmz de acceder para la resolución de DNS. Se crea el ACL necesario y lo aplica a la interfaz del dmz así que el ASA puede reemplazar esa conducta de seguridad predeterminada, mencionada anteriormente, para el tráfico que ingresa esa interfaz.
Configuración de comandos:
object network dns-server
host 192.160.0.53

access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any

access-group dmz_acl in interface dmz
PRUEBA DE LA CONFIGURACIÓN CON LA CARACTERÍSTICA DEL TRAZA-LÍNEAS DEL PAQUETE

Finalizada la configuración, se procede a probar para asegurar su funcionalidad. El método más fácil es utilizar los hosts reales. Además, en interés de probar la línea de comando y explorar algunas de las herramientas ASA, se utiliza el traza-líneas del paquete para probar y potencialmente para hacer el debug de cualquier problema encontrado.

El traza-líneas del paquete trabaja simulando un paquete basado en una serie de parámetros y la inyección de ese paquete al trayecto de datos de la interfaz, similar a un paquete real tomado del alambre. Este paquete se sigue con la mirada de los controles y de los procesos que se hacen encendido mientras que pasan con el Firewall y traza-líneas del paquete observando el resultado.

Para simular un paquete TCP que viene en la interfaz interior de la dirección IP 192.160.0.125 en el puerto de origen 12345 destinado a un IP Address de 203.0.113.1 en el puerto 80

ciscoasa# packet-tracer input inside tcp 192.160.0.125 12345 203.0.113.1 80

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config: Additional Information:
in 0.0.0.0 0.0.0.0 outside

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
object network inside-subnet
nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 192.168.0.125/12345 to 198.51.100.100/12345

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow

El resultado final es que el tráfico está permitido. Se observa que el paquete fue traducido en la fase 3 y los detalles de esa fase muestran lo que dice la regla. El host 192.160.0.125 se traduce dinámicamente a 198.51.100.100 según la configuración.
Luego se ejecuta para una conexión de Internet al web server, los hosts en Internet accederá el web server conectando con 192.51.100.101 en la interfaz exterior.

Configuración de un paquete TCP que viene en la interfaz exterior de la dirección IP 192.0.2.123 en el puerto de origen 12345 destinado a un IP Address de 198.51.100.101 en el puerto 80

ciscoasa# packet-tracer input outside tcp 192.0.2.123 12345 98.51.100.101 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network webserver
 nat (dmz,outside) static webserver-external-ip service tcp www www
Additional Information:
NAT divert to egress interface dmz
Untranslate 98.51.100.101/80 to 192.168.1.100/80

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside_acl in interface outside
access-list outside_acl extended permit tcp any object webserver eq www
Additional Information:

Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 5
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network webserver
 nat (dmz,outside) static webserver-external-ip service tcp www www

Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 3, packet dispatched to next module

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: dmz
output-status: up
output-line-status: up
Action: allow

Se muestra que el resultado del paquete está permitido. Los ACL marcan hacia fuera, las miradas de la configuración muy bien, y los usuarios en Internet (afuera) deben poder acceder ese web server usando IP externa.

La configuración final ASA 5510:

```
ASA Version 9.1(1)
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 198.51.100.100 255.255.0.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.160.0.1 255.255.0.0
!
```

```
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 192.160.1.1 255.255.0.0
!
object network inside-subnet
 subnet 192.160.0.0 255.255.0.0
object network dmz-subnet
 subnet 192.160.1.0 255.255.0.0
object network webserver
 host 192.160.1.100
object network webserver-external-ip
 host 198.51.100.101
object network dns-server
 host 192.160.0.53

access-list outside_acl extended permit tcp any object webserver eq www
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any
!
object network inside-subnet
 nat (inside,outside) dynamic interface
object network dmz-subnet
 nat (dmz,outside) dynamic interface
object network webserver
 nat (dmz,outside) static webserver-external-ip service tcp www www
access-group outside_acl in interface outside
access-group dmz_acl in interface dmz
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1 1
```