Universidad Autónoma Metropolitana
Unidad Azcapotzalco

División de Ciencias Básicas e Ingeniería
Licenciatura en Ingeniería en Computación

Diseño e implementación de un sistema de seguridad en una red empresarial con un corta fuegos serie PA-3020

Modalidad: Estancia Profesional

Datos del Alumno:
Karla Ariana Rosas Millán
205205005
ave0905@gmail.com

Asesor:

M. en C. José Ignacio Vega Luna
Categoría: Titular C
Departamento de Electrónica.
vlji@correo.azc.uam.mx

Co-Asesor:

Ing. Julio Cesar Zamora Trejo
Director del área de Redes e implementación
(SIJISA.S.A de C.V)
Julio.zamora@sijisa.net

Yo, José Ignacio Vega Luna, declaro que aprobé el contenido del presente Reporte de Proyecto de Integración y doy mi autorización para su publicación en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.

M. en C. José Ignacio Vega Luna

Yo, Julio Cesar Zamora Trejo, declaro que aprobé el contenido del presente Reporte de Proyecto de Integración y doy mi autorización para su publicación en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.

Ing. Julio Cesar Zamora Trejo

Yo, Karla Ariana Rosas Millán, doy mi autorización a la Coordinación de Servicios de Información de la Universidad Autónoma Metropolitana, Unidad Azcapotzalco, para publicar el presente documento en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco

Karla Ariana Rosas Millán.

Resumen

Las empresas poseen un conjunto de computadoras conectadas a la misma red y al exterior que deben ser capaces de establecer comunicaciones confiables con cualquier dispositivo en la red.
Por estas razones y debido a la importancia de la información que se maneja en las organizaciones es que se realizó la implementación de un cortafuegos de la plataforma Palo Alto Networks de la serie PA-3020, el cual será ahora el encargado de la seguridad perimetral en la red de la empresa Autotransportes TUM S.A de C.V.
Cabe mencionar que ya se contaba con una implementación previa de un cortafuegos de la plataforma CISCO-ASA, el cual se decide cambiar a Palo Alto como parte de la actualización de su sistema de seguridad ya que CISCO, anuncio en septiembre de 2013 que ya no venderán las plataformas CISCO-ASA, lo cual no valdría la pena seguir utilizando ya que por parte del fabricante ya no se crearía nuevos parches para reforzar la seguridad, por esta razón y entre otras tantas que serán expuestas en el marco teórico es que se decide a migrar a esta nueva plataforma de próxima generación.
Se tiene que tener mucho cuidado al implementar ya que la arquitectura que maneja CISCO es por módulos de seguridad donde viene una primera etapa de inspección donde algunas comunicaciones se dejan pasar siempre y cuando cumplan con condiciones de origen y destino, después vienen una cadena de filtros donde intentaran encontrar aplicaciones no deseadas así como la búsqueda de vulnerabilidades o virus no autorizadas que se intentaran bloquear. La arquitectura de la plataforma de Palo Alto es de una única pasada el tráfico esta contextualizado en el entorno de la aplicación se aplican políticas y controles sobre esa aplicación por lo tanto no hacen falta los módulos.
Por ellos y para ir validando que las reglas establecidas así como las políticas que están en el CISCO realicen la misma función de seguridad en el Palo Alto, es que se utiliza la herramienta para esta migración.
Una vez realizado el proceso se realizaron pruebas para verificar que funcione la implementación de manera correcta ya con tráfico en la red.

Tabla de Contenido

INDICE DE FIGURAS Y TABLAS

1. Introducción

La implementación de una red en una empresa permite compartir información o recursos para optimizar procesos. Sin embargo, la llegada de Internet y la importancia del manejo de información considerada como el activo más importante dentro de las organizaciones es objeto de diversas amenazas informáticas. Como parte de la solución existen herramientas lógicas y físicas tales como: antivirus, cortafuegos (*firewall* en inglés) y *software* de prevención de fuga de datos. Estas herramientas ayudan a proteger y mantener el control para evitar eventos no deseados que se detectan en la red o en los servicios.

Un corta fuegos es parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo cierta comunicación autorizada. La primera generación de cortafuegos consistió en sistemas de filtrado de paquetes. La segunda generación de cortafuegos consistió en la inspección de estado de paquetes. La tercera generación actúa sobre la capa de aplicación (capa 7).

La clave de un corta fuegos de aplicación es que puede entender ciertas aplicaciones y protocolos y permite detectar si un protocolo no deseado se coló a través de un puerto no estándar o si se está abusando de un protocolo de forma prejudicial. El cortafuegos de próxima generación trabaja hasta capa 7, proporciona una manera segura de habilitar las aplicaciones que los usuarios necesitan, evitando las amenazas de seguridad en Internet al inspeccionar todo el tráfico, incluidas aplicaciones, amenazas y contenido, vinculado al usuario independientemente de la ubicación o el tipo de dispositivo.
Debido al avance en la tecnología a nivel seguridad perimetral, es de suma importancia el mantener actualizado el sistema de seguridad en la red con mecanismos que permitan brindar protección de aquellas amenazas o ataques al que se pueden estar expuestos.
Por ello es que se llevará a cabo una actualización del diseño de red, así como un cambio en las herramientas de seguridad perimetral entre plataformas de cortafuegos, debido a que no se cubre con las necesidades de seguridad actuales de la empresa, debido a que *CISCO* ha dejado de producir la serie *CISCO-ASA*, por ello la empresa TUM Transportes S.A de C.V decidió implementar un cortafuego de nueva generación de la plataforma de *Palo Alto Networks* de la serie PA-3020 que cumplirá con sus expectativas a nivel seguridad perimetral.

2. Antecedentes

Se realizó una investigación acerca de trabajos relacionados con el tema de la estancia aquí propuesta y se encontraron las siguientes implantaciones de seguridad en redes usando un corta fuegos Fortigate:

I. Administración y seguridad de una red corporativa mediante un cortafuegos Fortigate 90D [1].

Estancia profesional realizada por Guillermo Donaciano Escobar de la UAM Azcapotzalco. La diferencia con respecto al trabajo a realizar en esta propuesta es que el llevado cabo previamente se usó un corta fuegos de otro proveedor y tecnología más antigua.

II. Integración y administración de un sistema de seguridad utilizando un Fortigate 90D [2].

Estancia profesional realizada por Stefano Araiza Salvatierra de la UAM Azcapotzalco. Este trabajo se realizó con un corta fuegos de otro proveedor y en una empresa donde las reglas y características de seguridad de la red son diferentes a las que se usarán en la propuesta aquí planteada.

III. Sistema de seguridad perimetral de una red con un cortafuegos Fortigate 60D [3].

Proyecto realizado por Aarón López Vázquez alumno de la UAM Azcapotzalco. La diferencia está en la plataforma donde se implementará y se actualizará el sistema de seguridad ya que se realizará un respaldo desde una plataforma a otra, así como también en la creación de túneles, políticas de seguridad y reglas *NAT*.

IV. Firewall Migration: 3 Tips To Help Make The Process Easier, artículo escrito por Bill Kleyman [4].

El artículo referencia a la importancia de tener actualizados las plataformas donde se confía la seguridad en la red, proporciona una guía o serie de pasos que se pueden usar al levar a cabo la migración de plataformas en cortafuegos y resalta puntos importantes para tomar en cuenta cuando se realice.

V. Análisis e implementación de mecanismos de seguridad para una red corporativa [5].

Estancia profesional realizada por Leticia Pérez Bonilla de la UAM Azcapotzalco.
La diferencia está en la plataforma donde se implementará y se actualizará el sistema de seguridad ya que se realizará un respaldo desde una plataforma a otra. Este trabajo analizo el estado de la red así como las necesidades de seguridad y se propuso una metodología con base en el empleo de algoritmos para su sistema de seguridad así como la implementación de políticas de seguridad, VPN, técnicas de priorización de datos y calidad de servicio a través de un cortafuegos Fortigate.

VI. Análisis y gestión de recursos para brindar seguridad en una red empresarial [6].

Estancia profesional realizada por Dávila Ávila Castillo de la UAM Azcapotzalco. Este trabajo consto de una evaluación de los recursos de la red con la que contaba la empresa, en base en el análisis se brindó la propuesta de solución, donde se implementaron reglas de seguridad, creación de políticas, VPN en un cortafuegos Fortigate 40 C.

3. Justificación

El beneficio de diseñar, implementar y actualizar un sistema de seguridad de red a través de un cortafuegos es controlar la salida y entrada de información, permitiendo o negando accesos por medio de políticas de seguridad, delimitando quién y qué tipo de información es a la que puede tener acceso. Así, de manera muy específica se sabe quién o quiénes son las personas autorizadas para acceder a la información definida de uso exclusivo. El fallo en la seguridad de los centros de datos se puede presentar debido a un ineficiente diseño de la red o a la falta de actualización de los dispositivos que proveen la seguridad, ya que si el diseño no es eficiente para las necesidades de la empresa, es posible que no proteja la información, así mismo si no se cumple con el propósito de un *software o hardware* de poder evolucionar, se pone en riesgo la seguridad de la empresa por lo cual no se podrá hacer frente a las amenazas informáticas como: robo de información, robo de identidad, pérdida o manipulación de datos e interrupción del servicio. Estos son algunos problemas o amenazas que se pueden presentar en una empresa provocando pérdida de datos sensibles. Por ello, se debe diseñar e implementar un sistema de seguridad en la red acorde a las necesidades del cliente con mira al futuro.

Este proyecto tiene como objetivo realizar el diseño e implementación de la actualización de la seguridad en la red de la empresa TUM Transportes S.A de C.V. usando un corta fuegos de próxima generación *Palo Alto Networks* PA-3020. En la implementación se llevará a cabo un respaldo del cortafuegos Cisco-ASA, el cual es usado actualmente para implantar la seguridad de la red de la empresa, ya que el cliente requiere sean usadas las políticas de seguridad actuales al implantar el cortafuegos con la nueva plataforma PA-3020.

4. Objetivos

Objetivo general

Diseñar e implementar un sistema de seguridad en la red de TUM Transportes S.A. de C.V. usando un cortafuegos serie PA-3020.

Objetivos específicos

- Diseñar un sistema de seguridad en la red de TUM Transportes S.A. de C.V. con un corta fuegos de *Palo Alto Networks* serie PA-3020.
- Obtener y validar la información de usuarios, políticas de seguridad, reglas *NAT* e interfaces en la configuración actual del cortafuegos la red de TUM Transportes S.A. de C.V.
- Crear las políticas de seguridad, zonas y reglas *NAT* para la seguridad de la red en un cortafuegos serie PA-3020.
- Crear túneles *VPN* entre los centros de datos de TUM Transportes S.A. de C.V. en el PA-3020 y optimizar los existentes para establecer una conexión de forma segura y cifrada

5. Marco Teórico

El uso de las computadoras se ha convertido en la herramienta esencial para el manejo de información en nuestra vida cotidiana y más aún en la realización de los negocios.

Como consecuencia ha esto surgió la necesidad de compartir información entre usuarios y organizaciones o empresas. Esta necesidad se generó por medio de dos fuerzas: los laboratorios y los proyectos de investigación, que ante la necesidad de colaboración al compartir información entre diferentes grupos situados en lugares remotos, desarrollaron protocolos y métodos para transferir datos; también se vieron involucrados los intereses por parte de las empresas, de mejorar el intercambio de información corporativa entre oficinas o edificios, así pues se llevaron a cabo el desarrollo de varios protocolos y métodos desarrollados para este fin.

Los firewalls ofrecen una solución a estos problemas y ha surgido una amplia variedad de tecnologías y estrategias de entre las cuales se encuentran, como innovación de los últimos tiempos, los firewalls distribuidos, que permiten establecer

5.1 Seguridad en redes

Muchas organizaciones ofrecen servicios mediante sus sistemas de comunicación, la efectividad de tales servicios requiere el acceso a recursos críticos del sistema de información de la empresa (archivos, dispositivos de almacenamiento, líneas telefónicas, etc.). Tales recursos deben ser protegidos contra el uso indiscriminado y malicioso por parte de usuarios no deseados.

Por ello la implementación de un buen sistema de seguridad requiere el uso de ciertas funciones que permitan asegurar la confidencialidad e integridad de los recursos de nuestra red contra los ataques de intrusos. De este planteamiento surgen preguntas, que se deberán responder al momento de implementar un mecanismo de seguridad efectivo para una red:

¿Qué queremos proteger?

- Los recursos del sistema

Hardware
Software
Datos.

- Tipos de ataque a los recursos:

Interrupción: recurso queda inutilizable o no disponible
Intercepción: captura de un recurso o acceso al mismo
Modificación o destrucción: Intercepción y manipulación del recurso
Fabricación: generación de recursos similares a los atacados

¿De qué nos queremos proteger?

- De todos aquellos agentes que puedan atacar a nuestros recursos

Personas: empleados, ex-empleados, curiosos, piratas, terroristas, intrusos remunerados
Amenazas lógicas: software defectuoso, herramientas de seguridad, puertas traseras, bombas lógicas, canales ocultos, virus, gusanos, caballos de Troya, etc.
Catástrofes

- ¿Cómo nos podemos proteger?

Análisis de amenazas
Evaluación de (posibles) pérdidas y su probabilidad
Definición de una política de seguridad
Implementación de la política: mecanismos de seguridad
De prevención: durante el funcionamiento normal del sistema
De detección: mientras se produce un intento de ataque
De recuperación: tras un ataque, para retornar a un funcionamiento correcto: Análisis forense

5.2 Cortafuegos(firewall)

La tecnología de los cortafuegos surgió a finales de 1980, cuando Internet era una tecnología bastante nueva en cuanto a su uso global y la conectividad. Los predecesores de los cortafuegos para la seguridad de la red fueron los routers utilizados a finales de 1980, que mantenían a las redes separadas unas de otras. La visión de Internet como una comunidad relativamente pequeña de usuarios con máquinas compatibles, que valoraba la predisposición para el intercambio y la colaboración, terminó con una serie de importantes violaciones de seguridad de Internet que se produjo a finales de los 80

- **Primera generación – cortafuegos de red: filtrado de paquetes**

El primer documento publicado para la tecnología firewall data de 1988, cuando el equipo de ingenieros Digital Equipment Corporation (DEC) desarrolló los sistemas de filtro conocidos como cortafuegos de filtrado de paquetes. Este sistema, bastante básico, fue la primera generación de lo que se convertiría en una característica más técnica y evolucionada de la seguridad de Internet. En AT&T Bell, Bill Cheswick y Steve Bellovin, continuaban sus investigaciones en el filtrado de paquetes y desarrollaron un modelo de trabajo para su propia empresa, con base en su arquitectura original de la primera generación

- ## Segunda generación – cortafuegos de estado

Durante 1989 y 1990, tres colegas de los laboratorios AT&T Bell, Dave Presetto, Janardan Sharma, y Nigam Kshitij, desarrollaron la segunda generación de servidores de seguridad. Esta segunda generación de cortafuegos tiene en cuenta, además, la colocación de cada paquete individual dentro de una serie de paquetes. Esta tecnología se conoce generalmente como la inspección de estado de paquetes, ya que mantiene registros de todas las conexiones que pasan por el corta fuegos, siendo capaz de determinar si un paquete indica el inicio de una nueva conexión, es parte de una conexión existente, o es un paquete erróneo. Este tipo de cortafuegos pueden ayudar a prevenir ataques contra conexiones en curso o ciertos ataques de denegación de servicio.

- ## Tercera generación – cortafuegos de aplicación

Son aquellos que actúan sobre la capa de aplicación del modelo OSI. La clave de un cortafuegos de aplicación es que puede entender ciertas aplicaciones y protocolos (por ejemplo: protocolo de transferencia de ficheros, DNS o navegación web), y permite detectar si un protocolo no deseado se coló a través de un puerto no estándar o si se está abusando de un protocolo de forma prejudicial

- ## Cortafuegos de nueva generación

Los cortafuegos de nueva generación, *Next-Generation Firewall* (NGFW), surgieron para revolucionar la seguridad de la red tal y como la conocíamos hasta ahora. Los firewalls tradicionales se limitan a la inspección de paquetes por estado y a reglas de control de acceso, pero a medida que los hackers se hacen más sofisticados, las amenazas son más avanzadas y este sistema ha dejado de ser eficaz. Con el fin de proteger un negocio de amenazas en constante evolución, el Firewall de Nueva Generación debe ser capaz de ofrecer un nivel más profundo de seguridad de red.

Para ello la clave es garantizar la inspección de todos los bytes de cada paquete, pero esto ha de conseguirse manteniendo el rendimiento elevado y la baja latencia para que la redes con mucho tráfico sigan funcionando de forma óptima. Además de combatir amenazas de forma eficaz y abordar problemas de productividad cada vez más acuciantes, las empresas requieren un nivel más profundo de seguridad y control. Para ello tus clientes necesitan un firewall de nueva generación que contenga:

- **Descifrado e inspección de SSL**

Las organizaciones actuales que no disponen de descifrado e inspección de SSL no tienen control sobre una tercera parte del tráfico de su red.

- **IPS con tecnología anti-evasión**

Los cibercriminales suelen intentar esquivar los IPS utilizando algoritmos complejos que eluden la detección.

- **Control de aplicaciones basado en contexto**

La popularidad de las aplicaciones basadas en acceso de red se ha disparado en los diez últimos años, lo que ha complicado a los administradores la tarea de supervisar la actividad de los usuarios y el uso del tráfico por parte de las aplicaciones.

- **Protección contra malware basada en red**

Cada hora se desarrollan nuevas variantes de malware. Mantenerse informado de todas esas amenazas gracias a la protección contra malware basada en red, que utilice una base de datos en la nube que se actualice constantemente es fundamental para bloquear las nuevas amenazas en cuanto aparecen.

6. Desarrollo del Proyecto

El primer paso como parte inicial del desarrollo o implementación de sistemas, se requiere el acercamiento con el cliente para obtener información acerca de las características con lo que cuenta en su red así como de los recursos que desea proteger ya que antes de realizar la migración del ASA a Palo Alto debemos tener o tomar en cuenta ciertas consideraciones que se tiene previstas tales como:

- Obtener el archivo de migración de ASA del cliente
- Saber la topología con el ASA
- Saber cómo esta migración se ajusta a los conjuntos de reglas existentes de Palo Alto
- Saber cuál es su destino para esta migración (panorama o firewall).
- Quien o quienes tendrán acceso al equipo y de qué tipo
- que servicios se agregaran

6.1 Características de las plataformas CISCO ASA y Palo Alto

En esta tabla podemos ver las características de un CISCO-ASA que es un cortafuegos capa 4, y las características de un cortafuegos de la plataforma de próxima generación de Palo Alto Networks

	CISCO-ASA	**Palo Alto Networks**
Arquitectura	Marco de política modular	Arquitectura de paso único
Políticas	• Decisión política basada en puertos / protocolos • Múltiples políticas para FW, IPS, AVC, etc.	• Decisión de política basada en aplicaciones independientemente de puertos y protocolos. • Una base de regla de política unificada
Protección contra amenazas	Modulo AIP-SSM(IPS) Modulo AIP-CSC(A/V)	Marco completo de protección de amenazas (conocido y desconocido)
Zonas/interfaces	Interfaces	Zonas de seguridad
Modos de despliegue	Capa 2 y Capa 3	Modo tap, cable virtual(capa 1), capa 2, capa 3
Administración	CSM, Prime, IME, ASDM, Cloud, Web Security Portal	Panorama, GUI del dispositivo

TABLA 1. CARACTERÍSTICAS DE CORTAFUEGOS

Estas características deben ser tomadas en cuenta para efectuar con éxito la migración e implementación a la plataforma de Palo Alto ya que por ejemplo en la arquitectura del CISCO-ASA esta viene por módulos y son hasta capa 4, y la de Palo Alto son en capa 7.

6.2 Evaluación de Archivo extraído del ASA

Una vez que el cliente nos provee de dicho archivo procedemos a utilizar la herramienta de Palo Alto Networks y que tiene una base de datos que rastrea cada tarea que está realizando.

FIGURA 1.- ARCHIVO ASA

Toda la interacción con la herramienta se llevará a cabo a través de una interfaz web donde se podrá reiniciar, apagar, borrar su configuración de registro y reiniciar su base de datos. La herramienta que se utilizara para la migración se entrega como parte de un paquete en una máquina virtual; necesita un entorno virtual para ejecutar la herramienta de migración Palo Alto Networks en MS Windows, Mac OS X o Linux.

Después de que el cliente nos provee del archivo extraído de su ASA debemos considerar los siguientes puntos:

- Evaluar la configuración actual
- Política heredada
  Las políticas se crearon originalmente con la mentalidad de puerto / protocolo / IP y no se optimizaron para aplicaciones y usuarios
- Historia perdida
  Muchas empresas se enfrentan a "Inflamación de la política" y "cruft" en sus configuraciones de firewall
- -Auditoría
  Migración de cortafuegos heredada
  verificar la política actual de efectividad y seguridad
  limpiar la política antes de la conversión
- Analizar
  Comprender cómo se integra el firewall actual en el entorno de red
  Encuentra los casos de esquina que necesitan migrarse manualmente
- Convertir
  Objetos, servicios y políticas para PAN-OS
  Pruebe / verifique la política convertida
  Configurar manualmente los "casos de esquina" (NAT y VPN)

6.3 Implementación en una Virtual Machine

Esta herramienta nos ayudara a tener una visión más amplia de lo que son las políticas de seguridad, Reglas de ruteo, reglas NAT y tipos de accesos, nos lleva a un ambiente virtual más amigable.

Una vez terminado de montar el archivo en la VM, se comienza por verifica que las reglas estáticas ya existentes estén todas en el Palo Alto, de no ser así se deben ir una por una agregando

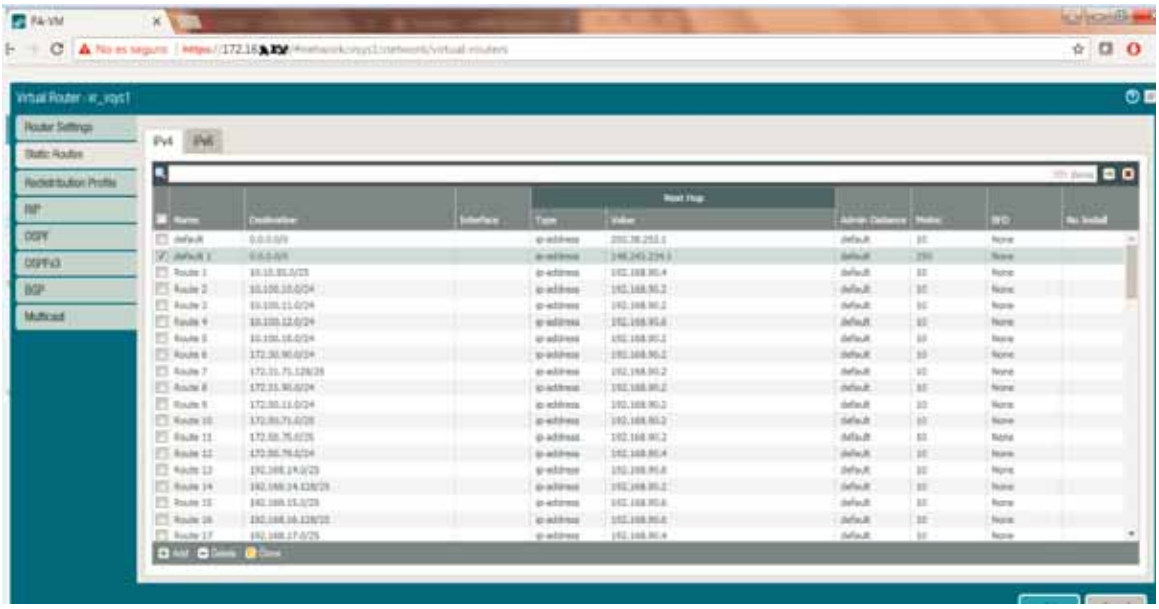


FIGURA 2.- RUTAS ESTATICAS

El Router Virtual contiene las rutas para alcanzar los diferentes segmentos de red y VPN dentro de la empresa.

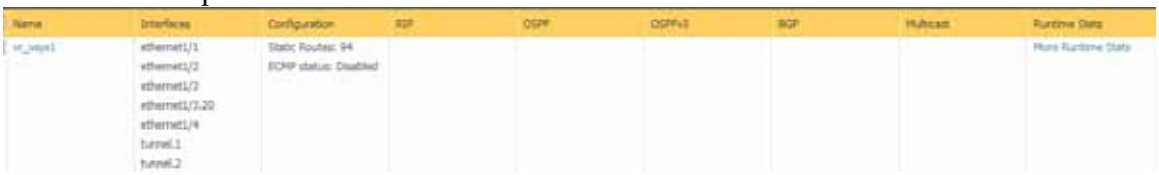


FIGURA 3.- RUTAS VIRTUALES

6.4 Zonas de seguridad

Network>>Zones

Se procede a validar las zonas de seguridad que estaban en el ASA, ahora estén implementadas en la VM de Palo Alto

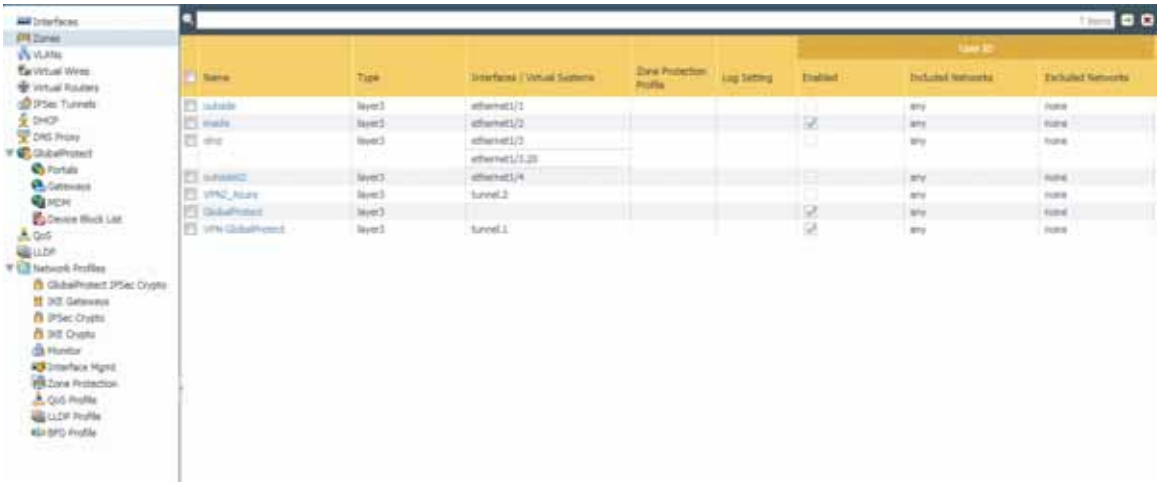


FIGURA 4.- ZONAS IMPLEMENTADAS

- **Interfaces**

Las interfaces de red fueron configuradas en Capa 3, cada una fue asignada a una zona de seguridad, estas fueron agregadas dentro de un router virtual y asignadas a un perfil de gestión como se muestra a continuación:

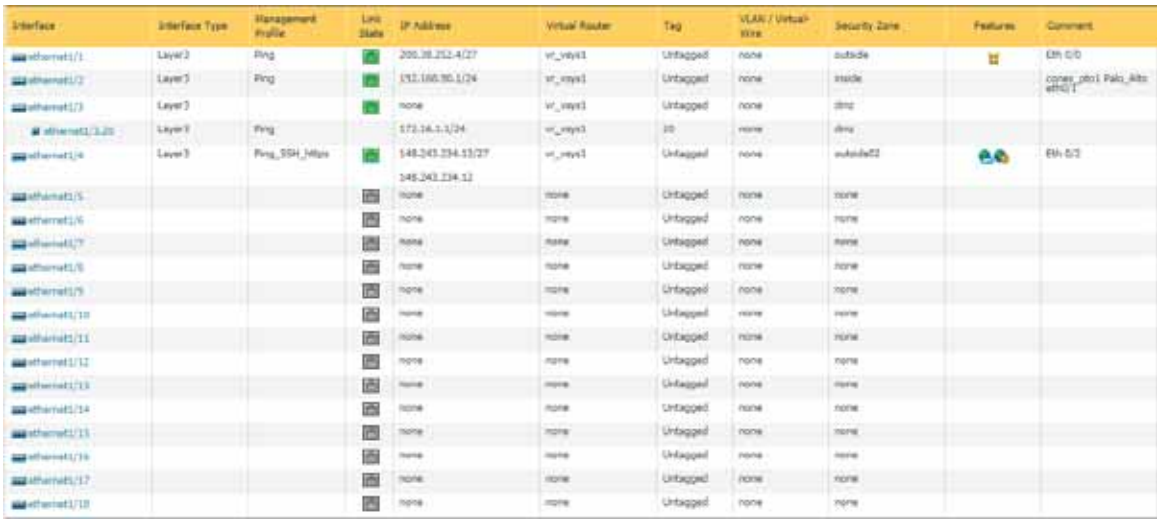


FIGURA 5.- INTERFACES VALIDADAS

- **Tunnel**

Se utiliza la configuración de Interfaces de tipo túnel utilizadas para la conexión VPN Site to Site hacia los sitios remotos. Para esta conexión VPN se necesitan lo siguiente:
IKE Gateway
Interfaz de túnel
Monitoreo de túnel
Intercambio de claves de internet (IKE) para VPN
IKEv2

Interface	Management Profile	IP Address	Virtual Router	Security Zone	Features	Comment
tunnel		none	none	none		
tunnel.1		none	vr_vsys1	VPN-GlobalProtect		Global Protect
tunnel.2		none	vr_vsys1	VPN2_Azure		

FIGURA 6.- VPN

6.5 Políticas de seguridad

Policies>>Security

Las políticas de seguridad fueron establecidas de acuerdo a los criterios solicitados por Autotransportes TUM S.A de C.V de acuerdo en sus políticas de seguridad validando que todas trabajen y se dirijan como estaban en el CISCO en caso de que esta no este, se debe agregar, esta operación de verificación debe irse agregando una a una. El cómo trabaja el firewall en esta parte es como sigue: Se identifica el tráfico por aplicación primero, usando la tecnología App-ID independientemente del puerto o protocolo. Esto te permite crear políticas de seguridad y uso basadas en aplicaciones y sus correspondientes funciones, como el chat o el intercambio de archivos. Se suele combinar la aplicación de ID con nuestra tecnología User-ID, que identifica usuarios independientemente de la dirección IP o dispositivo, para ver y comprender su tráfico dentro del contexto de quién está accediendo a qué en la red.

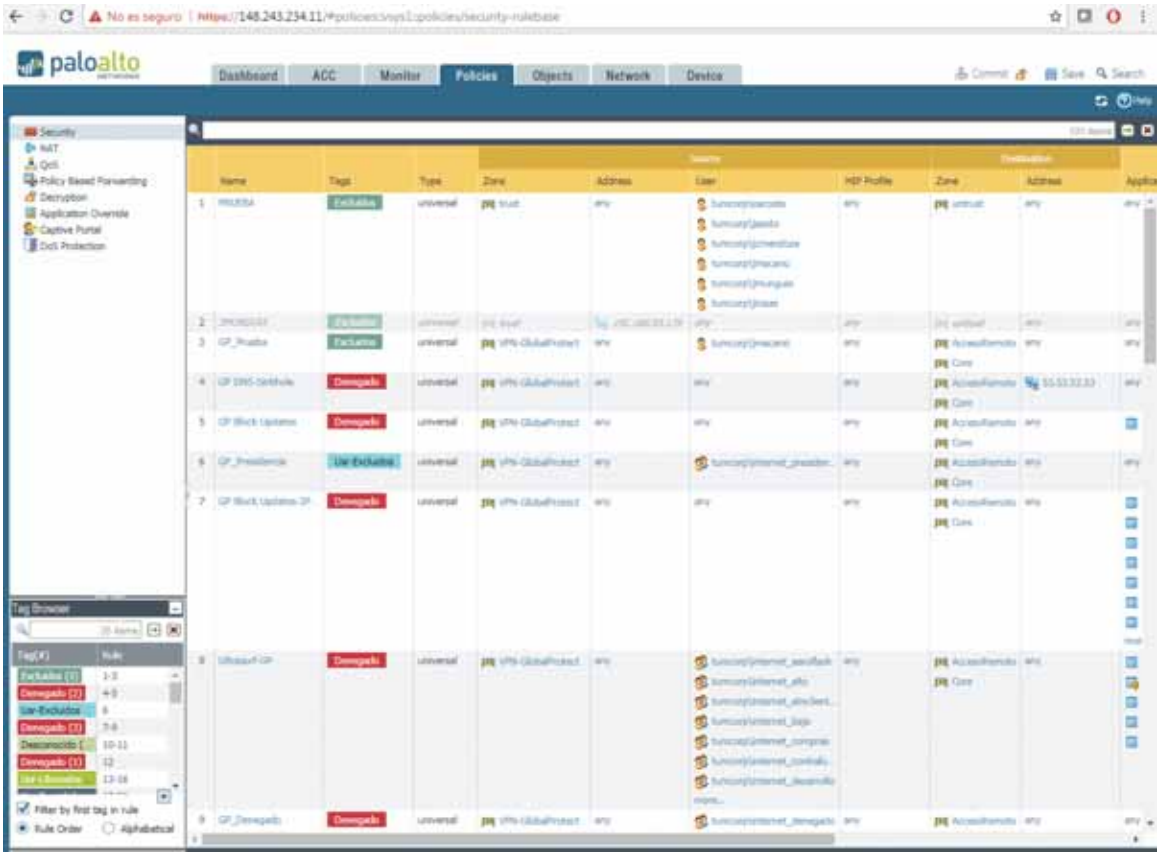


FIGURA 7.- POLÍTICAS DE SEGURIDAD

6.6 Políticas NAT

Las políticas de NAT fueron configuradas para permitir la navegación hacia internet de los usuarios en la red LAN y para la publicación en Internet de algunos servicios propios de la empresa.

Las reglas de NAT se basan en las zonas de origen y de destino, las direcciones de origen y destino y el servicio de aplicación (como HTTP). Al igual que las políticas de seguridad, las reglas de políticas NAT se comparan con el tráfico entrante en secuencia, y se aplica la primera regla que coincide con el tráfico.

Se agregan las rutas estáticas al enrutador local para que el tráfico a todas las direcciones públicas se enrute al cortafuegos. También es posible que necesite agregar rutas estáticas a la interfaz de recepción en el firewall para enrutar el tráfico a la dirección privada.

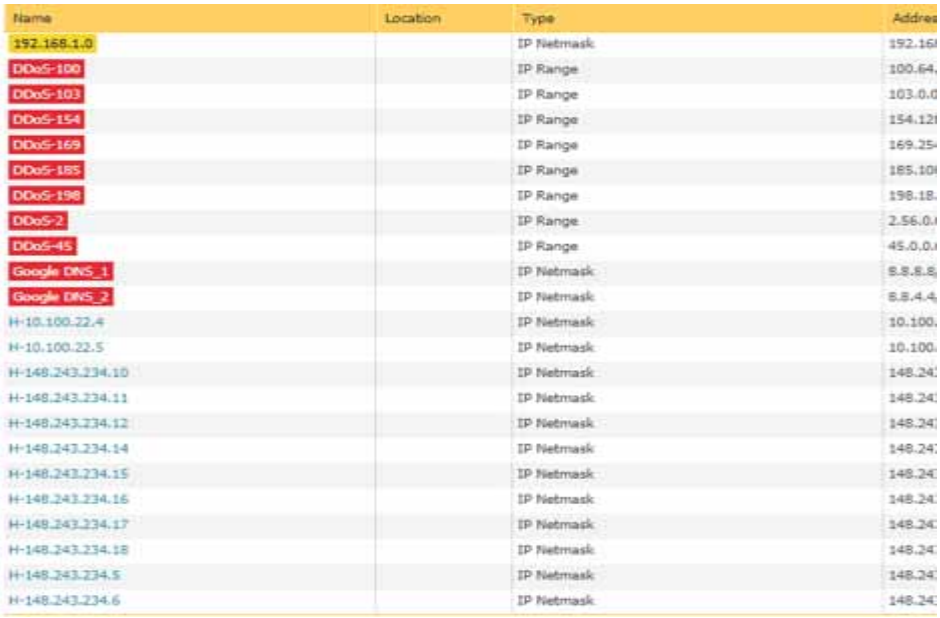
			Original Packet						Translate
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation
1	AutoNat HOST80.65	Servicios_Public	outside	outside	any	any	H-200.38.252.27	any	none
2	AutoNat HOST80.49	Servicios_Public	outside	outside	any	any	H-200.38.252.22	any	none
3	AutoNat HOST80.48	Servicios_Public	outside	outside	any	any	H-200.38.252.9	any	none
4	AutoNat HOSTDMZ1.9	Servicios_Public	outside	outside	any	any	H-200.38.252.12	any	none
5	AutoNat HOSTDMZ1.7	Servicios_Public	outside	outside	any	any	H-200.38.252.23	any	none
6	AutoNat HOST80.13	Servicios_Public	outside	outside	any	any	H-200.38.252.5	any	none
7	AutoNat HOSTDMZ1.24	Servicios_Public	outside	outside	any	any	H-200.38.252.24	any	none
8	AutoNat HOSTDMZ1.25	Servicios_Public	outside	outside	any	any	H-200.38.252.13	any	none
9	AutoNat HOSTDMZ1.26	Servicios_Public	outside	outside	any	any	H-200.38.252.11	any	none
10	AutoNat HOST67.163	Servicios_Public	outside	outside	any	any	H-200.38.252.20	any	none
11	AutoNat HOSTDMZ1.27	Servicios_Public	outside	outside	any	any	H-200.38.252.15	any	none
12	AutoNat HOST80.31	Servicios_Public	outside	outside	any	any	H-200.38.252.18	any	none
13	AutoNat HOSTDMZ1.31	Servicios_Public	outside	outside	any	any	H-200.38.252.28	any	none
14	AutoNat HOST80.133	Servicios_Public	outside	outside	any	any	H-200.38.252.10	any	none
15	AutoNat HOST80.134	Servicios_Public	outside	outside	any	any	H-200.38.252.30	any	none
16	AutoNat HOST80.110	Servicios_Public	outside	outside	any	any	H-200.38.252.6	any	none
17	AutoNat HOST63.21	Servicios_Public	outside02	outside02	any	any	H-148.243.234.5	any	none
18	AutoNat HOSTDMZ1.8	Servicios_Public	outside	outside	any	any	H-200.38.252.26	any	none
19	AutoNat HOST80.99	Servicios_Public	outside	outside	any	any	H-200.38.252.16	any	none
20	AutoNat HOST80.252	Servicios_Public	outside02	outside02	any	any	H-148.243.234.10	any	none
21	AutoNat HOSTDMZ1.10	Servicios_Public	outside02	outside02	any	any	H-148.243.234.6	any	none
22	AutoNat HOST80.50	Servicios_Public	outside	outside	any	any	H-200.38.252.29	any	none
22	AutoNat HOST80.50	Servicios_Public	outside	outside	any	any	H-200.38.252.29	any	none
23	AutoNat HOST78.2	Servicios_Public	outside02	outside02	any	any	H-148.243.234.11	any	none
24	AutoNat HOST80.202	Servicios_Public	outside02	outside02	any	any	H-148.243.234.12	any	none
25	AutoNat HOST78.34	Servicios_Public	outside02	outside02	any	any	H-148.243.234.14	any	none
26	AutoNat HOST78.52	Servicios_Public	outside02	outside02	any	any	H-148.243.234.15	any	none
27	AutoNat HOST78.59	Servicios_Public	outside02	outside02	any	any	H-148.243.234.16	any	none
28	AutoNat HOST78.43	Servicios_Public	outside02	outside02	any	any	H-148.243.234.17	any	none
29	AutoNat HOST80.69	Servicios_Public	outside	outside	any	any	H-200.38.252.7	any	none
30	Nat_80.58	Servicios_Public	outside	outside	any	any	H-200.38.252.8	any	none
31	AutoNat HOST78.45	Servicios_Public	outside02	outside02	any	any	H-148.243.234.18	any	none
32	AutoNat HOST80.33	Servicios_Public	outside	outside	any	any	H-200.38.252.17	any	none
33	AutoNat HOST80.68	Servicios_Public	outside	outside	any	any	H-200.38.252.14	any	none
34	AutoNat HOST80.60	Servicios_Public	outside	outside	any	any	H-200.38.252.19	any	none
35	Nat_80.79	Servicios_Public	outside02	outside02	any	any	148.243.234.7	any	none
36	Nat_80.135	Servicios_Public	outside	outside	any	any	H-200.38.252.3	any	none
37	Host_80_81	Servicios_Public	outside02	outside02	any	any	148.243.234.19	any	none
38	Host_80_82	Servicios_Public	outside02	outside02	any	any	148.243.234.20	any	none

FIGURA 8.- REGLAS NAT

6.7 Objetos

Objects>>Addresses

En este módulo se pueden agregar objetos de direcciones a la base de datos local del firewall con la finalidad de aplicar políticas en la cuales se pueda contar con una administración más sencilla.



Name	Location	Type	Addres
192.168.1.0		IP Netmask	192.16
DDoS-100		IP Range	100.64.
DDoS-103		IP Range	103.0.0
DDoS-154		IP Range	154.12
DDoS-169		IP Range	169.25
DDoS-185		IP Range	185.10
DDoS-198		IP Range	198.18.
DDoS-2		IP Range	2.56.0.
DDoS-45		IP Range	45.0.0.
Google DNS_1		IP Netmask	8.8.8.8
Google DNS_2		IP Netmask	8.8.4.4
H-10.100.22.4		IP Netmask	10.100.
H-10.100.22.5		IP Netmask	10.100.
H-148.243.234.10		IP Netmask	148.24
H-148.243.234.11		IP Netmask	148.24
H-148.243.234.12		IP Netmask	148.24
H-148.243.234.14		IP Netmask	148.24
H-148.243.234.15		IP Netmask	148.24
H-148.243.234.16		IP Netmask	148.24
H-148.243.234.17		IP Netmask	148.24
H-148.243.234.18		IP Netmask	148.24
H-148.243.234.5		IP Netmask	148.24
H-148.243.234.6		IP Netmask	148.24

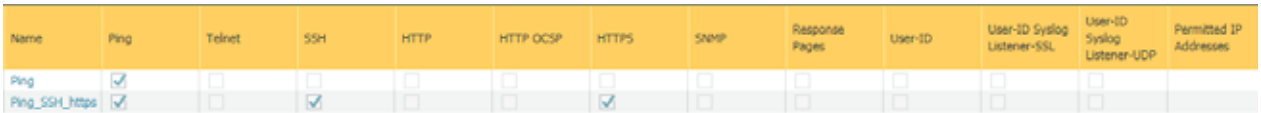
FIGURA 9.- OBJETOS

También se tiene clasificadas los grupos de direcciones para saber a qué o quién se permite

FIGURA 10.- GRUPOS DE OBJETOS

- **Interface Mgmt**

Los perfiles de gestión tienen la función de permitir la administración del equipo usando los siguientes protocolos para las distintas interfaces del firewall PAN-3020.



Name	Ping	Telnet	SSH	HTTP	HTTP OCSP	HTTPS	SNMP	Response Pages	User-ID	User-ID Syslog Listener-SSL	User-ID Syslog Listener-UDP	Permitted IP Addresses
Ping	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
Ping_SSH_https	☑	☐	☑	☐	☐	☑	☐	☐	☐	☐	☐	

FIGURA 11.- INTERFACES DE ADMINISTRACIÓN

7. Resultados

El resultado de esta implementación se validó en una ventana ya con tráfico en la red, cabe mencionar que el PA-3020 estuvo en modo transparente acorde al siguiente diagrama

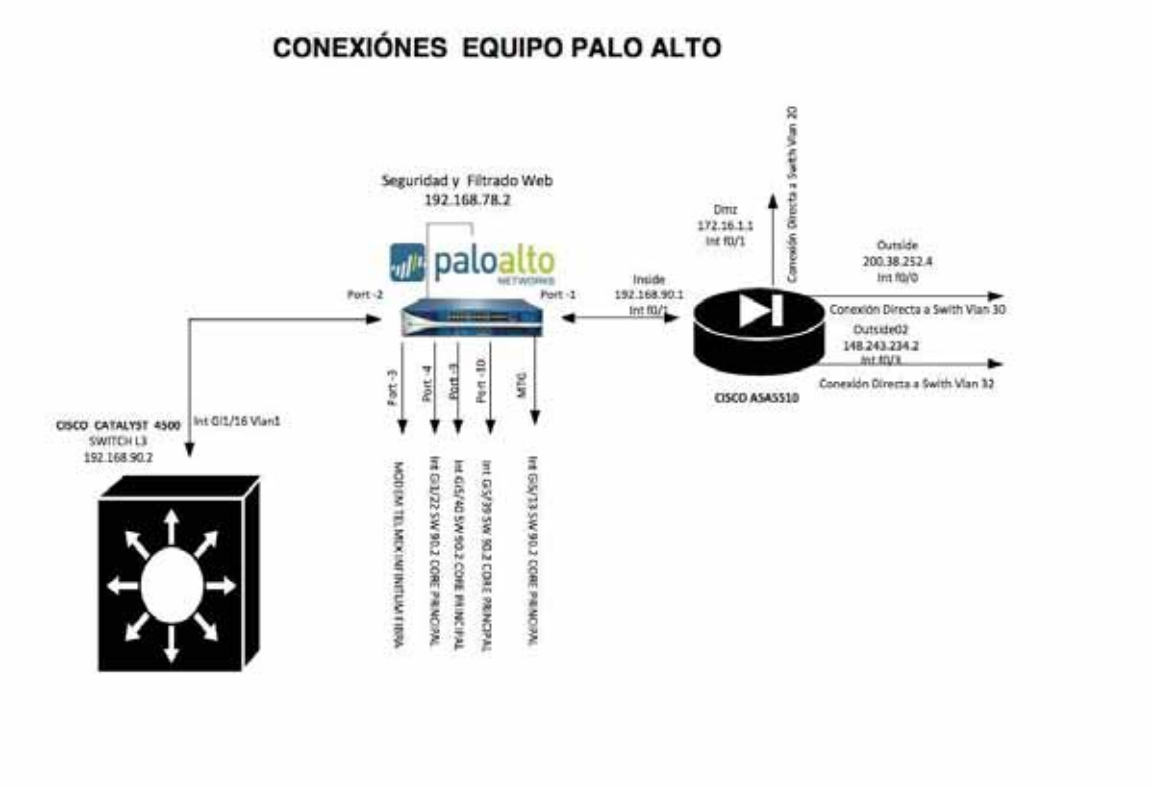


FIGURA 12.- DIAGRAMA DE RED DE MIGRACIÓN

Trabajo con el ASA, y el día de la ventana se validaron todas las implementaciones y en la cual se hizo lo siguiente:

- Se cargó la configuración L3 en el equipo PA-3020
- Se cambiaron cables para las interfaces
- Se realizó la configuración para AD
- Se realizó la configuración para Global Protect (VPN)
- Se realizó conferencia con el proveedor de Azure
- Se confirmaron las validaciones para los servicios publicados, Global protect a través de AD, y usuarios locales, pruebas de conectividad con servidores de Azure, así como también validaciones de todas las rutas y puertos permitidos para sus servicios.

Se ajustaron puertos en varios servicios publicados

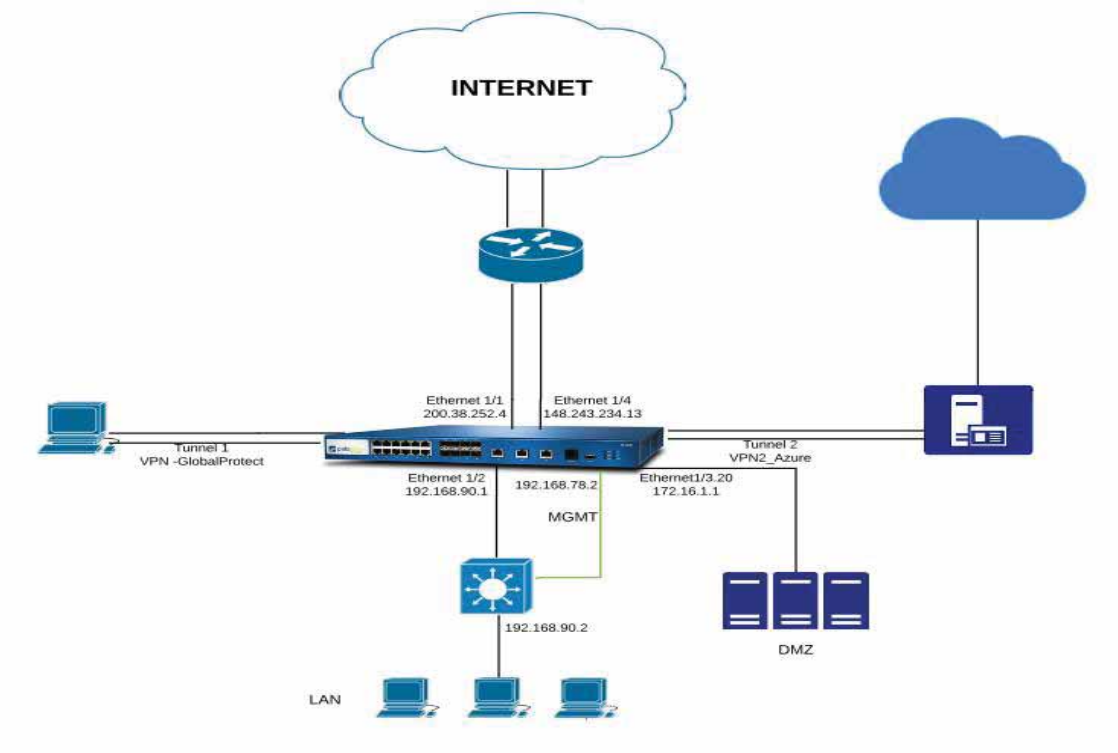


FIGURA 13.- DIAGRAMA DE RED, IMPLEMENTACIÓN FINAL

El la figura 13 se muestra la topología de red de TUM, en la cual el cortafuegos PA-3020 es el encargados de realizar las funciones de ruteo, NAT, políticas de seguridad, QoS así como permitir la navegación de los usuarios. En este se muestra la salida de internet por las interface 1/1 y 1/4 respectivamente y con ello se logra realizar un tráfico seguro tanto en la red interna como hacia internet y enviando el tráfico de manera direccional según sea necesaria su recepción.

Al realizar la evaluación con tráfico en la red, surgen los siguientes problemas:

- Problema de ruteo en el cual la configuración del switch no nos dejaba llegar correctamente a los servidores
- Validación y ajuste de políticas de seguridad
- Ajuste de puertos en políticas de servicios

Se procede a darle solución a los problemas surgidos.

8. Conclusiones

En la estancia profesional, se implementó un sistema de seguridad a la empresa Autotransportes TUM. S.A de C.V. El manejo de la tecnología de Palo Alto requiere de mucho estudio y comprensión de las reglas sobre todo la lógica de funcionamiento. También verificamos que las políticas establecidas realmente satisfagan la necesidad de la empresa por ello se evaluó y se dejó trabajando de forma óptima el equipo y se continua monitoreando el manejo de este brindándole el soporte para que en caso de existir cualquier tipo de problema este pueda ser atendido y solucionado o si en algún momento existe alguna duda o modificación en cuanto a permisos o creación de nuevas reglas o dando de alta algún objeto para poder utilizar o entrar a la red, se valida diariamente que el comportamiento del equipo de manera remota por el túnel VPN y así poder ofrecer al cliente la completa satisfacción de su funcionamiento que no haya un reinicio y si lo hay de manera inesperada ir a las bitácoras para saber la causa del reinicio y en dado caso informar al cliente que es lo que pasa o si no existe nada en las bitácoras, saber si fue algún tipo de falla en el sitio.

9. Bibliografía

[1] G. Donaciano, Administración y seguridad de una red corporativa mediante un cortafuegos Fortigate 90D, proyecto terminal, División de Ciencias Básicas e Ingeniería, Universidad Autónoma Metropolitana Unidad Azcapotzalco, Ciudad de México, 14 de marzo de 2016.

[2] S. Araiza, Integración y administración de un sistema de seguridad utilizando un cortafuegos Fortigate 90D, proyecto terminal, División de Ciencias Básicas e Ingeniería, Universidad Autónoma Metropolitana Unidad Azcapotzalco, Ciudad de México, 18 de julio de 2017.

[3] A. Vázquez, Sistema de seguridad perimetral de una red con un cortafuegos Fortigate 60D, proyecto terminal, División de Ciencias Básicas e Ingeniería, Universidad Autónoma Metropolitana Unidad Azcapotzalco, Ciudad de México, 5 de enero de 2017.

[4] https://blog.algosec.com/2014/08/firewall-migration-3-things-know.html,.

[5] L. Pérez, Análisis e implementación de mecanismos de seguridad para una red corporativa, proyecto terminal, División de Ciencias Básicas e Ingeniería, Universidad Autónoma Metropolitana Unidad Azcapotzalco, Ciudad de México, diciembre de 2014.

[6] D. Castillo, Análisis y gestión de recursos para brindar seguridad en una red empresarial, proyecto terminal, División de Ciencias Básicas e Ingeniería, Universidad Autónoma Metropolitana Unidad Azcapotzalco, Ciudad de México, 11 de diciembre de 2015.

[7] Data sheet Cisco ASA
https://www.cisco.com/c/dam/global/es_es/assets/publicaciones/07-08-cisco-dispositivos-serie-ASA5500.pdf

[8] Data sheet PAN-3020
https://www.paloaltonetworks.com/resources/datasheets/pa-3000-series-specsheet

[9] CERTSUPERIOR
https://www.certsuperior.com/SeguridadenRedes.aspx

[10]
http://repositorio.pucp.edu.pe/index/bitstream/handle/123456789/28691/Redes_Cap24.pdf?sequence=24

[11] https://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio

[12] http://noticias.gti.es/fabricantes/que-es-firewall-de-nueva-generacion/