



Reporte Final de Estadía

Angel Ramírez Ramírez

Firewall Perimetral



Programa Educativo
Tecnologías de la Información

Reporte para obtener título de
Ingeniero en Tecnologías de la Información

Proyecto de estadía realizado en la empresa
Tecapps S.A. de .C.V.

Nombre del proyecto
“Firewall Perimetral”

Presenta
Angel Ramírez Ramírez

Cuitláhuac, Ver., a 20 de Abril de 2018.



Programa Educativo
Tecnologías de la Información

Nombre del Asesor Industrial
Reyna Patricia Floresvillar Sevilla

Nombre del Asesor Académico
Erik Gerardo Martínez Galindo

Jefe de Carrera
Lic. Cesar Aldaraca Juárez

Nombre del Alumno
Angel Ramírez Ramírez

Contenido

RESUMEN	1
CAPÍTULO 1. INTRODUCCIÓN	2
1.1 Estado del Arte	2
1.2 Planteamiento del Problema	4
1.3 Objetivos	4
1.4 Definición de variables	4
1.5 Hipótesis.....	5
1.6 Justificación del Proyecto.....	5
1.7 Limitaciones y Alcances.....	5
1.8 La Empresa (TECAPPS).....	6
CAPÍTULO 2. METODOLOGÍA	7
CAPÍTULO 3. DESARROLLO DEL PROYECTO.....	9
4.1 Resultados	32
TABLA DE DIRECCIONES EN LA ZONA TRUST	52
4.2 Trabajos Futuros.....	164
4.3 Recomendaciones	164
ANEXOS	165
BIBLIOGRAFÍA.....	169

Tabla de ilustraciones

ILUSTRACIÓN 1 FACES	9
ILUSTRACIÓN 2 CONFIGURACION DE DOS EQUIPOS JUNIPER.....	17
ILUSTRACIÓN 3 INTERFACES NETWORK.....	18
ILUSTRACIÓN 4 TUNNEL INTERFACE	19
ILUSTRACIÓN 5 FASE 1 GATEWAY.....	19
ILUSTRACIÓN 6 PARAMETROS	20
ILUSTRACIÓN 7 CREACION DE VPN	20
ILUSTRACIÓN 8 NOMBRE DE LA VPN	21
ILUSTRACIÓN 9 CONFIGURACION DE RUTAS.....	21
ILUSTRACIÓN 10 RUTAS	22
ILUSTRACIÓN 11 CREACION DE POLITICA	23
ILUSTRACIÓN 12 CREACION DE POLITICAS DE RED.....	24
ILUSTRACIÓN 13 ACTIVAR NATEO.....	24
ILUSTRACIÓN 14 PARAMETROS	25
ILUSTRACIÓN 15 TRES POLITICAS.....	25
ILUSTRACIÓN 16 ZONA UNTRUST	31
ILUSTRACIÓN 17 REENVIO DE RUTAS.....	32
ILUSTRACIÓN 18 INFRAESTRUCTURA DE CONECTIVIDAD.....	33
ILUSTRACIÓN 19 CONEXIÓN PPPOE POR WEB	38
ILUSTRACIÓN 20 ASIGNACION DE IP PUBLICA	39
ILUSTRACIÓN 21 CONFIGURACION INICIAL	165
ILUSTRACIÓN 22 COMPAÑEROS DEL TRABAJO.....	166
ILUSTRACIÓN 23 ACCESS POINT.....	166
ILUSTRACIÓN 24 CAMARA DE SEGUIRIDAD	166
ILUSTRACIÓN 25 RACK	167
ILUSTRACIÓN 26 RACK	167
ILUSTRACIÓN 27 PRUEBA DEL PROBLEMA DE LA EMPRESA.....	168

TABLAS

TABLAS 1TECAPPS	35
TABLAS 2 DE USUARIO Y PASSWORD DE INFINITUM.....	39
TABLAS 3 TECAPPS EN LA CONFIGURACIÓN PPPOE	41
TABLAS 4 RUTEO POR DESTINO	43
TABLAS 5 RUTEO UNTRUST-VR	46
TABLAS 6 RUTEO VR-INFINITUM	47
TABLAS 7 RUTEO POR ORIGEN > TRUST-VR	49
TABLAS 8 TABLA DE DIRECCIONES EN LA ZONA TRUST	54
TABLAS 9 DE GRUPOS DE DIRECCIONES EN LA ZONA TRUST.....	56
TABLAS 10 DE DIRECCIONES EN LA ZONA UNTRUST	57
TABLAS 11 DIRECCIONES EN LA ZONA DMZ.....	58
TABLAS 12 DIRECCIONES EN LA ZONA DEDICADO	59
TABLAS 13 DIRECCIONES EN LA ZONA INFINITUM	60
TABLAS 14 TABLA DE LISTA DE SERVICIOS	63
TABLAS 15 VPN's	65
TABLAS 16 DEFINICIÓN DE NATEOS (MIP, VIP)	68
TABLAS 17 POLÍTICAS DMZ-UNTRUST.....	71
TABLAS 18 POLÍTICAS DMZ-TRUST.....	71
TABLAS 19 POLÍTICAS TRUST-DEDICADO	72
TABLAS 20 POLÍTICAS DEDICADO- TRUST	74
TABLAS 21 POLÍTICAS TRUST-DMZ.....	75
TABLAS 22 POLÍTICAS TRUST – INFINITUM	76
TABLAS 23 POLÍTICAS TRUST – UNTRUST	76
TABLAS 24 POLÍTICAS UNTRUST- TRUST	77
TABLAS 25 POLÍTICAS DMZ-INFINITUM	77
TABLAS 26 POLÍTICAS DMZ-DEDICADO.....	79
TABLAS 27 POLÍTICAS DEDICADO-INFINITUM.....	79
TABLAS 28 POLÍTICAS DEDICADO- DMZ.....	82
TABLAS 29 POLÍTICAS INFINITUM-DEDICADO.....	83
TABLAS 30 POLÍTICAS INFINITUM-TRUST.....	83
TABLAS 31 POLÍTICAS INFINITUM-DMZ	84

RESUMEN

El presente documento describe el proceso que se llevó a cabo de la seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática, dadas las cambiantes condiciones, la posibilidad de interconectarse a través de redes; al mismo tiempo que se han abierto brechas de inseguridad en diversos sistemas, situación que ha llevado a la aparición de nuevas amenazas en los sistemas computarizados.

En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para proteger, por lo cual, se necesita concientizar a cada uno de los miembros de la organización sobre la importancia, la información sensible y servicios críticos que permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

Analizar e implementar la combinación de reglas y políticas de acceso a la red de datos para la prevención y detección de intrusos y software malicioso, desde el perímetro de la organización con base a la combinación de estrategias.

En el presente documento encontraras los antecedentes de la empresa así como la problemática que actualmente enfrenta y a la cual nos damos a la tarea de solucionar para ello tuvimos que dividir el proyecto en varias secciones las cuales se presentan en las páginas siguientes iniciando con el objetivo general y los específicos que se pretenden alcanzar en así como él porque es importante, contenido en la justificación del mismo y el tipo de metodología utilizado explicando en que consiste y para qué es importante en el desarrollo del proyecto

CAPÍTULO 1. INTRODUCCIÓN

El termino seguridad de la información, seguridad informática y garantía de la información son usados con frecuencia, aunque su significado no es el mismo, persiguen una misma finalidad al proteger la información. al conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información .

En caso de que la información confidencial de una empresa o compañía, los clientes, su información, sus decisiones y su estado financiero caigan en manos de un competidor, salgan a la luz o se vuelvan públicas de forma no autorizada, podría ser pérdida de credibilidad de los clientes, perdidas de negocios, demandas legales o incluso la quiebra de la misma.

1.1 Estado del Arte

Un cortafuego (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Historia del Firewall

El término firewall / fireblock significaba originalmente una pared para confinar un incendio o riesgo potencial de incendio en un edificio. Más adelante se usa para referirse a las estructuras similares, como la hoja de metal que separa el compartimiento del motor de un vehículo o una aeronave de la cabina. 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 Kshitiij, 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 los cortafuegos, 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

1.2 Planteamiento del Problema

La empresa TECAPPS Improve your experience. Especializadas soluciones empresariales de comunicación, colaboración, comunicaciones unificadas, grabación voz y video, contactcenter, video colaboración en tiempo real, redes y servicios relacionados para empresas pequeñas, medianas y grandes tiene el problema que cuenta con una escasez de seguridad informática, teniendo así ataques cibernéticos, como también fuga de información poniendo en riesgo la integridad, confiabilidad e integridad. La empresa propone analizar e implementar la combinación de reglas y políticas de acceso a la red de datos para la prevención y detección de intrusos y software malicioso, desde el perímetro de la organización con base en la combinación de estrategias.

1.3 Objetivos

Analizar e implementar la combinación de reglas y políticas de acceso a la red de datos para la prevención y detección de intrusos y software malicioso, desde el perímetro de la organización con base a la combinación de estrategias.

Objetivos específicos:

- Realizar la implementación de firewall JUNIPER
- Realizar las pruebas locales y externas para delimitar la seguridad de infraestructura de red.
- Implementar un sistema de prevención de intrusos de la red, proporcionado por el mismo proveedor de firewall JUNIPER.
- Monitorear el tráfico que fluye a través de su enlace
- Controlar el tráfico en redes de ordenadores para así lograr optimizar o garantizar el rendimiento
- Implementar método para prevenir el correo basura.

1.4 Definición de variables

- Información desactualizada
- Entorno en el que se ejecutan los equipos
- Ausencia de personal
- Falta de tiempo
- El control de equipos

1.5 Hipótesis

Un firewall o cortafuegos es un dispositivo de hardware o un software que nos permite gestionar y filtrar la totalidad de tráfico entrante y saliente que hay entre 2 redes u ordenadores de una misma red. La función de un firewall es proteger los equipos individuales, servidores o equipos conectados en red contra accesos no deseados de intrusos que nos pueden robar datos confidenciales, hacer perder información valiosa o incluso denegar servicios en nuestra red

La implementación que se llevó a cabo es para resolver el problema de la empresa TECAPPS se organizó pruebas donde se indicaba que cualquier persona podía acceder a la red sin restricción en cual era una vulnerabilidad muy importante y muy crítica ya que podía robar información delicada y confidencial de la empresa por lo cual se implementó un firewall en perímetro de red solamente para tener accesos a la red.

1.6 Justificación del Proyecto

Un Firewall es una forma de mitigar estos ataques es mediante la protección de un equipo firewall que se encargue de gestionar y controlar todas las conexiones que se hagan desde y hacia la red interna del lugar que deseamos proteger es una de las mejores alternativas que poseemos para poder proteger nuestras redes y para ellos debemos aprender los métodos, se implementó ya que es uno de los mejores en posicionado como la tecnología en seguridad, hoy en día la empresa TECAPPS en su red se encuentra segura, ya que se implementó un firewall en el perímetro red permitiendo los accesos solamente de las IPS permitidas solicitada por el cliente, ya si con esto nadie más podrá acceder a esta red. Prácticamente el firewall se convierte en el portero de nuestro edificio, en el primer filtro y puerta que podemos controlar para evitar ataques.

1.7 Limitaciones y Alcances

ALCANCE

Firewall es un sistema o un grupo de sistemas que impone una o varias políticas entre una red o unos equipos privados e internet, determinando que servicios de red son accesibles para los usuarios como externos e internos.

LIMITACIONES

- firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación.

- Firewall no puede protegerse de las amenazas a que está sometido por traidores o usuarios inconscientes.
- Firewall no puede protegerse contra los ataques posibles a la red interna por virus informáticos a través de archivos y software.

1.8 La Empresa (TECAPPS)

HISTORIA DE LA EMPRESA

La empresa TECAPPS, fue fundada por el Ingeniero Gerardo Padilla en el año del 2016 con la intención de ser una empresa que provee soluciones empresariales de comunicación, colaboración, comunicaciones unificadas, grabación voz y vídeo, Contact Center, vídeo colaboración en tiempo real, redes y servicios relacionados. Todo para empresas pequeñas, medianas y grandes.

Son reconocidos por su experiencia, capacidad y dedicación de cada uno de los elementos que integra su organización, así como por el compromiso de servicio que tienen en cada uno de sus clientes, proveedores y personal interno.

VISIÓN

Ser una empresa sólida, comprometida, con valores, orientada a procesos que nos permitirá alcanzar la excelencia con nuestros clientes. Expansión a nivel internacional, garantizar la mejora continua.

MISIÓN

Entregar los mejores productos y servicios, privilegiar la honradez, superar y cumplir las expectativas de nuestros clientes, continuidad de nuestros recursos certificados con actitud de servicio.

PROCESOS QUE SE REALIZAN EN LA EMPRESA

Soluciones empresariales de comunicación, colaboración, comunicaciones unificadas, grabación voz y vídeo, Contact Center, vídeo colaboración en tiempo real, redes y servicios relacionados. Todo para empresas pequeñas, medianas y grandes.

CAPÍTULO 2. METODOLOGÍA

ESPIRAL

El modelo en espiral, propuesto originalmente por Boehm, es un modelo de proceso de software evolutivo que conjuga la naturaleza iterativa de construcción de prototipos con los aspectos controlados y sistemáticos del modelo lineal secuencial. Proporciona el potencial para el desarrollo rápido de versiones incrementales del software. En el modelo espiral, el software se desarrolla en una serie de versiones incrementales. Durante las primeras iteraciones, la versión incremental podría ser un modelo en papel o un prototipo. Durante las últimas iteraciones, se producen versiones cada vez más completas del sistema diseñado.

El modelo en espiral se divide en un número de actividades de marco de trabajo, también llamadas regiones de tareas. Generalmente, existen entre tres y seis regiones de tareas.

- Comunicación con el cliente: Las tareas requeridas para establecer comunicación entre el desarrollador y el cliente.
- Planificación: Las tareas requeridas para definir recursos, el tiempo y otra información relacionadas con el proyecto.
- Análisis de riesgos: Las tareas requeridas para evaluar riesgos técnicos y de gestión.
- Ingeniería: Las tareas requeridas para construir una o más representaciones de la aplicación.
- Construcción y acción: Las tareas requeridas para construir, probar, instalar y proporcionar soporte al usuario (por ejemplo: documentación y práctica).
- Evaluación del cliente: Las tareas requeridas para obtener la reacción del cliente según la evaluación de las representaciones del software creadas durante la etapa de ingeniería e implementada durante la etapa de instalación.

Cada una de las regiones está compuesta por un conjunto de tareas del trabajo, llamado conjunto de tareas, que se adaptan a las características del proyecto que va a emprenderse. Para proyectos pequeños, el número de tareas de trabajo y su formalidad es bajo. Para proyectos mayores y más críticos cada región de tareas contiene tareas de trabajo que se

definen para lograr un nivel más alto de formalidad. En todos los casos, se aplican las actividades de protección (por ejemplo: gestión de configuración del software y garantía de calidad del software).

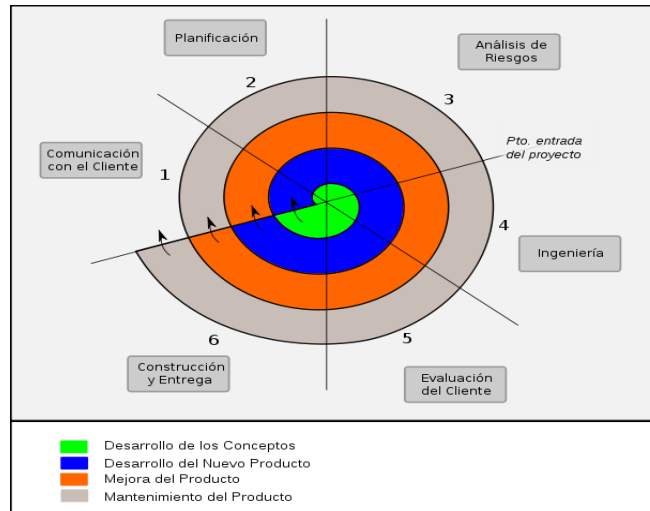
Cuando empieza este proceso evolutivo, el equipo de ingeniería del software gira alrededor de la espiral en la dirección de las agujas del reloj, comenzando por el centro. El primer circuito de la espiral puede producir el desarrollo de una especificación de productos; los pasos siguientes en la espiral se podrían utilizar para desarrollar un prototipo y progresivamente versiones más sofisticadas del software. Cada paso por la región de planificación produce ajustes en el plan del proyecto.

El coste y la planificación se ajustan con la realimentación ante la evaluación del cliente. Además, el gestor del proyecto ajusta el número planificado de iteraciones requeridas para completar el software.

El modelo en espiral es un enfoque realista del desarrollo de sistemas y de software a gran escala. Como el software evoluciona, a medida que progresa el proceso el desarrollador y el cliente comprende y reaccionan mejor ante riesgos en cada uno de los niveles evolutivos.

El modelo en espiral demanda una consideración directa de los riesgos técnicos en todas las etapas del proyecto, y, si se aplica adecuadamente, debe reducir los riesgos antes de que se conviertan en problemáticos. Pero al igual que otros paradigmas, el modelo en espiral no es la panacea. Puede resultar difícil convencer a grandes clientes (particularmente en situaciones bajo contrato) de que el enfoque evolutivo es controlable.

Requiere una considerable habilidad para la evaluación del riesgo, y cuenta con esta habilidad para el éxito. Si un riesgo importante no es descubierto y gestionado, indudablemente surgirán problemas. Finalmente, el modelo no se ha utilizado tanto como los paradigmas lineales secuenciales o de construcción de prototipos. Todavía tendrán que pasar muchos años antes de que se determine con absoluta certeza la eficacia de este nuevo e importante paradigma



CAPÍTULO 3. DESARROLLO DEL PROYECTO

DESCRIPCIÓN DE UN FIREWALL.

Un firewall es un sistema o un grupo de sistemas que impone una o varias políticas entre una red o unos equipos privados e internet, determinando que servicios de red son accesibles para los usuarios como externos e internos. Para que así el firewall funcione de forma efectiva, todo el tráfico de la información tendrá que pasar por él, para poder ser inspeccionado mediante el uso de las políticas de seguridad y supervisar los registros de seguridad creando un perímetro de defensa para proteger la información.

Las principales funciones de los firewalls o como se dice en español cortafuegos son las siguientes:

- Bloquear el acceso a determinados lugares en internet (redes, subredes, nodos específicos), o prevenir que ciertos usuarios o maquinas puedan acceder a ciertos servidores o servicios y bloquear el acceso a nuestra res o equipo desde ciertas maquinas.
- Filtrar los paquetes que circulan entre la red local e internet, de modo que solo aquellos correspondientes a servicios permitidos puedan pasar (Telnet, e-mail, ftp, www...).
- Vigilar el tráfico.
- Supervisar el destino, origen y cantidad e información enviados y recibidos.

Un firewall puede permitir desde una red local hacia internet servicios de web, correo y ftp, pero no a IRC que puede ser innecesario para nuestro trabajo. También podemos configurar accesos que se hagan desde internet hacia la red local y podemos denegarlos de todos modos o permitir algunos servicios como el de la web.

BENEFICIOS DEL FIREWALL.

Uno de los puntos a favor para la implementación de un firewall en una red:

Uno beneficio clave de un Firewall es la simplificación del trabajo para el administrador de la red, ya que permite gestionar un solo equipo, el Firewall, y así proteger al resto sin modificar los cientos de posibles computadores que existen en la red, evitando que se reduzca su tiempo.

Así se pueden examinar a fondo los archivos y conocer las páginas a las que se han ingresado, qué procesos o programas han entrado a Internet, y saber qué usuario ha hecho qué. Es muy útil porque para aplicar sanciones se tienen pruebas sólidas de lo sucedido.

Cabe aclarar que si uno de los usuarios está empeñado en acceder a la red privada de la institución o quiere filtrar información este lo puede lograr si se empeña en hacerlo. La misión de un Firewall es hacer más dura esta labor, más no imposible, porque no se puede; la seguridad total no existe. Por más segura que pueda ser una red siempre habrá un eslabón débil en esta cadena: el factor humano. A una persona se le puede engañar para que revele contraseñas, ayude a descubrir agujeros de seguridad o reemplace al atacante.

IMPLEMENTACION DE UN FIREWALL JUNIPER

CONEXIÓN DE UN FIREWALL

La conexión para un firewall necesita un enlace que nos brinde conexión a internet para poder empezar a ocupar los recursos que nos provee el equipo.

Existen dos maneras de realizar la conexión.

1. Conectando el equipo a un router, esto implica que el firewall se le asignó una IP pública.

2. Conectando a un modem y de esta manera obtendrá una IP privada por DHCP, o bien, asignar una dirección IP privada de manera estática.

Una vez realizado lo anterior se debe hacer pruebas de conectividad, una de ellas puede ser mandando un ping del firewall a un DNS público (4.2.2.2), si el ping es exitoso se procede a dar salida de internet a la LAN.

Ya así tenemos las dos formas de poder tener conexión con un firewall y empezar a configurar con las necesidades necesarias para la empresa.

GENERACIÓN DE ZONAS DE SEGURIDAD (TRUST, UNTRUST, DMZ). ZONA DE SEGURIDAD

Una zona de seguridad es el área de la informática que se enfoca en la protección de la infraestructura computacional todo lo relacionado con esta y, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras. Para ellos existen una serie de estándares, protocolos métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

El conjunto de uno o varios segmentos de red que comparten las mismas necesidades y que se requieren que se controle el tráfico entrante y saliente mediante políticas de seguridad, las zonas de seguridad tienen asociadas una o varias interfaces.

Las zonas de seguridad por default son TRUST, UNTRUST Y DMZ

TRUST: en esta zona se encuentra la red LAN (red segura).

UNTRUST: en esta zona se encuentra la red hacia internet.

DMZ: en esta zona se encuentran los servidores que pueden ser accesados por la red externa.

En la configuración de un firewall se pueden crear las zonas de seguridad dependiendo a las necesidades de la empresa.

CONEXIÓN A INTERNET, ZONA TRUST

Conexión a internet o acceso a internet es un mecanismo de enlace con que una red o una computadora cuentan para conectarse a internet, lo que permite visualizar páginas desde un navegador y/o poder acceder a otros servicios que ofrezca la red. Hay varias formas de acceder a internet desde la conexión vía línea conmutada, banda de ancha fija (cable de fibra óptica, cobre o cable coaxial), wifi, vía banda ancha móvil, vía satelital y teléfonos celulares o móviles con tecnología 2G/3G/4G.

Para que la red LAN pueda tener acceso a internet se debe aplicar una política de seguridad permitiendo el tráfico saliente, para que la conexión sea exitosa la política debe llevar un NAT o de otra forma es mediante un NAT en la interfaz, es más conveniente realizarlo por política ya que se puede controlar el tráfico saliente.

CAMBIAR LA DIRECCIÓN IP DE ADMINISTRACIÓN

La dirección IP de administración en JUNIPER por default la tiene la bgroup0 que contiene la interfaz Ethernet 0.2, 0.3 y 0.4 que tiene una dirección IP 192.168.1.1 para así poder administrar el equipo vía web, para seguridad del equipo se debe cambiar la IP de administración ya que cualquier tipo de persona que conozca las configuraciones del firewall puede administrarlo sin autorización.

CAMBIO IP DE ADMINISTRACIÓN

Dependiendo de la configuración que se obtenga, la IP se va administrar por la red por la cual el usuario requiera su conexión esto es en el listado de las interfaces, editando la requerida y colocar la nueva IP de administración y asignar a las personas encargadas que puedan acceder a ellas para poder modificar y eliminar lo necesario para las necesidades de ella.

CONFIGURACIÓN DE NAT DE DESTINO PARA PUBLICAR UN SERVIDOR EN LA DMZ

El NAT es la traducción de direcciones IPs, por lo regular de IPs privadas a IPs públicas, una de las utilidades del NAT es para dar salida a internet de la red interna o publicar servicios.

En los equipos de Juniper Networks existen 5 tipos de NAT que son VIP, MIP, DIP, SOURCE Y DESTINATION.

- VIP: el vip es un tipo de NAT para poder publicar servicio de una IP pública a “n” direcciones IP privadas, donde hace referencia a la IP pública hacia a la IP privada es mediante diferentes puertos, pero con una única IP pública (1: N).
- MIP: es un tipo de NAT que publica servicios de diferentes IPs publicas hacia diferentes IPs privadas, de una IP a una IP (1:1).
- DIP: permite configurar una serie o conjunto de direcciones IP desde las que el dispositivo de Juniper Networks puede tomar dinámicamente direcciones a utilizar al realizar nat. Al configurar grupos de direcciones en una interfaz el rango de dirección en un conjunto el DIP debe estar en la misma subred que la dirección IP asociada a un poco con eso, cualquier interfaz de la dirección de la interfaz, una dirección secundaria en la interfaz, o una dirección extendida en la interfaz.
- SOURCE: esta función basada en interfaces sin las limitaciones de la zona. la dirección de origen se es traducido a la dirección de la interfaz outbound. Traducción de puertos garantiza que cada sesión se identificó a unívocamente.
- DESTINATION: Tipo de nateo que se aplica de manera unidireccional basado en la interfaz donde se origina la sesión, una dirección pública se traslada a una dirección interna identificada en un pool de direcciones declaradas previamente.

CONFIGURACIÓN DE UNA VPN

Una VPN (Red Privada Virtual) es una extensión de una red local y privada que utiliza como medio de enlace una red pública como, por ejemplo, Internet. Este método permite enlazar dos o más redes simulando una única red privada permitiendo así la comunicación entre computadoras como si fuera punto a punto. Las Redes Privadas Virtuales utilizan tecnología de túnel (tunneling) para la transmisión de datos mediante un proceso de encapsulación y en su defecto de encriptación.

Una de las principales ventajas de una VPN es la seguridad, los paquetes viajan a través de infraestructuras públicas (Internet) en forma encriptado y a través del túnel de manera que sea prácticamente ilegible para quien intercepte estos paquetes. Esta tecnología es muy útil para establecer redes que se extienden sobre áreas geográficas extensas, por ejemplo, diferentes ciudades y a veces hasta países y continentes.

Las ventajas de utilizar las vpn's son:

- Integridad, confidencialidad y seguridad de datos.
- Las VPN reducen los costos y son sencillas de usar.
- Facilita la comunicación entre dos usuarios en lugares distantes.

CONFIGURACIÓN DE RUTAS ESTÁTICAS

Una ruta nos sirve para poder llegar a un destino.

Enrutamiento estático

Es una ruta fija predeterminada por el administrador de la red las rutas estáticas no se actualizan por si solas deben actualizarse por el administrador de forma manual.

Unas de las ventajas de las rutas estáticas son:

- Se configura manualmente.
- Son más estables.
- Manejan rutas por defecto.
- Fácil de configurar en redes pequeñas.
- Usan menos de ancho en banda.

Unas de sus desventajas son:

- El administrador debe tener una gran comprensión de la red.
- Si se agrega una nueva red debe agregarse en todos los routers.
- En grandes redes la actualización puede ser más complicada de hacer.

CONFIGURACIÓN DE POLÍTICAS DE SEGURIDAD, SÓLO PERMITIR LA CONEXIÓN AL SERVIDOR EN DMZ, Y DEFINIR ACCESO SÓLO A CIERTOS SERVICIOS EN LA INTERNET.

Una política de seguridad permite o deniega el tráfico entre zonas, en una política de seguridad se puede configurar el acceso o la denegación para un segmento de red o solamente algunos hosts así mismos se puede configurar solamente ciertos servicios como, por ejemplo: HTTP, HTTPS, FTP, ICMP, TELNET, etc. de esta manera es como se permite o se niega el acceso a los diferentes servidores.

CONFIGURACIÓN DE ENLACES REDUNDANTES

Redundancia, junto con alta disponibilidad comprenden la capacidad de un sistema de comunicación para detectar un fallo en la red de la manera más rápida posible y que a la vez sea capaz de recuperarse del problema de forma eficiente y efectivo, afectando lo menos posible al servicio.

La redundancia hace referencia a nodos completos que están replicados o componentes de estos, así como caminos u otros elementos de la red que están repetidos y que una de sus funciones principales es ser utilizados en caso de que haya una caída del sistema.

El equipo JUNIPER maneja virtual routers, los cuales son ruteadores internos que permiten la comunicación entre diferentes instancias de firewall que se encuentran operando concurrentemente en un solo dispositivo. Esto quiere decir, que todas las instancias de firewall son independientes entre sí. De esta manera es como Juniper maneja la redundancia, realizando la configuración de cada enlace en diferentes instancias de virtual router.

CONFIGURACIÓN DE QOS (TRAFFIC SHAPING).

Traffic Shaping (catalogación de tráfico en español) intenta controlar el tráfico en las redes para así lograr optimizar o garantizar el rendimiento, el traffic shaping propone conceptos de clasificaciones, colas, imposición de políticas, administrativas de congestión y calidad de servicio (Qos).

CONFIGURACIÓN DE FUNCIONALIDADES UTM

IPS (IDP).

IPS (Sistema de prevención de intrusos en español) ejerce un control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de prevención de intrusos es considerada por algunos como una extensión de los sistemas de detección de intrusos (IDP) pero en realidad es otro tipo de control de acceso, más cercano a los que son los firewall.

Los dispositivos de detención y prevención de intrusos tienen como funciones detectar accesos no permitidos a una red, poseen sensores que les permite obtener datos que cuando detecta tráfico le permita identificar por medio de anomalías o comportamientos extraños si se trata de un ataque o de un falso positivo.

El modo del funcionamiento es analizar a un nivel muy profundo el tráfico de red, en un momento donde dicho tráfico pasa sea con firmas de ataques ya reconocidos, así como también se controlan los comportamientos extraños como el escaneó de puertos.

FILTRADO WEB.

El filtrado Web le permite administrar el acceso a Internet y evitar el acceso a contenido de Web inapropiado. ScreenOS proporciona dos soluciones de filtrado Web:

- El filtrado de web integrado le admitir o bloquear el acceso a un sitio solicitado al asociar un perfil de filtrado de Web a una directiva de pared de fuego. Un perfil de filtrado de Web específica las categorías de URL y la acción que toma el dispositivo de seguridad (permitir o bloquear) cuando recibe una petición para acceder a una URL en cada categoría. Las categorías de URL son predefinidas y mantenidas por Surf Control o las define el usuario.
- El filtrado de Web redirigido redirige el dispositivo de seguridad para enviar la primera petición de HTTP en una conexión TCP a un servidor Websense o a un servidor Surf Control, lo que permite bloquear o permitir el acceso a diferentes sitios basándose en las URL, nombres de dominio y direcciones IP.

PRUEBAS DE CONEXIÓN EN DOS O MÁS PUNTOS DE MANERA SEGURA.

CONFIGURACIÓN DE DOS EQUIPOS JUNIPER

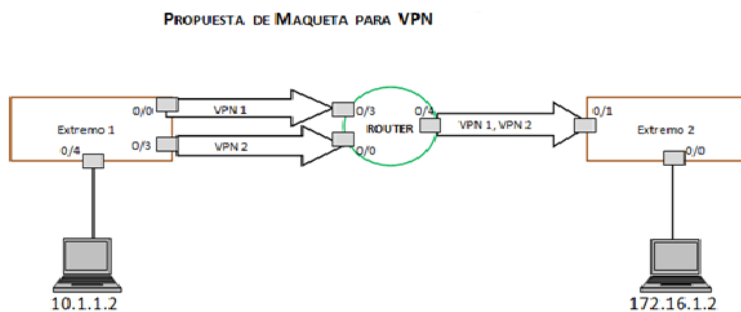


ILUSTRACIÓN 2 CONFIGURACION DE DOS EQUIPOS JUNIPER

CONFIGURACIÓN DE DISPOSITIVOS (EXTREMO 1)

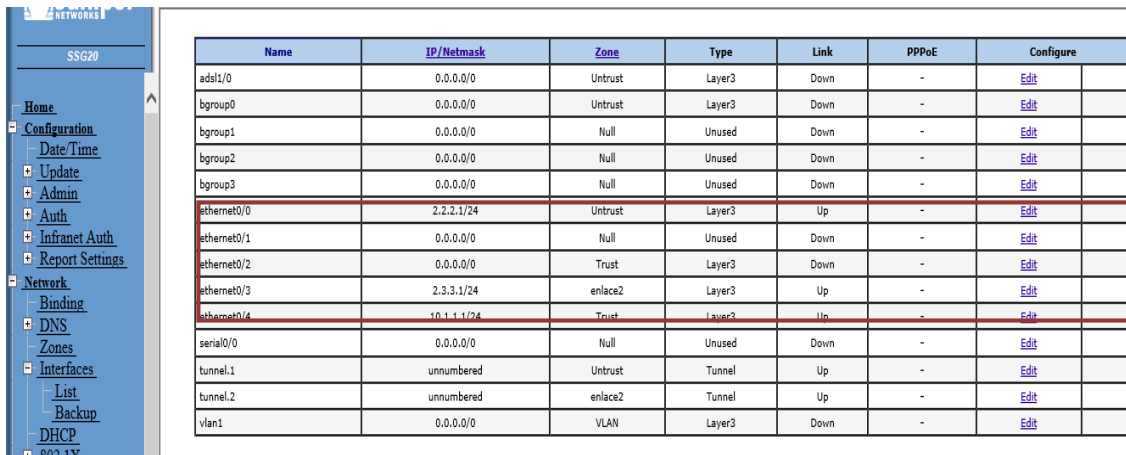
Basándonos en la maqueta, se asigna a cada equipo las interfaces requeridas con sus respectivas direcciones IP, así como a la zona a la cual pertenecerán de acuerdo con la siguiente tabla.

Dispositivo	Interfaz	Dirección IP	Zona	Función
SSG 20				Extremo 1
	0/0	2.2.2.1	Untrust	
	0/4	10.1.1.1	Trust	
	0/3	2.3.3.1	Enlace 2	
SRX240				Router
	0/0	2.3.3.2	Trust	

	0/3	2.2.2.2	Trust
	0/4	1.1.1.2	Untrust
SSG 20			Extremo 2
	0/0	172.16.1.1	Trust
	0/1	1.1.1.1	Untrust

CONFIGURACIÓN DE INTERFACES

Abrimos nuestro navegador > Introducimos la IP del dispositivo (**192.168.1.1**) > Nos autenticamos > **Network>Interfaces**> Seleccionamos la interfaz > **Edit.** >Asignamos IP y zona > **ok.**



Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure
ads1/0	0.0.0.0/0	Untrust	Layer3	Down	-	Edit
bgroup0	0.0.0.0/0	Untrust	Layer3	Down	-	Edit
bgroup1	0.0.0.0/0	Null	Unused	Down	-	Edit
bgroup2	0.0.0.0/0	Null	Unused	Down	-	Edit
bgroup3	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet0/0	2.2.2.1/24	Untrust	Layer3	Up	-	Edit
ethernet0/1	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet0/2	0.0.0.0/0	Trust	Layer3	Down	-	Edit
ethernet0/3	2.3.3.1/24	enlace2	Layer3	Up	-	Edit
ethernet0/4	10.1.1.1/24	Trust	Layer3	Up	-	Edit
serial0/0	0.0.0.0/0	Null	Unused	Down	-	Edit
tunnel.1	unnumbered	Untrust	Tunnel	Up	-	Edit
tunnel.2	unnumbered	enlace2	Tunnel	Up	-	Edit
vlan1	0.0.0.0/0	VLAN	Layer3	Down	-	Edit

ILUSTRACIÓN 3 INTERFACES NETWORK

CREACIÓN DEL TÚNEL PARA VPN1

Network>Interfaces>New> Se especifican los parámetros para el túnel:

- **Tunnel Interface Name** (nombre del túnel)
- Seleccionamos **Unnumbered**
- **Interface** (la interfaz donde empieza el túnel)

- Ok

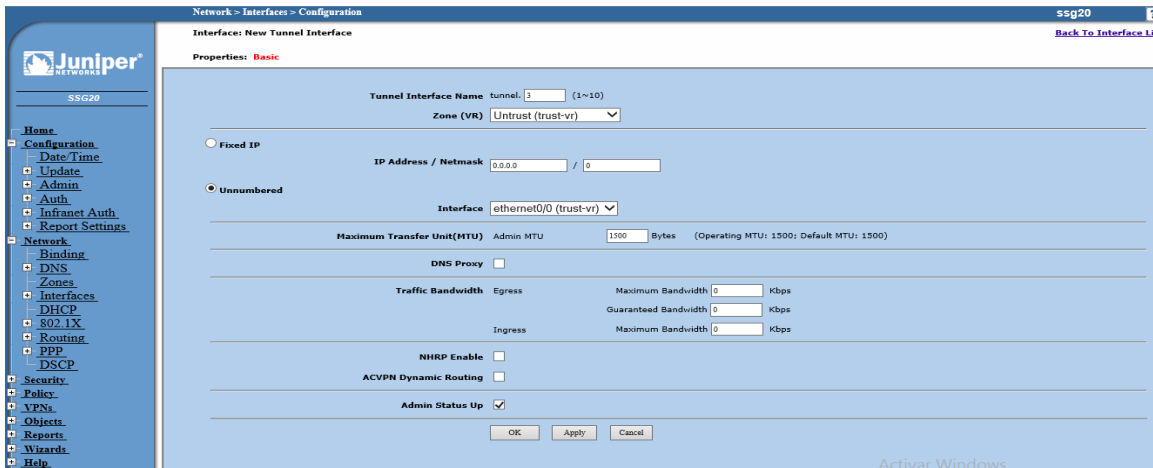


ILUSTRACIÓN 4 TUNNEL INTERFACE

CONFIGURACIÓN DE LA FASE 1 (GATEWAY)

VPNs > AutoKey Advanced > Gateway > New > Se especifica los parámetros del Gateway.

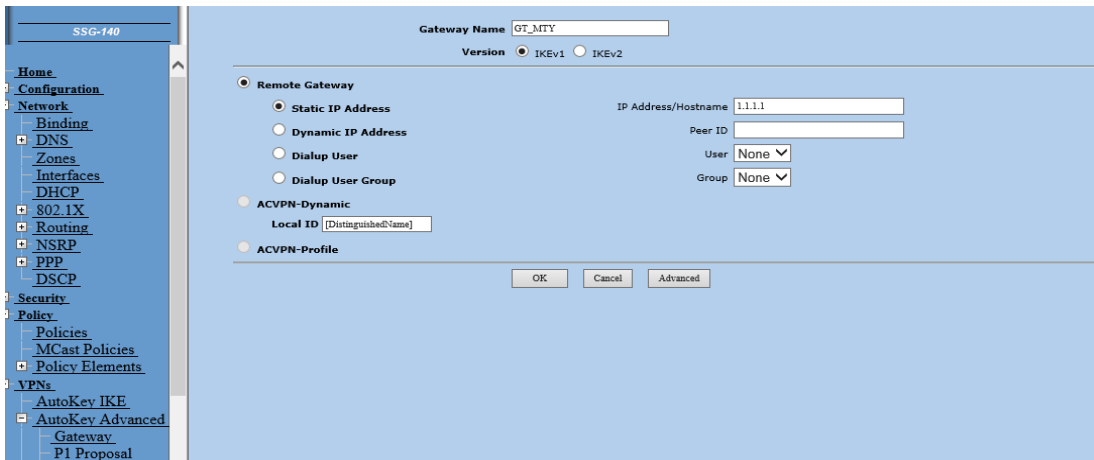


ILUSTRACIÓN 5 FASE 1 GATEWAY

- **Gateway Name** (Nombre del Gateway)
- **IP Address/Hostname** (IP donde acaba el túnel 1)
- Clic en **Advanced**> Establecemos los parámetros faltantes:

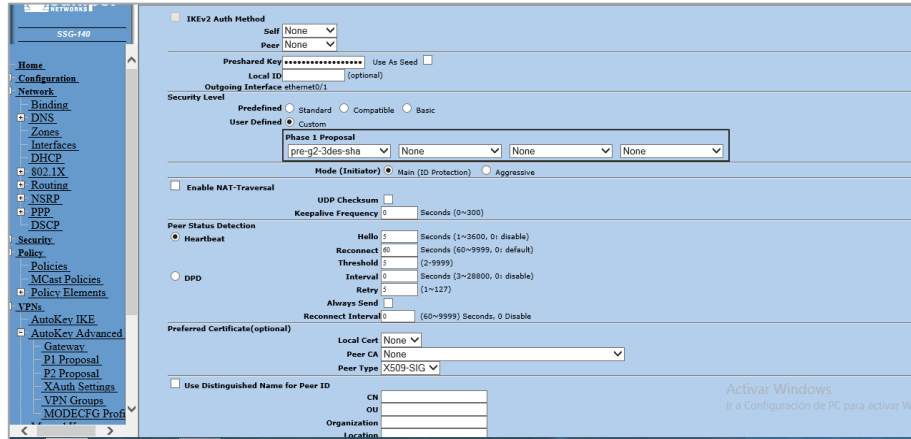


ILUSTRACIÓN 6 PARAMETROS

- **Preshared Key** (Esta clave debe ser la misma para los 2 extremos de la VPN)
- **Outgoing Interface** (La interfaz donde empieza el túnel)
- **Phase 1 Proposal** (Se recomienda que sea pre-g2-3des-sha)
- **Hello** (se establece 5 seconds)
Reconnect (se establece 60 seconds).

CONFIGURACIÓN DE LA FASE 2 (CREACIÓN DE VPN)

VPNs > AutoKey IKE > New > Establecemos los parámetros

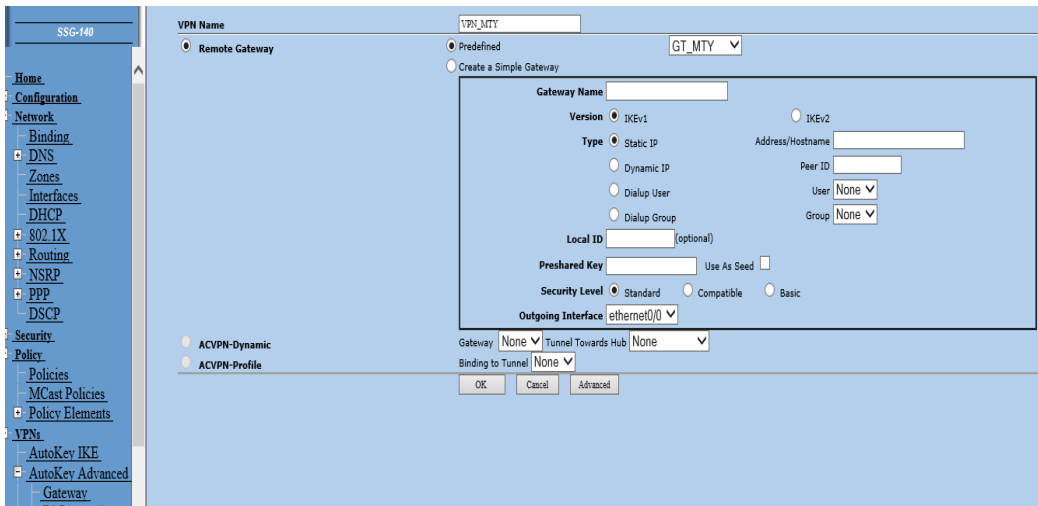


ILUSTRACIÓN 7 CREACION DE VPN

- **VPN Name** (Nombre de la VPN)
- **Predefinid** (Seleccionamos el GW creado en la fase 1)
Clic en **Advanced** > Establecemos los parámetros faltantes

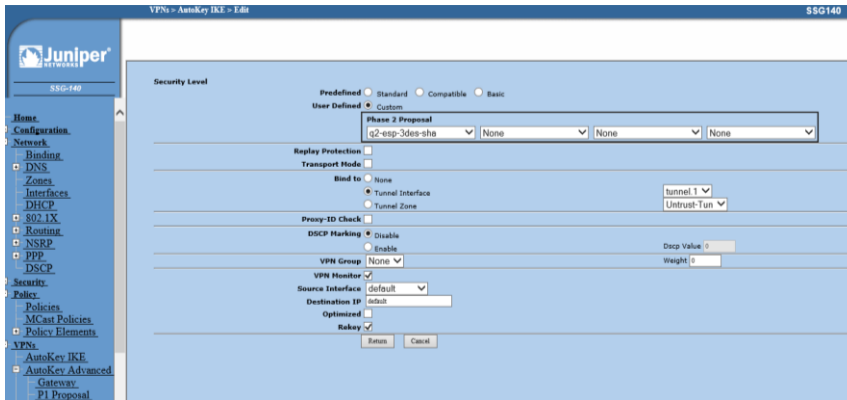


ILUSTRACIÓN 8 NOMBRE DE LA VPN

- **Phase 2 Proposal** (Debe ser la misma que en la fase 1 pre-g2-3des-sha)
- **Túnel Interfaces** (se selecciona el túnel 1)
- Seleccionamos **VPN Monitor** (esto nos muestra si la VPN está activa)
- Se selecciona **Rekey** (con esto se le indica ala VPN que cada intervalo de tiempo tiene que verificar que la VPN2 está activa)
- **Return**
- **Ok**

CONFIGURACIÓN DE RUTAS

Network > Routing > Destination > New > Asignamos los parámetros > OK

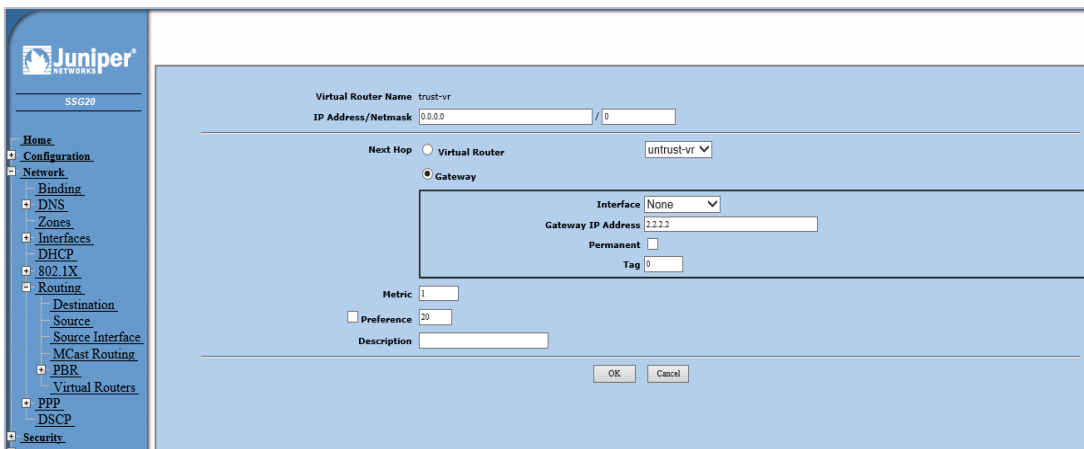
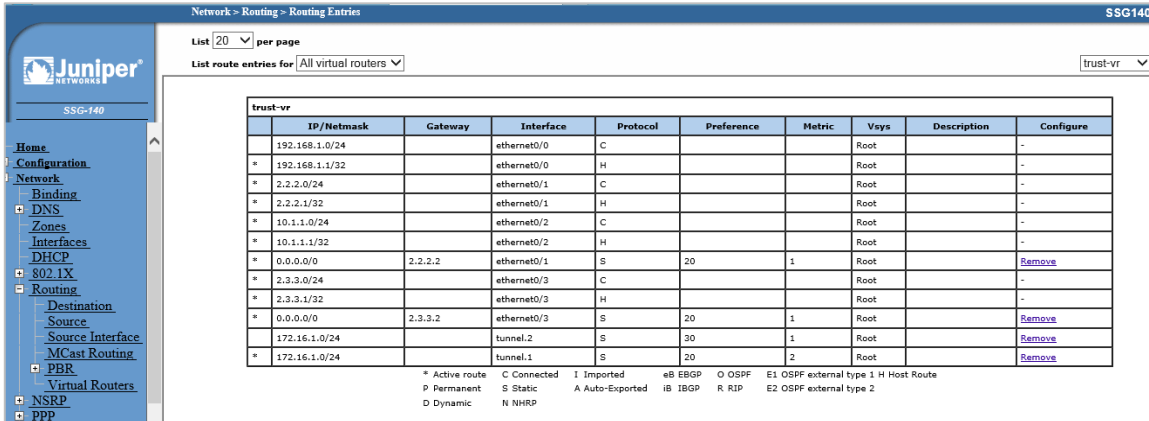


ILUSTRACIÓN 9 CONFIGURACION DE RUTAS

- **IP Address/Netmask** (Dirección destino)
- **Gateway IP Address** (Dirección del Gateway)
-

Quedando las rutas de la siguiente manera



The screenshot shows the Juniper SSG140 configuration interface for Routing Entries. The table displays the following data:

trust-vr	IP/Netmask	Gateway	Interface	Protocol	Preference	Metric	Vsys	Description	Configure
	192.168.1.0/24		ethernet0/0	C			Root	-	
*	192.168.1.1/32		ethernet0/0	H			Root	-	
*	2.2.2.0/24		ethernet0/1	C			Root	-	
*	2.2.2.1/32		ethernet0/1	H			Root	-	
*	10.1.1.0/24		ethernet0/2	C			Root	-	
*	10.1.1.1/32		ethernet0/2	H			Root	-	
#	0.0.0.0/0	2.2.2.2	ethernet0/1	S	20	1	Root		Remove
*	2.3.3.0/24		ethernet0/3	C			Root	-	
*	2.3.3.1/32		ethernet0/3	H			Root	-	
*	0.0.0.0/0	2.3.3.2	ethernet0/3	S	20	1	Root		Remove
*	172.16.1.0/24		tunnel.2	S	30	1	Root		Remove
#	172.16.1.0/24		tunnel.1	S	20	2	Root		Remove

Legend:
 * Active route C Connected I Imported eB EBGP O OSPF E1 OSPF external type 1 H Host Route
 P Permanent S Static A Auto-Exported iB IBGP R RIP E2 OSPF external type 2
 D Dynamic N NHRP

ILUSTRACIÓN 10 RUTAS

CONFIGURACIÓN DE POLÍTICAS

Se busca que los usuarios puedan hacer uso de la VPN, pero al mismo tiempo se les permite la salida a internet, de acuerdo con las necesidades de cada usuario. Para lograr esto nos apoyamos en la creación de políticas dentro del dispositivo.

CREACIÓN DE POLÍTICA PARA VPN

Creamos una política para permitir el paso desde la zona Trust a Untrust, de este modo restringimos el paso por el túnel únicamente a los usuarios que lo soliciten.

Policy > Policies > New > Se establecen los parámetros > Ok

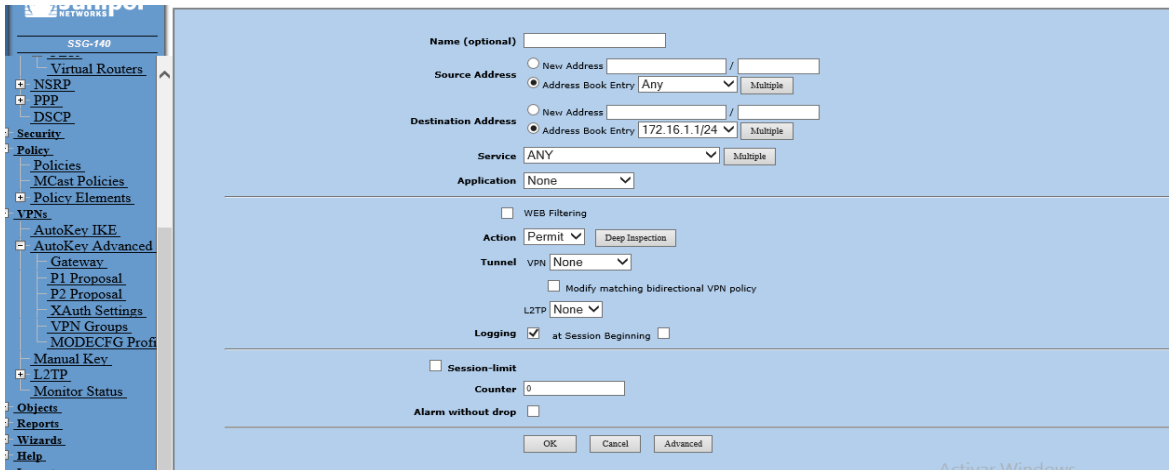


ILUSTRACIÓN 11 CREACION DE POLITICA

- **Source Address** (Dirección o direcciones origen)
- **Destination Address** (Dirección origen)
- **Action** (Las acciones que va tomar la política)
- **Logging** (Activa los logs de la política)

CREACIÓN DE POLÍTICA PARA INTERNET

Creamos una política para permitir el paso desde la zona Trust a Untrust, pero aplicando NAT, de este modo únicamente podrán acceder a internet los usuarios que lo requieran sin necesidad de hacer uso del túnel.

Policy>Policies> New> Se establecen los parámetros

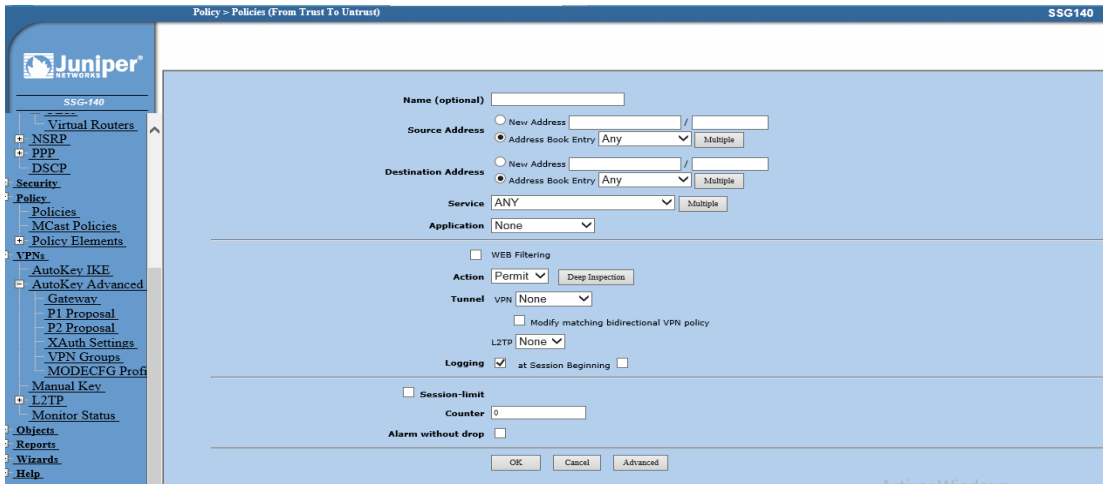


ILUSTRACIÓN 12 CREACION DE POLITICAS DE RED

- **Source Address** (Dirección o direcciones origen)
- **Destination Address** (Dirección origen)
- **Action** (Las acciones que va tomar la política)
- **Logging** (Activa los logs de la política)

Clic en **Advance** > Seleccionamos **Source Translation** para activar el Nateo > **Return** > **OK**

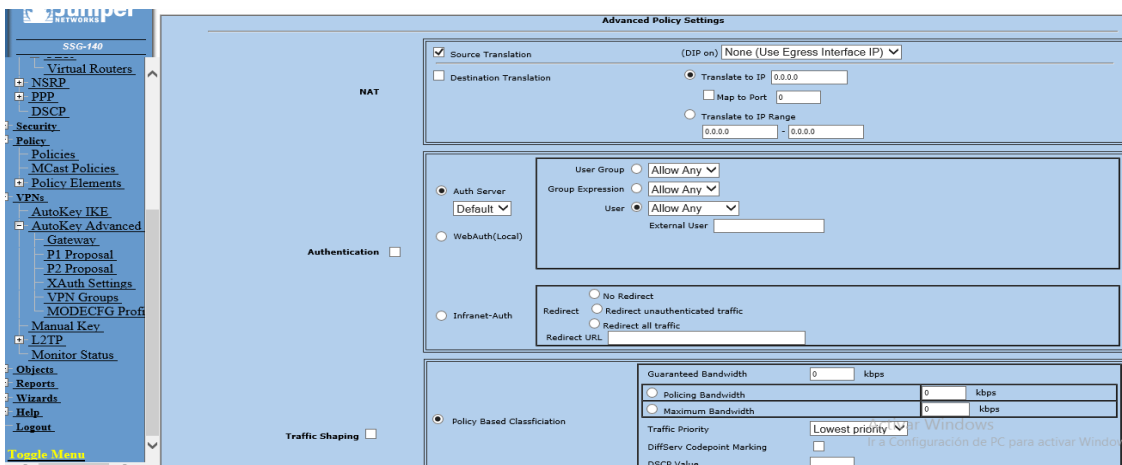


ILUSTRACIÓN 13 ACTIVAR NATEO

CREACIÓN DE POLÍTICA UNTRUST – TRUST

Se crea la política de zona Untrust a Trust, para permitir que la información llegue hasta nuestra red LAN

Policy > Políticas > New > Se establecen los parámetros

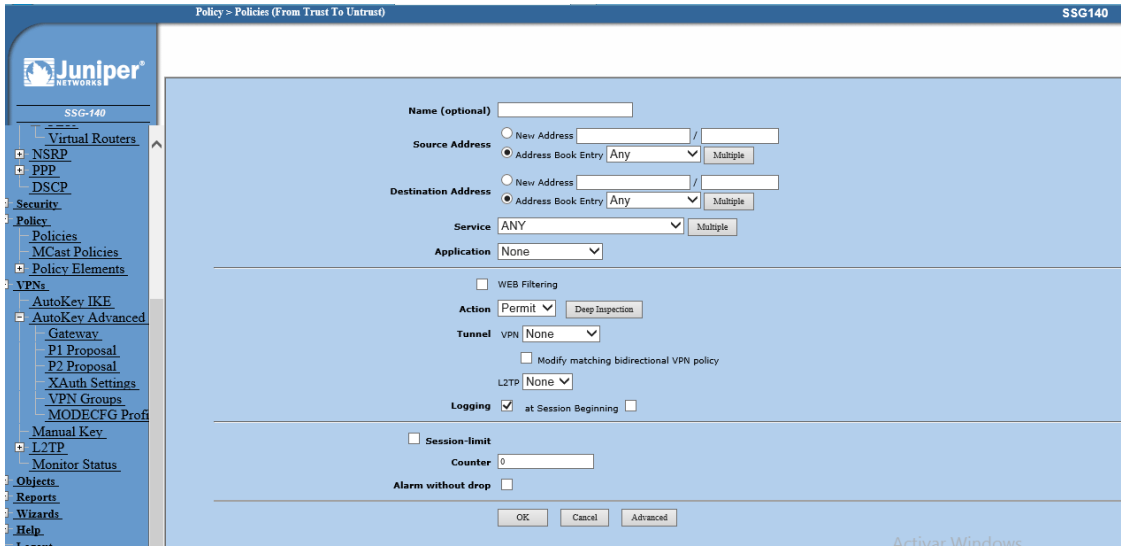


ILUSTRACIÓN 14 PARAMETROS

Quedando nuestras 3 políticas de la siguiente manera:










From Trust To Untrust, total policy: 2										
ID	Source	Destination	Service	Action	Options	Configure			Enable	Move
3	Any	172.16.1.1/24	ANY			Edit	Clone	Remove	<input checked="" type="checkbox"/>	
1	Any	Any	ANY			Edit	Clone	Remove	<input checked="" type="checkbox"/>	
From Untrust To Trust, total policy: 1										
ID	Source	Destination	Service	Action	Options	Configure			Enable	Move
2	Any	Any	ANY			Edit	Clone	Remove	<input checked="" type="checkbox"/>	

ILUSTRACIÓN 15 TRES POLITICAS

IMPLEMENTACIÓN DE LOS DIFERENTES MÓDULOS DE PROTECCIÓN.

ROBUSTECIMIENTO DE LAS POLÍTICAS DE UTM

FILTRADO WEB.

Para activar el filtrado de Web, primero asocia un perfil de filtrado de Web a una directiva. Con el filtrado de Web integrado, el dispositivo de seguridad Juniper Networks intercepta cada petición http, determina si permite o bloquea el acceso a un sitio solicitado al categorizar su URL, luego coincide la categoría de URL a un perfil de filtrado de Web.

Screening > **Web Filtering** > Protocol Selection: **Selecione Integrated**

(Surf Control), luego haga clic en **Apply**. Luego seleccione **Enable Web Filtering**

Vía CPA Server, y nuevamente haga clic en **Apply**.

IPS (IDP).

Los mecanismos de detección y defensa de ataques se describen las opciones de seguridad de Juniper Networks disponibles en ScreenOS. Muchas de ellas son opciones screen que se pueden activar en el nivel de zona de seguridad.

Las opciones screen se aplican al tráfico que llega al dispositivo de seguridad de Juniper Networks a través de cualquier interfaz asociada a una zona para la que se hayan activado dichas opciones. Las opciones SCREEN ofrecen protección contra análisis de puertos y direcciones IP, ataques de rechazo de servicio (DoS) y cualquier otro tipo de actividad maliciosa. Es posible aplicar otras opciones de seguridad de red, como el filtrado de Web, la comprobación antivirus y la detección y prevención de intrusiones (IDP), a nivel de directivas. Estas opciones sólo se aplican al tráfico que se encuentre bajo la jurisdicción de las directivas en las que se activan.

ANTIVIRUS.

Los dispositivos de seguridad de Juniper Networks admiten un analizador antivirus interno que se puede configurar para filtrar el tráfico FTP, HTTP, IMAP, POP3 y SMTP. Si el analizador AV incorporado detecta un virus, descarta el paquete y envía un mensaje al cliente que inició el tráfico para informarle sobre dicho virus.

El análisis AV interno se realiza cuando el motor de análisis del dispositivo analiza el tráfico en busca de virus. El motor de análisis incorporado o interno es un motor de análisis Juniper-Kaspersky.

MONITOREO DE TRÁFICO Y DEPURACIÓN

El dispositivo de seguridad Juniper Networks puede supervisar y registrar el tráfico que autoriza o deniega basándose en las directivas previamente configuradas. Puede habilitar la opción de registro para cada directiva que configure. Al habilitar la opción de registro para una directiva de autorización de tráfico, el dispositivo registra el tráfico autorizado por esa directiva. Al habilitar la opción de registro para una directiva de denegación de tráfico, el dispositivo registra el tráfico que intenta pasar a través del dispositivo pero que resulta anulado por esa directiva.

En un registro de tráfico se anotan los siguientes elementos de cada sesión:

- Fecha y hora de inicio de la conexión
- Duración
- Dirección de origen y número de puerto
- Dirección de origen traducida y número de puerto
- Dirección de destino y número de puerto
- La duración de la sesión
- El servicio utilizado en la sesión.

Para registrar todo el tráfico recibido por un dispositivo de seguridad, debe habilitarse la opción de registro para todas las directivas. Para registrar tráfico específico, habilite el registro solamente para las directivas que afecten a ese tipo de tráfico. Para habilitar la opción de registro de una directiva, ejecute cualquiera de los siguientes procedimientos:

WebUI

Policies > (From: zona_orig, To: zona_dest) New: Seleccione Logging y haga clic en OK.

CLI

set policy from zona_orig to zona_dest dir_orig dir_dest servicio acción log.

Además de registrar el tráfico de una directiva, el dispositivo también puede mantener una cuenta en bytes de todo el tráfico de la red al que se aplicó la directiva. Cuando se habilita la opción de recuento, el dispositivo incluye la siguiente información al mostrar entradas del registro de tráfico.

- Bytes transmitidos de un origen a un destino
- Bytes transmitidos de un destino a un origen

Puede habilitar el recuento de una directiva desde WebUI y desde CLI.

WebUI

Policies > (From: zona_orig, To: zona_dest) New > Advanced: Seleccione Counting, haga clic en Return y luego haga clic en OK.

CLI

set policy from zona_orig to zona_dest dir_orig dir_dest servicio acción log count

Visualización del registro de tráfico

Las entradas del registro de tráfico almacenadas en la memoria flash del dispositivo de seguridad se pueden ver por medio del uso de la CLI o de WebUI:

WebUI

Policies > Logging (para la directiva con ID número) o bien Reports > Policies > (para la directiva con ID número)

CLI

get log traffic policy número

Ejemplo: Visualizar las entradas del registro de tráfico

En este ejemplo se visualizan los detalles del registro de tráfico de una directiva con la identificación número 3, para la que previamente se ha habilitado el registro:

WebUI

Directivas: Haga clic en el icono de registro para la directiva con el número de identificación 3.

Aparece la información siguiente:

- Date/Time: 2003-01-09 21:33:43
- Duration: 1800 seg.
- Source IP Address/Port: 1.1.1.1:1046
- Destination IP Address/Port: 10.1.1.5:80
- Service: HTTP
- Reason for Close: Age out
- Translated Source IP Address/Port: 1.1.1.1:1046
- Translated Destination IP Address/Port: 10.1.1.5:80
- Policy ID number: 3

CLI

get log traffic policy 3 Clasificación y filtrado del registro de tráfico De forma similar al registro de eventos, cuando se utiliza la CLI para ver el registro de tráfico se pueden clasificar o filtrar las entradas del registro según los criterios siguientes:

- Dirección IP de origen o de destino: El registro de tráfico se puede clasificar por direcciones IP de origen o de destino. También se puede filtrar el registro de tráfico especificando una dirección IP de origen o de destino, o bien un rango de direcciones.
- Fecha: El registro de tráfico se puede clasificar por fechas solamente, o bien por fecha y hora. El dispositivo muestra las entradas del registro en orden descendente por fecha y hora. También se pueden filtrar las entradas del registro de eventos especificando una fecha de comienzo, una fecha de final, o bien un intervalo de fechas. Cuando se especifica una fecha de comienzo, el dispositivo muestra las entradas del registro que tengan marcas de fecha/hora posteriores a la fecha de comienzo. Si se especifica una fecha de final, el dispositivo muestra las entradas del registro que tengan marcas de fecha/hora anteriores a la misma.
- Hora: Al clasificar el registro de tráfico por hora, el dispositivo muestra las entradas del registro en orden descendente según su hora, sin importar la fecha. Si se especifica una hora de comienzo, el dispositivo muestra las entradas del registro cuyas marcas de hora sean posteriores a la hora de comienzo especificada, sin importar la fecha. Si se especifica una hora de final, el dispositivo muestra las entradas del registro cuyas marcas de hora sean anteriores a la hora de final especificada, sin importar la fecha. Si se especifica una hora de comienzo y otra de final, el dispositivo muestra las entradas del registro cuyas marcas de hora se encuentren dentro del periodo de tiempo especificado.

APLICACIÓN DE DISTINTOS TIPOS DE POLÍTICAS.

Los dispositivos de seguridad de Juniper Networks aseguran la red inspeccionando, y luego permitiendo o denegando, todo intento de conexión que necesite pasar de una zona de seguridad a otra.

De forma predeterminada, un dispositivo de seguridad denegará todo el tráfico en todos los sentidos. La creación de directivas permite controlar el flujo de tráfico entre zonas definiendo qué tipo de tráfico puede pasar de los orígenes a los destinos especificados en determinado momento de acuerdo con una programación. En el nivel más permisivo, es

posible permitir que todo tipo de tráfico pase de cualquier origen en una zona a cualquier destino en el resto de zonas sin ninguna restricción en el tiempo. En el nivel más restrictivo, se puede crear una directiva que sólo permita un tipo de tráfico entre un host determinado en una zona y otro en otra zona durante un periodo de tiempo programado.

NOTA: Algunos dispositivos de seguridad se suministran con una directiva predeterminada que permite cualquier tráfico saliente de la zona Trust a la zona Untrust, pero rechaza todo el tráfico entrante que procede de la zona Untrust hacia la zona Trust.

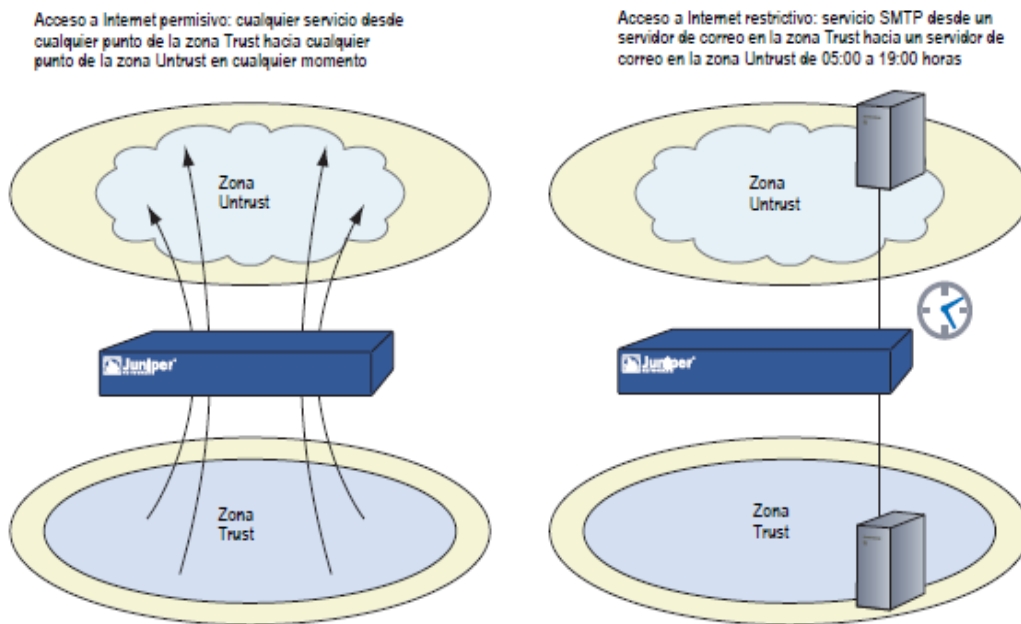


ILUSTRACIÓN 16 ZONA UNTRUST

Cada vez que un paquete intenta pasar de una zona a otra o entre dos interfaces enlazadas a la misma zona, el dispositivo de seguridad comprueba si en su lista de directivas existe alguna que permita ese tipo de tráfico. Para que el tráfico pueda pasar de una zona de seguridad a otra (p. ej., de la zona A a la zona B), es necesario configurar una directiva que permita que la zona A envíe tráfico a la zona B. Para que el tráfico pueda pasar en sentido inverso, se debe configurar otra directiva que permita el tráfico de la zona B a la zona A. Para que cualquier tipo de tráfico pase de una zona a otra, debe haber una directiva que lo permita. Asimismo, cuando está habilitado el bloqueo intrazona (bloqueo del interior de una

zona), deberá existir una directiva que permita que el tráfico pase de una interfaz a otra dentro de esa misma zona.

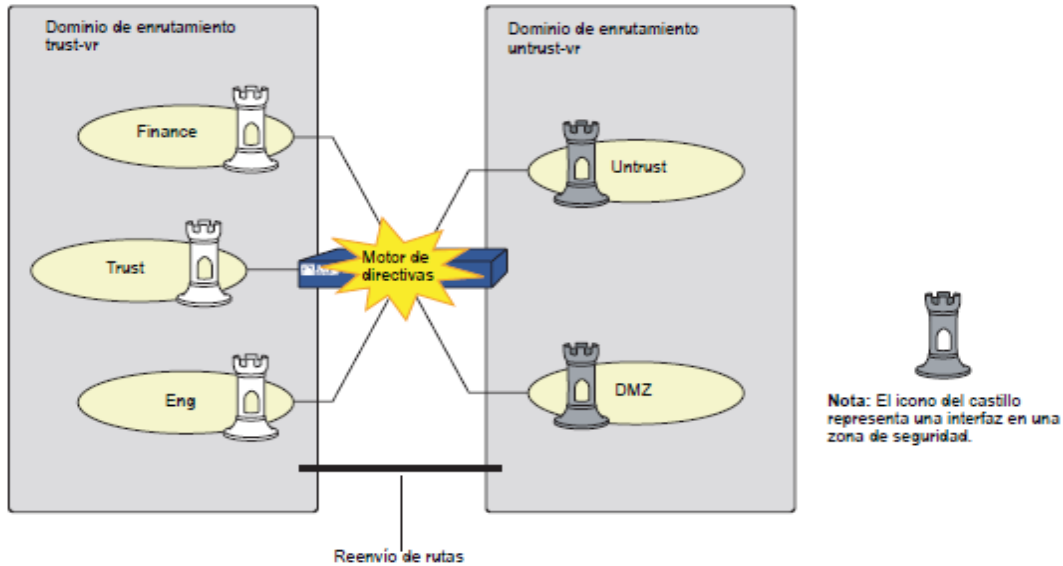


ILUSTRACIÓN 17 REENVIO DE RUTAS

CAPÍTULO 4. RESULTADOS Y CONCLUSIONES

4.1 Resultados

IMPLEMENTACIÓN TOTAL DE UN FIREWALL JUNIPER

A continuación, se mostrará el seguimiento de la implementación total de un firewall JUNIPER Network SSG 140 implementado TECAPPS para cumplir los requerimientos establecidos por Laboratorios TECAPPS

REQUERIMIENTOS

La empresa TECAPPS requiere un esquema de protección completo, implementando a la vez un esquema protección perimetral, administración centralizada y control de acceso, integrando diferentes métodos de seguridad, esto con el fin de contar con un nivel tecnológico de punta.

Es la razón por la cual, Seguridad, empresa de seguridad y consultoría en TI, la cual, cuenta con expertos certificados en plataformas de Seguridad Informática, propuso un esquema de Seguridad y conectividad que resguarde los activos informáticos críticos para la operación de la empresa, brindando también la comunicación segura a todos sus hosts, adoptando como nueva tecnología un Firewall Juniper SSG 140.

La infraestructura de conectividad, quedo de la siguiente manera:

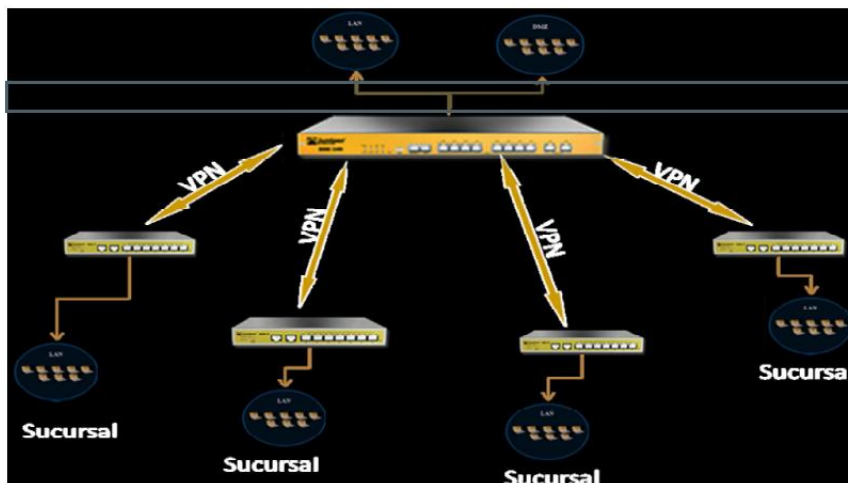


ILUSTRACIÓN 18 INFRAESTRUCTURA DE CONECTIVIDAD

PROCESO DE IMPLEMENTACIÓN

- **Actualización del Sistema Operativo**

Se actualizo el sistema operativo del firewall a la versión ssg5.6.2.0r5.0.zip

FIREWALL SSG-140

CREACIÓN DE ZONAS DE SEGURIDAD POR INTERFACES

En un solo dispositivo de seguridad se pueden configurar varias zonas de seguridad, dividiendo la red en segmentos a los que se pueden aplicar diversas opciones de seguridad para satisfacer las necesidades de cada segmento.

Deben definirse como mínimo dos zonas de seguridad, básicamente para proteger un área de la red de la otra. En algunas plataformas de seguridad se pueden definir muchas zonas de seguridad, lo que refina aún más la granularidad del diseño de seguridad de la red, evitando la necesidad de distribuir múltiples dispositivos de seguridad para conseguir el mismo fin.

Se propone que la red de la empresa corresponda a cinco Zonas de seguridad por el momento, las cuales son:

La zona Trust, Untrust y DMZ, Infinitum y Dedicado.

En la zona Trust (LAN), en esta interface existe la conexión hacia el switch, y nos sirve para la comunicación con la LAN de la Empresa.

En la zona Untrust (Internet), por medio de esta interface se le dota el servicio hacia internet al firewall.

En la zona DMZ (zona desmilitarizada), en esta interface, se encontrarán los servidores que la Empresa pública hacia internet, como es la página Web, el correo etc.

En la zona Infinitum (Internet), esta sería una zona de seguridad de reserva internet y en este se realizó la publicación del servidor de cámaras de seguridad, así como del checador.

En la zona Dedicado (Internet), esta sería un enlace más hacia internet en el firewall, por medio de este enlace se realizaron las publicaciones de los servidores más críticos hacia internet, así como la configuración de VPN's hacia las sucursales.

El siguiente diagrama muestra lo descrito anteriormente, en la Empresa TECAPPS

Nombre	IP/Netmask	Zone
ethernet0/0	172.16.1.1/24	Trust
ethernet0/1	192.168.1.1/24	DMZ
ethernet0/2	100.100.100.2/24	Untrust
ethernet0/3	200.67.204.204/32	Infinitem
ethernet0/4	201.116.35.115/28	Dedicado
tunnel.1	Unnumbered	Dedicado
tunnel.10	Unnumbered	Dedicado
tunnel.11	Unnumbered	Dedicado
tunnel.12	Unnumbered	Dedicado
tunnel.13	Unnumbered	Dedicado
tunnel.14	Unnumbered	Infinitem
tunnel.15	Unnumbered	Infinitem
tunnel.2	Unnumbered	Dedicado
tunnel.3	Unnumbered	Dedicado
tunnel.4	Unnumbered	Dedicado

tunnel.5	Unnumbered	Dedicado
tunnel.6	Unnumbered	Dedicado
tunnel.7	Unnumbered	Dedicado
tunnel.8	Unnumbered	Dedicado
tunnel.9	Unnumbered	Dedicado

TABLAS 1TECAPPS

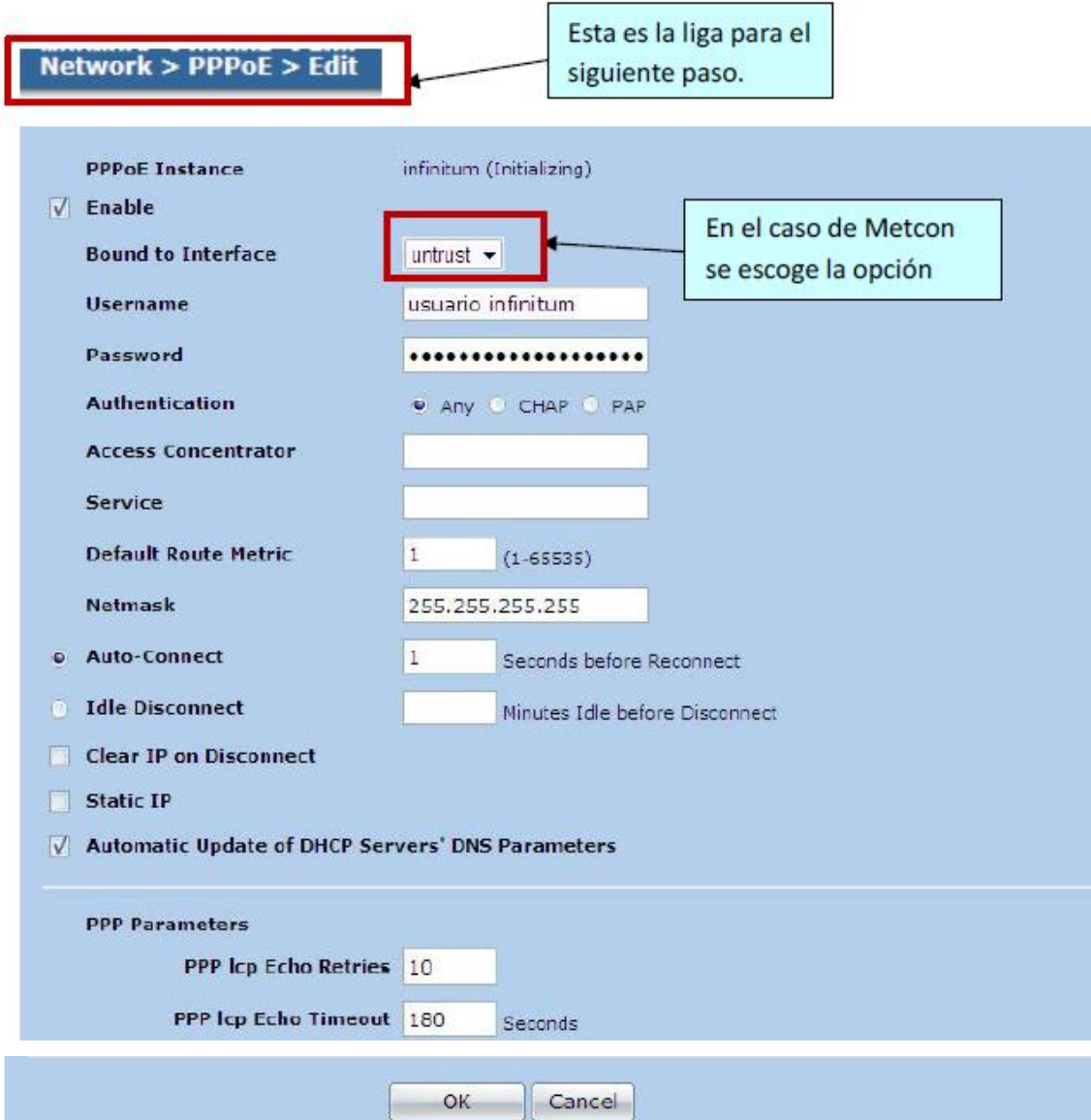
Línea de comando (CLI)

- set interface "ethernet0/0" zone "Trust"
- set interface "ethernet0/1" zone "DMZ"
- set interface "ethernet0/2" zone "Untrust"
- set interface "ethernet0/3" zone "Infinitum"
- set interface "ethernet0/4" zone "Dedicado"
- set interface "tunnel.1" zone "Dedicado"
- set interface "tunnel.2" zone "Dedicado"
- set interface "tunnel.3" zone "Dedicado"
- set interface "tunnel.4" zone "Dedicado"
- set interface "tunnel.5" zone "Dedicado"
- set interface "tunnel.6" zone "Dedicado"
- set interface "tunnel.7" zone "Dedicado"
- set interface "tunnel.8" zone "Dedicado"
- set interface "tunnel.9" zone "Dedicado"
- set interface "tunnel.10" zone "Dedicado"
- set interface "tunnel.11" zone "Dedicado"
- set interface "tunnel.12" zone "Dedicado"
- set interface "tunnel.13" zone "Dedicado"
- set interface "tunnel.14" zone "Infinitum"
- set interface "tunnel.15" zone "Infinitum"
- set interface ethernet0/0 ip 172.16.1.1/24
- set interface ethernet0/0 route
- unset interface vlan1 ip
- set interface ethernet0/1 ip 192.168.1.1/24
- set interface ethernet0/1 route
- set interface ethernet0/2 ip 100.100.100.2/24
- set interface ethernet0/2 route
- set interface ethernet0/3 ip 200.67.204.204/32
- set interface ethernet0/3 route
- set interface ethernet0/4 ip 201.116.35.115/28

- set interface ethernet0/4 route
- set interface tunnel.1 ip unnumbered interface ethernet0/4
- set interface tunnel.2 ip unnumbered interface ethernet0/4
- set interface tunnel.3 ip unnumbered interface ethernet0/4
- set interface tunnel.4 ip unnumbered interface ethernet0/4
- set interface tunnel.5 ip unnumbered interface ethernet0/4
- set interface tunnel.6 ip unnumbered interface ethernet0/4
- set interface tunnel.7 ip unnumbered interface ethernet0/4
- set interface tunnel.8 ip unnumbered interface ethernet0/4
- set interface tunnel.9 ip unnumbered interface ethernet0/4
- set interface tunnel.10 ip unnumbered interface ethernet0/4
- set interface tunnel.11 ip unnumbered interface ethernet0/4
- set interface tunnel.12 ip unnumbered interface ethernet0/4
- set interface tunnel.13 ip unnumbered interface ethernet0/4
- set interface tunnel.14 ip unnumbered interface ethernet0/3
- set interface tunnel.15 ip unnumbered interface ethernet0/3

CONFIGURACIÓN DE PPPOE

PROCEDIMIENTOS PARA CREAR CONEXIÓN PPPOE POR WEB.



The screenshot shows the configuration page for a PPPoE instance named 'infinitem (Initializing)'. The 'Bound to Interface' dropdown menu is highlighted with a red box and labeled 'untrust'. A callout box points to this dropdown with the text: 'En el caso de Metcon se escoge la opción'. Another callout box points to the breadcrumb 'Network > PPPoE > Edit' with the text: 'Esta es la liga para el siguiente paso.' The configuration includes fields for Username (usuario infinitem), Password (masked), Authentication (Any selected), Access Concentrator, Service, Default Route Metric (1), Netmask (255.255.255.255), and various options like Auto-Connect, Idle Disconnect, Clear IP on Disconnect, Static IP, and Automatic Update of DHCP Servers' DNS Parameters. At the bottom, there are 'OK' and 'Cancel' buttons.

ILUSTRACIÓN 19 CONEXIÓN PPPOE POR WEB

PPPoE Instance	Interface	User	Mac address	Enabled	State	Action	Configure
infinitem	untrust	usuario infinitem	00.10.db.b3.88.f1	Yes	Initializing	Connect	Edit Remove

Le damos click en connect

Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure
eerial	0.0.0.0/0	Null	Unused	Down	-	Edit
trust	172.16.1.1/24	Trust	Layer3	Up	-	Edit
tunnel.1	unnumbered	Untrust	Tunnel	Down	-	Edit Remove
untrust	192.168.1.125/24	Untrust	Layer3	Up	✖	Edit
vlan1	0.0.0.0/0	VLAN	Layer3	Down	-	Edit

Se pondrá en color verde y nos asignara la dirección ip pública

ILUSTRACIÓN 20 ASIGNACION DE IP PÚBLICA

USUARIO Y PASSWORD DE INFINITUM.

Interface	Usuario	Password
Eth0/4 Infinitem_Fijo	jenneranil	jenneranil
Eth0/3 Infinitem_Dina	lcl5558036205	5558036205

TABLAS 2 DE USUARIO Y PASSWORD DE INFINITUM

VALORES QUE TIENE TECAPPS EN LA CONFIGURACIÓN PPPOE.

Configuration PPPoE	
PPPoE Instance	Infinitem_Fijo
Enable	Yes
Bound to Interface	ethernet0/3
Username	jenneranil
Password	jenneranil
Autentication	Any
Access concentrator	-
Service	-
Default Route Metric	1
Netmask	255.255.255.255
Auto- connect	1
Idle Disconnect	-
Clear IP Disconnect	Enable
Static IP	Enable
Automatic Update of DHCP Servers DNS Parameters	-
PPP Parameters	
PPP Icp Echo Retries	10
PPP Icp Echo Time out (Seconds)	180

PPPoE Instance	Interface	Usuario	Mac address	Enable	State	Acción
Infinitem_Fijo	ethernet0/3	jenneranil		Yes	Conected	Disconnect

TABLAS 3 TECAPPS EN LA CONFIGURACIÓN PPPOE

Línea de comando (CLI).

- set pppoe name "Infinitem_Dina"
- set pppoe name "Infinitem_Dina" username "Tecappsanil" password "9eRDWWjKNfEHL/syEHCDfA/1dFnYKulE7w=="
- set pppoe name "Infinitem_Dina" idle 0
- set pppoe name "Infinitem_Dina" static-ip
- set pppoe name "Infinitem_Dina" interface ethernet0/3
- unset pppoe name "Infinitem_Dina" update-dhcpserver
- set pppoe name "Infinitem_Dina" auto-connect 1
- set pppoe name "Infinitem_Dina" clear-on-disconnect
- set pppoe name "Infinitem_Dinamica"
- set pppoe name "Infinitem_Dinamica" username "lcl5558036205" password "kWEEv4JANGAUgns5KHC7n0H8UcnJ2s92og=="
- set pppoe name "Infinitem_Dinamica" idle 0
- unset pppoe name "Infinitem_Dinamica" update-dhcpserver
- set pppoe name "Infinitem_Dinamica" auto-connect 1

CONFIGURACIÓN DE RUTEO.

RUTAS VIRTUALES (TRUST-VR, UNTRUST-VR E INFINITEM-VR)

Se crearon rutas alternas virtuales para que la red pueda llegar a otras redes sin la necesidad de otro equipo, saliendo por cada uno de los enlaces los servicios que les correspondían, se metieron rutas tanto como para que los usuarios puedan salir a Internet, así como ruteo para que se puedan comunicar las VPN's que van desde el Corporativo

central de TECAPPS, hasta cada una de las sucursales. Estas rutas se dividen en 3 pasos, dirección IP destino, la dirección del Gateway que utilizaras para alcanzar dicha IP y la interface por medio de la cual te comunicaras para alcanzar el objetivo.

El siguiente diagrama se muestra lo descrito anteriormente.

RUTEO POR DESTINO > TRUST-VR

FIREWALL PERIMETRAL

IP / NetMask	Interface / V-router	Gateway	Preference
172.16.1.0/24	ethernet0/0		
172.16.1.1/32	ethernet0/0		
192.168.1.0/24	ethernet0/1		
192.168.1.1/32	ethernet0/1		
100.100.100.0/24	ethernet0/2		
100.100.100.2/32	ethernet0/2		
172.16.1.128/28	ethernet0/0		
10.200.200.0/24	ethernet0/1	192.168.1.15	
10.200.200.0/24	ethernet0/1		
0.0.0.0/0	ethernet0/2	100.100.100.1	
172.16.123.0/24	tunnel.15		30
172.16.123.0/24	tunnel.12		
0.0.0.0/0	untrust-vr		60
0.0.0.0/0	VR-Infinitem		50
172.16.101.0/24	untrust-vr		
172.16.125.0/24	untrust-vr		
172.16.102.0/24	untrust-vr		
172.16.103.0/24	untrust-vr		
172.16.106.0/24	untrust-vr		
172.16.107.0/24	untrust-vr		
172.16.111.0/24	untrust-vr		
172.16.114.0/24	untrust-vr		
172.16.116.0/24	untrust-vr		
172.16.121.0/24	untrust-vr		
172.16.117.0/24	untrust-vr		
172.16.104.0/24	untrust-vr		
10.30.30.0/24	VR-Infinitem		
172.16.150.0/24	untrust-vr		
172.16.105.0/24	untrust-vr		
192.168.125.13/32	untrust-vr		
172.16.100.0/24	untrust-vr		

TABLAS 4 RUTEO POR DESTINO

Línea de comando (CLI)

- set vrouter "trust-vr"
- set source-routing enable
- unset add-default-route
- set route 172.16.1.128/28 interface ethernet0/0
- set route 10.200.200.0/24 interface ethernet0/1 gateway 192.168.1.15
- set route 172.16.123.0/24 interface tunnel.15 preference 30
- set route 172.16.123.0/24 interface tunnel.12
- set route 0.0.0.0/0 vrouter "untrust-vr" preference 60 metric 1
- set route 0.0.0.0/0 vrouter "VR-Infinitem" preference 50 metric 1
- set route 172.16.101.0/24 vrouter "untrust-vr" preference 20 metric 1
- set route 10.30.30.0/24 vrouter "VR-Infinitem" preference 20 metric 1
- set route source 192.168.1.20/32 vrouter "untrust-vr" preference 20 metric 1

RUTEO UNTRUST-VR

IP / NetMask	Interface/V-router	Gateway
201.116.35.112/28	ethernet0/4	
201.116.35.115/32	ethernet0/4	
0.0.0.0/0	ethernet0/4	201.116.35.113
172.16.125.0/24	tunnel.1	
172.16.101.0/24	tunnel.2	
172.16.102.0/24	tunnel.3	
172.16.103.0/24	tunnel.4	
172.16.104.0/24	tunnel.5	
172.16.106.0/24	tunnel.6	
172.16.107.0/24	tunnel.7	
172.16.114.0/24	tunnel.9	
172.16.116.0/24	tunnel.10	
172.16.123.0/24	tunnel.12	
172.16.121.0/24	tunnel.11	
172.16.117.0/24	tunnel.13	

172.16.105.0/24	tunnel.8	
192.168.125.13/32	ethernet0/4	201.116.35.113
172.16.100.0/24	tunnel.12	
192.168.1.0/24	trust-vr	
172.16.1.0/24	trust-vr	
10.30.30.0/24	VR-Infinitem	

TABLAS 5 RUTEO UNTRUST-VR

Línea de comando (CLI)

- set vrouter "untrust-vr"
- set route 0.0.0.0/0 interface ethernet0/4 gateway 201.116.35.113
- set route 172.16.125.0/24 interface tunnel.1
- set route 172.16.101.0/24 interface tunnel.2
- set route 172.16.102.0/24 interface tunnel.3
- set route 172.16.103.0/24 interface tunnel.4
- set route 172.16.104.0/24 interface tunnel.5
- set route 172.16.106.0/24 interface tunnel.6
- set route 172.16.107.0/24 interface tunnel.7
- set route 172.16.114.0/24 interface tunnel.9
- set route 172.16.116.0/24 interface tunnel.10
- set route 172.16.123.0/24 interface tunnel.12
- set route 172.16.121.0/24 interface tunnel.11
- set route 172.16.117.0/24 interface tunnel.13
- set route 172.16.105.0/24 interface tunnel.8
- set route 192.168.125.13/32 interface ethernet0/4 gateway 201.116.35.113
- set route 172.16.100.0/24 interface tunnel.12
- set route 192.168.1.0/24 vrouter "trust-vr" preference 20 metric 1
- set route 172.16.1.0/24 vrouter "trust-vr" preference 20 metric 1
- set route 10.30.30.0/24 vrouter "VR-Infinitem" preference 20 metric 1

RUTEO VR-INFINITUM

IP / NetMask	Interface/V-router	Gateway	Preference
200.67.204.204/32	ethernet0/3		
200.67.204.204/32	ethernet0/3		
10.30.30.0/24	tunnel.14		
192.168.1.0/24	trust-vr		
172.16.1.0/24	trust-vr		
0.0.0.0/0	trust-vr		55
172.16.0.0/16	trust-vr		
0.0.0.0/0	ethernet0/3	200.38.193.226	

TABLAS 6 RUTEO VR-INFINITUM

Línea de comando (CLI)

- set vrouter "VR-Infinitem"
- set route 10.30.30.0/24 interface tunnel.14
- set route 192.168.1.0/24 vrouter "trust-vr" preference 20 metric 1
- set route 172.16.1.0/24 vrouter "trust-vr" preference 20 metric 1

- set route 0.0.0.0/0 vrouter "trust-vr" preference 55 metric 1
- set route 172.16.0.0/16 vrouter "trust-vr" preference 20 metric 1
- exit

RUTEO POR ORIGEN > TRUST-VR

IP / NetMask	Interface/V-router	Gateway
172.16.1.32/28	VR-Infinitem	
172.16.1.64/28	VR-Infinitem	
192.168.1.16/32	untrust-vr	
192.168.1.10/32	untrust-vr	
192.168.1.11/32	untrust-vr	
172.16.1.2/32	untrust-vr	
172.16.1.3/32	untrust-vr	
172.16.1.4/32	untrust-vr	
172.16.1.5/32	untrust-vr	
172.16.1.7/32	untrust-vr	
172.16.1.6/32	untrust-vr	
172.16.1.8/32	untrust-vr	
172.16.1.9/32	untrust-vr	
172.16.1.10/32	untrust-vr	
172.16.1.11/32	untrust-vr	
172.16.1.12/32	untrust-vr	
172.16.1.13/32	untrust-vr	
172.16.1.14/32	untrust-vr	
172.16.1.120/32	untrust-vr	
192.168.1.13/32	untrust-vr	
192.168.1.20/32	untrust-vr	

TABLAS 7 RUTEO POR ORIGEN > TRUST-VR

Línea de comando (CLI)

- set route source 172.16.1.32/28 vrouter "VR-Infinitem" preference 20 metric 1
- set route source 172.16.1.64/28 vrouter "VR-Infinitem" preference 20 metric 1
- set route source 192.168.1.16/32 vrouter "untrust-vr" preference 20 metric 1
- set route source 192.168.1.10/32 vrouter "untrust-vr" preference 20 metric 1
- set route source 192.168.1.11/32 vrouter "untrust-vr" preference 20 metric 1
- set route source 172.16.1.2/32 vrouter "untrust-vr" preference 20 metric 1
- set route source 172.16.1.5/32 vrouter "untrust-vr" preference 20 metric 1
- set route source 172.16.1.7/32 vrouter "untrust-vr" preference 20 metric 1
- set route source 172.16.1.6/32 vrouter "untrust-vr" preference 20 metric 1
- set route source 172.16.1.8/32 vrouter "untrust-vr" preference 20 metric 1
- set route source 172.16.1.9/32 vrouter "untrust-vr" preference 20 metric 1
- set route source 172.16.1.10/32 vrouter "untrust-vr" preference 20 metric 1
- set route source 172.16.1.11/32 vrouter "untrust-vr" preference 20 metric 1
- set route source 172.16.1.12/32 vrouter "untrust-vr" preference 20 metric 1
- set route source 172.16.1.13/32 vrouter "untrust-vr" preference 20 metric 1
- set route source 172.16.1.14/32 vrouter "untrust-vr" preference 20 metric 1
- set route source 172.16.1.120/32 vrouter "untrust-vr" preference 20 metric 1
- set route source 192.168.1.13/32 vrouter "untrust-vr" preference 20 metric 1
- set route source 192.168.1.20/32 vrouter "untrust-vr" preference 20 metric 1
- exit.

LISTA Y GRUPOS DE DIRECCIONES

Se creó una lista de direcciones IP de las maquinas principales y servidores de la empresa, en las diferentes zonas de seguridad en donde se requería conocer el host que se tienen que comunicar con otros, con el fin de tener un mayor control y administración de estos.

La administración de las direcciones IP, se puede llevar a cabo ya sea por medio de una sola dirección IP o a todo un grupo de direcciones según se requiera.

Cabe aclarar que pueden establecerse direcciones IP, que estén dentro o fuera del corporativo, según sea el caso.

La lista de direcciones IP se dividieron en las diferentes zonas de seguridad, ya sea que estén dentro de una zona confiable del corporativo, (Trust, DMZ) y las direcciones que estén fuera de una zona confiable del corporativo, (Untrust, Infinitum, Dedicado).

El siguiente diagrama muestra lo descrito anteriormente, en la Empresa TECAPPS.

TABLA DE DIRECCIONES EN LA ZONA TRUST

Nombre	Direccion IP	Mascara de Red	Comentario
0.0.0.0/0	0.0.0.0	0.0.0.0	Internet
10.30.30.0/24	10.30.30.0	255.255.255.0	
172.16.0.0/16	172.16.0.0	255.255.0.0	
172.16.1.13/32	172.16.1.13	255.255.255.255	
172.16.1.135/32	172.16.1.135	255.255.255.255	
172.16.1.137/32	172.16.1.137	255.255.255.255	
172.16.1.14/32	172.16.1.14	255.255.255.255	
172.16.1.15/32	172.16.1.15	255.255.255.255	
172.16.1.7/32	172.16.1.7	255.255.255.255	
172.16.1.77/32	172.16.1.77	255.255.255.255	
192.168.125.0/24	192.168.125.0	255.255.255.0	
192.168.125.13/32	192.168.125.14	255.255.255.255	
Administrador	JNRCORP042.laboratoriojenner.com.mx		
Adriana Icelo	172.16.1.4	255.255.255.255	
Angel Valera	172.16.1.8	255.255.255.255	
ASISTGERENCIA	JNRCORP015.laboratoriojenner.com.mx		
AUDITORIA	JNRCORP004.laboratoriojenner.com.mx		
AUXILIAR	JNRCORP016.laboratoriojenner.com.mx		
BAN01	JNRCORP010.laboratoriojenner.com.mx		
BANCOS	JNRCORP033.laboratoriojenner.com.mx		
Call Center	172.16.1.6	255.255.255.255	
CALLCENTER3	JNRCORP018.laboratoriojenner.com.mx		
callcenter4	JNRCORP037.laboratoriojenner.com.mx		
CALLCENTERII	JNRCORP025.laboratoriojenner.com.mx		
CALLCENTERIII	JNRCORP023.laboratoriojenner.com.mx		
CAPO2	JNRCORP040.laboratoriojenner.com.mx		

FIREWALL PERIMETRAL

CCVT	JNRCORP008.laboratoriojenner.com.mx		
COMPRAS	JNRCORP029.laboratoriojenner.com.mx		
CONTA0102	JNRCORP005.laboratoriojenner.com.mx		
CONTABILIDAD	JNRCORP022.laboratoriojenner.com.mx		
CORP12	JNRCORP024.laboratoriojenner.com.mx		
DESARROLLO	JNRCORP013.laboratoriojenner.com.mx		
DH	172.16.1.12	255.255.255.255	
DH2	JNRCORP009.laboratoriojenner.com.mx		
DH3	JNRCORP035.laboratoriojenner.com.mx		
DIRECCION	JNRCORP001.laboratoriojenner.com.mx		
Dra Ana Sainez	172.16.1.2	255.255.255.255	
FACTURACION	JNRCORP011.laboratoriojenner.com.mx		
Fernando Ramirez	172.16.1.5	255.255.255.255	
FTP	JNRCORP007.laboratoriojenner.com.mx		
Gerardo Herrera	172.16.1.12	255.255.255.255	
HERRERA	JNRCORP014.laboratoriojenner.com.mx		
Jesus Ramirez	172.16.1.9	255.255.255.255	
JNRCORP038	JNRCORP038.laboratoriojenner.com.mx		
Mac	172.16.1.105	255.255.255.255	
MARISOL	JNRCORP036.laboratoriojenner.com.mx		
MKT	JNRCORP039.laboratoriojenner.com.mx		
MOVIL	JNRCORP021.laboratoriojenner.com.mx		
OPERACIONES	JNRCORP026.laboratoriojenner.com.mx		
OPERASISTENT	JNRCORP017.laboratoriojenner.com.mx		
PROMOCION	JNRCORP034.laboratoriojenner.com.mx		
prueba	JNRCORP043.laboratoriojenner.com.mx		
Raul Aguilar	172.16.1.7	255.255.255.255	
Red_Jenner	172.16.1.0	255.255.255.0	
Red_Wireless	172.16.1.128	255.255.255.240	
SALA	JNRCORP027.laboratoriojenner.com.mx		

Sala de Juntas	172.16.1.10		
Salvador Vanegas	172.16.1.3	255.255.255.255	
SINCAL	JNRCORP006.laboratoriojenner.com.mx		
SIS0101	JNRCORP020.laboratoriojenner.com.mx		
SIS0102	JNRCORP019.laboratoriojenner.com.mx		
SISTEMAS001	JNRCORP002.laboratoriojenner.com.mx		
SISTEMASMARIO	JNRCORP030.laboratoriojenner.com.mx		
TRAMITES	JNRCORP032.laboratoriojenner.com.mx		
VENTAS	JNRCORP031.laboratoriojenner.com.mx		
Veronica Aguirre	172.16.1.11	255.255.255.255	
Wireless-129	172.16.1.129	255.255.255.255	
Wireless-130	172.16.1.130	255.255.255.255	
Wireless-131	172.16.1.131	255.255.255.255	
Wireless-132	172.16.1.132	255.255.255.255	
Wireless-133	172.16.1.133	255.255.255.255	
Wireless-134	172.16.1.134	255.255.255.255	
Wireless-135	172.16.1.135	255.255.255.255	
Wireless-136	172.16.1.136	255.255.255.255	

TABLAS 8 TABLA DE DIRECCIONES EN LA ZONA TRUST

Línea de comando (CLI)

- set address "Trust" "0.0.0.0/0" 0.0.0.0 0.0.0.0
- set address "Trust" "10.30.30.0/24" 10.30.30.0 255.255.255.0
- set address "Trust" "172.16.0.0/16" 172.16.0.0 255.255.0.0
- set address "Trust" "172.16.1.13/32" 172.16.1.13 255.255.255.255
- set address "Trust" "172.16.1.135/32" 172.16.1.135 255.255.255.255
- set address "Trust" "172.16.1.137/32" 172.16.1.137 255.255.255.255
- set address "Trust" "172.16.1.14/32" 172.16.1.14 255.255.255.255
- set address "Trust" "172.16.1.15/32" 172.16.1.15 255.255.255.255
- set address "Trust" "172.16.1.7/32" 172.16.1.7 255.255.255.255
- set address "Trust" "172.16.1.77/32" 172.16.1.77 255.255.255.255
- set address "Trust" "192.168.125.0/24" 192.168.125.0 255.255.255.0
- set address "Trust" "192.168.125.13/32" 192.168.125.14 255.255.255.255
- set address "Trust" "Administrador" JNRCORP042.j.David@Tecapps.com.mx
- set address "Trust" "Adriana Icelo" 172.16.1.4 255.255.255.255
- set address "Trust" "Angel Valera" 172.16.1.8 255.255.255.255

DE GRUPOS DE DIRECCIONES EN LA ZONA TRUST

Zona	Nombre del Grupo	Lista de Direcciones
Trust	Grupo_AccesoTotal	172.16.1.13
Trust	Grupo_AccesoTotal	172.16.1.14
Trust	Grupo_AccesoTotal	172.16.1.15
Trust	Grupo_AccesoTotal	Adriana Icelo
Trust	Grupo_AccesoTotal	Angel Valera
Trust	Grupo_AccesoTotal	Call Center
Trust	Grupo_AccesoTotal	Dra Ana Sainez
Trust	Grupo_AccesoTotal	Fernando Ramirez
Trust	Grupo_AccesoTotal	Gerardo Herrera
Trust	Grupo_AccesoTotal	Jesus Ramirez
Trust	Grupo_AccesoTotal	Raul Aguilar
Trust	Grupo_AccesoTotal	Sala de Juntas
Trust	Grupo_AccesoTotal	Salvador Vanega
Trust	Grupo_AccesoTotal	Veronica Aguirre

TABLAS 9 DE GRUPOS DE DIRECCIONES EN LA ZONA TRUST

Línea de comando (CLI)

- set group address "Trust" "Grupo_AccesoTotal"
- set group address "Trust" "Grupo_AccesoTotal" add "172.16.1.13/32"
- set group address "Trust" "Grupo_AccesoTotal" add "172.16.1.14/32"
- set group address "Trust" "Grupo_AccesoTotal" add "172.16.1.15/32"
- set group address "Trust" "Grupo_AccesoTotal" add "Adriana Icelo"
- set group address "Trust" "Grupo_AccesoTotal" add "Angel Valera"
- set group address "Trust" "Grupo_AccesoTotal" add "Call Center"
- set group address "Trust" "Grupo_AccesoTotal" add "Dra Ana Sainez"
- set group address "Trust" "Grupo_AccesoTotal" add "Angel Ramirez"
- set group address "Trust" "Grupo_AccesoTotal" add "Gerardo Herrera"
- set group address "Trust" "Grupo_AccesoTotal" add "Jesus Ramirez"
- set group address "Trust" "Grupo_AccesoTotal" add "Raul Aguilar"
- set group address "Trust" "Grupo_AccesoTotal" add "Sala de Juntas"
- set group address "Trust" "Grupo_AccesoTotal" add "Salvador Vanegas"
- set group address "Trust" "Grupo_AccesoTotal" add "Veronica Aguirre"

TABLA DE DIRECCIONES EN LA ZONA UNTRUST

Nombre	Direccion IP	Mascara de Red	Comentario
224.0.0.1/32	224.0.0.1	255.255.255.255	
65.55.13.91/32	65.55.13.91	255.255.255.255	

TABLAS 10 DE DIRECCIONES EN LA ZONA UNTRUST

Línea de comando (CLI)

- set address "Untrust" "224.0.0.1/32" 224.0.0.1 255.255.255.255
- set address "Untrust" "65.55.13.91/32" 65.55.13.91 255.255.255.255 6.4 TABLA DE DIRECCIONES EN LA ZONA DMZ

Nombre	Direccion IP	Mascara de Red	Comentario
192.168.1.15/32	192.168.1.15	255.255.255.255	
192.168.1.16/32	192.168.1.16	255.255.255.255	
192.168.1.19/32	192.168.1.19	255.255.255.255	
192.168.1.198/32	192.168.1.198	255.255.255.255	
192.168.1.20/32	192.168.1.20	255.255.255.255	
Active_Directory	192.168.1.198	255.255.255.255	
Exchange	192.168.1.11	255.255.255.255	
FTP_Aspel	192.168.1.18	255.255.255.255	
Red_DMZ	192.168.1.0	255.255.255.0	
Red_Secure Access	10.200.200.0	255.255.255.0	
Stratix	192.168.1.12	255.255.255.255	
Visualab	192.168.1.13	255.255.255.255	
Web	192.168.1.10	255.255.255.255	

TABLAS 11 DIRECCIONES EN LA ZONA DMZ

Línea de comando (CLI)

- set address "DMZ" "192.168.1.15/32" 192.168.1.15 255.255.255.255
- set address "DMZ" "192.168.1.16/32" 192.168.1.16 255.255.255.255
- set address "DMZ" "192.168.1.19/32" 192.168.1.19 255.255.255.255
- set address "DMZ" "192.168.1.198/32" 192.168.1.198 255.255.255.255
- set address "DMZ" "192.168.1.20/32" 192.168.1.20 255.255.255.255
- set address "DMZ" "Active_Directory" 192.168.1.198 255.255.255.255
- set address "DMZ" "Exchange" 192.168.1.11 255.255.255.255
- set address "DMZ" "FTP_Aspel" 192.168.1.18 255.255.255.255

- set address "DMZ" "Red_DMZ" 192.168.1.0 255.255.255.0
- set address "DMZ" "Red_Secure Access" 10.200.200.0 255.255.255.0
- set address "DMZ" "Stratix" 192.168.1.12 255.255.255.255
- set address "DMZ" "Visualab" 192.168.1.13 255.255.255.255
- set address "DMZ" "Web" 192.168.1.10 255.255.255.255

TABLA DE DIRECCIONES EN LA ZONA DEDICADO

Nombre	Direccion IP	Mascara de Red	Comentario
172.16.106.10/32	172.16.106.10	255.255.255.255	
172.16.117.0/24	172.16.117.0	255.255.255.0	
172.16.117.11/32	172.16.117.11	255.255.255.255	
172.16.150.0/24	172.16.150.0	255.255.255.0	
224.0.0.1/32	224.0.0.1	255.255.255.255	
65.55.13.91/32	65.55.13.91	255.255.255.255	
correo_de_salida	201.116.35.115	255.255.255.255	
Sucursal_AvMexico	172.16.123.0	255.255.255.0	Av. Mexico
Sucursal_AvMexico-lab	172.16.100.0	255.255.255.0	Laboratorio
Sucursal_Chicoloapan	172.16.117.0	255.255.255.0	Chicoloapan
Sucursal_Coyoacan	172.16.106.0	255.255.255.0	Coyoacan
Sucursal_Culhuacan	172.16.105.0	255.255.255.0	Culhuacan
Sucursal_Ermita	172.16.107.0	255.255.255.0	Ermita
Sucursal_Estadio	172.16.101.0	255.255.255.0	Estadio
Sucursal_Sur16	172.16.116.0	255.255.255.0	Sur16
Sucursal_Tepozanes	172.16.102.0	255.255.255.0	Tepozanes
Sucursal_Tezonco	172.16.104.0	255.255.255.0	Tezonco
Sucursal_Tulyehualco	172.16.103.0	255.255.255.0	Tulyehualco
Sucursal_Viaducto	172.16.125.0	255.255.255.0	Viaducto
Sucursal_Voca7	172.16.121.0	255.255.255.0	Voca7
Sucursal_Xochimilco	172.16.114.0	255.255.255.0	Xochimilco

TABLAS 12 DIRECCIONES EN LA ZONA DEDICADO

Línea de comando (CLI)

- set address "Dedicado" "172.16.106.10/32" 172.16.106.10 255.255.255.255

- set address "Dedicado" "172.16.117.0/24" 172.16.117.0 255.255.255.0
- set address "Dedicado" "172.16.117.11/32" 172.16.117.11 255.255.255.255
- set address "Dedicado" "172.16.150.0/24" 172.16.150.0 255.255.255.0
- set address "Dedicado" "224.0.0.1/32" 224.0.0.1 255.255.255.255
- set address "Dedicado" "65.55.13.91/32" 65.55.13.91 255.255.255.255
- set address "Dedicado" "correo_de_salida" 201.116.35.115 255.255.255.255
- set address "Dedicado" "Sucursal_AvMexico" 172.16.123.0 255.255.255.0
- set address "Dedicado" "Sucursal_AvMexico-lab" 172.16.100.0 255.255.255.0
- set address "Dedicado" "Sucursal_Chicoloapan" 172.16.117.0 255.255.255.0
- set address "Dedicado" "Sucursal_Coyoacan" 172.16.106.0 255.255.255.0
- set address "Dedicado" "Sucursal_Culhuacan" 172.16.105.0 255.255.255.0
- set address "Dedicado" "Sucursal_Ermita" 172.16.107.0 255.255.255.0
- set address "Dedicado" "Sucursal_Estadio" 172.16.101.0 255.255.255.0
- set address "Dedicado" "Sucursal_Sur16" 172.16.116.0 255.255.255.0

TABLA DE DIRECCIONES EN LA ZONA INFINITUM

Nombre	Direccion IP	Mascara de Red	Comentario
Red_Noc_BMC	10.30.30.0	255.255.255.0	
Noc_BMC_Orion	10.30.30.7	255.255.255.255	
Noc_BMC_Servo	10.30.30.8	255.255.255.255	
192.168.1.0/26	192.168.1.0	255.255.255.192	
192.168.1.145	192.168.1.145	255.255.255.240	
224.0.0.1/32	224.0.0.1	255.255.255.255	

TABLAS 13 DIRECCIONES EN LA ZONA INFINITUM

Línea de comando (CLI)

- set address "Infinitum" "10.30.30.0/24" 10.30.30.0 255.255.255.0
- set address "Infinitum" "10.30.30.7/32" 10.30.30.7 255.255.255.255
- set address "Infinitum" "10.30.30.8/32" 10.30.30.8 255.255.255.255
- set address "Infinitum" "192.168.1.0/26" 192.168.1.0 255.255.255.192
- set address "Infinitum" "192.168.1.145" 192.168.1.145 255.255.255.240

LISTA Y GRUPOS DE SERVICIOS

Algunas aplicaciones con las que cuenta el corporativo tienen la necesidad de una comunicación segura, estas aplicaciones son pertenecientes a la empresa y utilizan puertos especiales de consulta, para brindar una mayor seguridad a las páginas de acceso que ocupan para sus diferentes aplicaciones.

Para que la empresa TECAPPS pudiera acceder a ese tipo de páginas de aplicaciones, se configuraron servicios especiales en el firewall, agregándole puertos específicos de acceso, según lo requiera la aplicación a consultar.

El siguiente diagrama muestra lo descrito anteriormente, en la Empresa TECAPPS.

TABLA DE LISTA DE SERVICIOS

FIREWALL PERIMETRAL

Nombre	Protocolo	Pto. Origen	Pto. Destino
Pto_Visualab-1951	tcp	0-65535	1951-1951

Nombre	Protocolo	Pto. Origen	Pto. Destino
Pto_Escritorio_remoto	tcp	0-65535	3389-3389

Nombre	Protocolo	Pto. Origen	Pto. Destino
Pto_Stratix-1672	tcp	0-65535	1672-1672

Nombre	Protocolo	Pto. Origen	Pto. Destino
Puerto_Webmail	tcp	0-65535	32000-32000

Nombre	Protocolo	Pto. Origen	Pto. Destino
Pto._OUTLOOK-6001	tcp	0-65535	6001-6001

Nombre	Protocolo	Pto. Origen	Pto. Destino
Pto._OUTLOOK-6002	tcp	0-65535	6002-6002

Nombre	Protocolo	Pto. Origen	Pto. Destino
Pto._OUTLOOK-6003	tcp	0-65535	6003-6003

Nombre	Protocolo	Pto. Origen	Pto. Destino
Pto._OUTLOOK-6004	tcp	0-65535	6004-6004

Nombre	Protocolo	Pto. Origen	Pto. Destino
Pto-2500	tcp	9000-65535	2500-2500

Nombre	Protocolo	Pto. Origen	Pto. Destino
Pto-SIP	udp	0-65535	5004-5037
	udp	0-65535	10001-20000
	udp	0-65535	4569-4569
	tcp	0-65535	800-800
	tcp	0-65535	22-22
	tcp	0-65535	80-80
	udp	0-65535	5039-5082

Nombre	Protocolo	Pto. Origen	Pto. Destino
Pto-5038	tcp	0-65535	5038-5038
	udp	0-65535	5038-5038
	tcp	0-65535	3306-3306
	udp	0-65535	3306-3306

Nombre	Protocolo	Pto. Origen	Pto. Destino
stratix	tcp	0-65535	1672-1673
	udp	0-65535	1672-1673

TABLAS 14 TABLA DE LISTA DE SERVICIOS

Línea de comando (CLI)

- set service "Pto_Visualab-1951" protocol tcp src-port 0-65535 dst-port 1951-1951
- set service "Pto_Escritorio_remoto" protocol tcp src-port 0-65535 dst-port 3389-3389
- set service "Pto_Stratix-1672" protocol tcp src-port 0-65535 dst-port 1672-1672
- set service "Puerto_Webmail" protocol tcp src-port 0-65535 dst-port 32000-32000

- set service "Pto._OUTLOOK-6001" protocol tcp src-port 0-65535 dst-port 6001-6001
- set service "Pto._OUTLOOK-6002" protocol tcp src-port 0-65535 dst-port 6002-6002
- set service "Pto._OUTLOOK-6003" protocol tcp src-port 0-65535 dst-port 6003-6003
- set service "Pto._OUTLOOK-6004" protocol tcp src-port 0-65535 dst-port 6004-6004
- set service "Pto-2500" protocol tcp src-port 0-65535 dst-port 2500-2500
- set service "Pto-SIP" protocol udp src-port 0-65535 dst-port 5004-5037
- set service "Pto-SIP" + udp src-port 0-65535 dst-port 10001-20000
- set service "Pto-SIP" + udp src-port 0-65535 dst-port 4569-4569
- set service "Pto-SIP" + tcp src-port 0-65535 dst-port 800-800
- set service "Pto-SIP" + tcp src-port 0-65535 dst-port 22-22
- set service "Pto-SIP" + tcp src-port 0-65535 dst-port 80-80
- set service "Pto-SIP" + udp src-port 0-65535 dst-port 5039-5082
- set service "Pto-5038" protocol tcp src-port 0-65535 dst-port 5038-5038
- set service "Pto-5038" + udp src-port 0-65535 dst-port 5038-5038
- set service "Pto-5038" + tcp src-port 0-65535 dst-port 3306-3306
- set service "Pto-5038" + udp src-port 0-65535 dst-port 3306-3306
- set service "stratix" protocol tcp src-port 0-65535 dst-port 1672-1673
- set service "stratix" + udp src-port 0-65535 dst-port 1672-1673

VPN's

Las necesidades de hoy en día de tener una comunicación, y administración centralizada entre el corporativo y todas las sucursales de la empresa de una forma segura y eficaz, no importando en el lugar que te encuentres se han vuelto una necesidad indispensable.

Por ello para la empresa TECAPPS, se configuro un servicio especial para que esto fuera posible, este servicio es llamado VPN's (Redes Virtuales Privadas), Con lo cual personas solo autorizadas y autenticadas, podrán acceder a los recursos de la empresa que se le hayan asignado. Y así tener una comunicación constante entre Sucursales y Corporativo.

El siguiente diagrama muestra lo descrito anteriormente, en la Empresa TECAPPS.

Fase 1			Fase 2			
Gateway	IP Address/Peer Id	Outgoing-interface	proposal 1	Nombre VPN	Tunnel	Proposal 2
Cliente-Juniper	Usuario-Remotos	ethernet0/4	pre-g2-3des-sha	VPN-Cliente_juniper		g2-esp-3des-sha
GW-AV_Mexico	201.116.65.226	ethernet0/4	pre-g2-3des-sha	GW-AV_Mexico	tunnel.12	g2-esp-3des-sha
GW-Mexico-Infinitem	avmexico	ethernet0/3	pre-g2-3des-sha	GW-Mexico-Infinitem	tunnel.15	g2-esp-3des-sha
GW-Tulyehualco	suctulyehualco	ethernet0/4	pre-g2-3des-sha	VPN-Tulyehualco	tunnel.4	g2-esp-3des-sha
Gw-Chicoloapan	succhicoloapan	ethernet0/4	pre-g2-3des-sha	VPN-Chicoloapan	tunnel.13	g2-esp-3des-sha
Gw-Coyoacan	succoyoacan	ethernet0/4	pre-g2-3des-sha	VPN-Coyoacan	tunnel.6	g2-esp-3des-sha
Gw-Culhuacan	sucecatepec	ethernet0/4	pre-g2-3des-sha	VPN-Culhuacan	tunnel.8	g2-esp-3des-sha
Gw-Ermita	sucermita	ethernet0/4	pre-g2-3des-sha	VPN-Ermita	tunnel.7	g2-esp-3des-sha
Gw-Estadio	sucestadio	ethernet0/4	pre-g2-3des-sha	VPN-Estadio	tunnel.2	g2-esp-
						3des-sha
Gw-Suc	200.67.250.192	ethernet0/3	pre-g2-3des-sha	VPN-Suc	tunnel.14	g2-esp-3des-sha
Gw-Sur16	sucsur16	ethernet0/4	pre-g2-3des-sha	VPN-Sur16	tunnel.10	g2-esp-3des-sha
Gw-Tepozanes	suctepozanes	ethernet0/4	pre-g2-3des-sha	VPN-Tepozanes	tunnel.3	g2-esp-3des-sha
Gw-Tezonco	suctezonco	ethernet0/4	pre-g2-3des-sha	VPN-Tezonco	tunnel.5	g2-esp-3des-sha
Gw-Viaducto	sucursalviaducto	ethernet0/4	pre-g2-3des-sha	VPN-Viaducto	tunnel.1	g2-esp-3des-sha
Gw-Voca7	sucvoca7	ethernet0/4	pre-g2-3des-sha	VPN-Voca7	tunnel.11	g2-esp-3des-sha
Gw-Xochimilco	sucxochimilco	ethernet0/4	pre-g2-3des-sha	VPN-Xochimilco	tunnel.9	g2-esp-3des-sha

TABLAS 15 VPN's

Línea de comando (CLI)

- set ike gateway "Gw-Viaducto" address 0.0.0.0 id "sucursalviaducto" Aggr outgoing-interface "ethernet0/4" preshare "gGcQQecWNcXMumsnPnCtZP9kFanpiRr2qG/e4g3tTz8Mjicq7PGMJzs=" proposal "pre-g2-3des-sha"
- unset ike gateway "Gw-Viaducto" nat-traversal
- set ike gateway "Gw-Estadio" address 0.0.0.0 id "sucestadio" Aggr outgoing-interface "ethernet0/4" preshare

"JEaTZU3CNKGXCPsKVNCqHGCpZFnSmNBcZEVpQDwVeiQy5di/uxP4ml=" proposal "pre-g2-3des-sha"

- unset ike gateway "Gw-Estadio" nat-traversal udp-checksum
- set ike gateway "Gw-Estadio" nat-traversal keepalive-frequency 0
- set ike gateway "Gw-Chicoloapan" address 0.0.0.0 id "succhicoloapan" Aggr outgoing-interface "ethernet0/4" preshare FjF4gH+jNlxLWES5I0C76rrb0anlyPTjkF8EzHJ4A34/6zEpDWePKH0=" proposal "pre-g2-3des-sha"

- set ike gateway "Gw-Chicoloapan" nat-traversal udp-checksum
- set ike gateway "Gw-Chicoloapan" nat-traversal keepalive-frequency 0
- unset ike gateway "Gw-Tepozanes" nat-traversal
- set ike gateway "Gw-Tezonco" address 0.0.0.0 id "suc-tezonco" Aggr outgoing-interface

- "ethernet0/4" preshare
- "C+bdvO9MNVtjBmsomuC2u+YVIrmnzHmTHUWbf7i//HPZwuJxnGnjeOc=" proposal "pre-g2-

- 3des-sha"
- unset ike gateway "Gw-Tezonco" nat-traversal
- set ike gateway "Gw-Coyoacan" address 0.0.0.0 id "succoyoacan" Aggr outgoing-interface

- "ethernet0/4" preshare
- "cU5L2yFWN9SRr2sqjRCTctuYULnkmAH9IQHssYQDoDO3IAThsrFkCxl=" proposal "pre-g1-dessha"

- set ike gateway "Gw-Coyoacan" nat-traversal udp-checksum
- set ike gateway "Gw-Viaducto" heartbeat hello 5
- set ike gateway "Gw-Viaducto" heartbeat reconnect 60
- set ike gateway "Gw-Estadio" heartbeat hello 5
- set ike gateway "Gw-Estadio" heartbeat reconnect 60
- set ike gateway "Gw-Chicoloapan" heartbeat hello 5
- set ike gateway "Gw-Chicoloapan" heartbeat reconnect 60
- set ike gateway "Gw-Tepozanes" heartbeat hello 5
- set ike gateway "Gw-Tepozanes" heartbeat reconnect 60

- set ike gateway "Gw-Tezonco" heartbeat hello 5
- set ike gateway "Gw-Tezonco" heartbeat reconnect 60
- set ike gateway "Gw-Coyoacan" heartbeat hello 5
- set ike gateway "Gw-Coyoacan" heartbeat reconnect 60
- unset ike ikeid-enumeration
- unset ike dos-protection
- unset ipsec access-session enable
- set ipsec access-session maximum 5000
- set ipsec access-session upper-threshold 0
- set ipsec access-session lower-threshold 0
- set ipsec access-session dead-p2-sa-timeout 0
- unset ipsec access-session log-error
- unset ipsec access-session info-exch-connected
- unset ipsec access-session use-error-log
- unset ike ikeid-enumeration
- unset ike dos-protection
- unset ipsec access-session enable
- set ipsec access-session maximum 5000
- set ipsec access-session upper-threshold 0
- set ipsec access-session lower-threshold 0
- set ipsec access-session dead-p2-sa-timeout 0
- unset ipsec access-session log-error
- unset ipsec access-session info-exch-connected
- unset ipsec access-session use-error-log

DEFINICIÓN DE NATEOS (MIP, VIP)

Aquí se configuraron los servidores que se publicaron hacia internet, como por ejemplo WEB, Correo, etc.

TABLA DE NAT					
	MIP		VIP		
	IP Virtual	Host	IP Virtual	Puerto	Host
Ethernet0/0	172.16.1.170	192.168.1.10			
	172.16.1.171	192.168.1.11			
	172.16.1.172	192.168.1.12			
	172.16.1.173	192.168.1.13			
	172.16.1.174	192.168.1.14			
	172.16.1.175	192.168.1.15			
	172.16.1.176	192.168.1.18			
	172.16.1.177	192.168.1.190			
	172.16.1.179	192.168.1.172			
	172.16.1.180	192.168.1.173			
	172.16.1.181	192.168.1.187			
	172.16.1.182	192.168.1.162			
	172.16.1.183	192.168.1.198			
Ethernet0/4	201.116.35.117	192.168.1.12	201.116.35.115	80	192.168.1.10
	201.116.35.114	192.168.1.13	201.116.35.115	25	192.168.1.19
	201.116.35.118	192.168.1.15	201.116.35.115	53	192.168.1.10
	201.116.35.116	192.168.1.187	201.116.35.115	6001	192.168.1.11
	201.116.35.119	192.168.1.16	201.116.35.115	443	192.168.1.11
	201.116.35.120	192.168.1.19	201.116.35.115	6002	192.168.1.11
	201.116.35.121	172.16.1.90	201.116.35.115	6003	192.168.1.11
			201.116.35.115	6004	192.168.1.11
			201.116.35.115	3389	192.168.1.198
Ethernet0/3			200.67.204.204	1672	192.168.1.12
			200.67.204.204	1951	192.168.1.13
			200.67.204.204	21	192.168.1.12
			200.67.204.204	3389	172.16.1.74

TABLAS 16 DEFINICIÓN DE NATEOS (MIP, VIP)

Línea de comando (CLI)

- set interface ethernet0/4 vip interface-ip 80 "HTTP" 192.168.1.10 manual
- set interface ethernet0/4 vip interface-ip 25 "MAIL" 192.168.1.19 manual
- set interface ethernet0/4 vip interface-ip 53 "DNS" 192.168.1.10 manual
- set interface ethernet0/4 vip interface-ip 6001 "Pto._OUTLOOK-6001" 192.168.1.11 manual
- set interface ethernet0/4 vip interface-ip 443 "HTTPS" 192.168.1.11 manual
- set interface ethernet0/4 vip interface-ip 6002 "Pto._OUTLOOK-6002" 192.168.1.11 manual
- set interface ethernet0/4 vip interface-ip 6003 "Pto._OUTLOOK-6003" 192.168.1.11 manual
- set interface ethernet0/4 vip interface-ip 6004 "Pto._OUTLOOK-6004" 192.168.1.11 manual
- set interface ethernet0/4 vip interface-ip 3389 "Pto_Escritorio_remoto" 192.168.1.198 manual
- set interface ethernet0/3 vip interface-ip 1672 "Pto_Stratix-1672" 192.168.1.12 manual
- set interface ethernet0/3 vip interface-ip 1951 "Pto_Visualab-1951" 192.168.1.13 manual
- set interface "ethernet0/0" mip 172.16.1.170 host 192.168.1.10 netmask 255.255.255.255 vr "trust-vr"
- set interface "ethernet0/0" mip 172.16.1.171 host 192.168.1.11 netmask 255.255.255.255 vr "trust-vr"
- set interface "ethernet0/0" mip 172.16.1.172 host 192.168.1.12 netmask 255.255.255.255 vr "trust-vr"
- set interface "ethernet0/0" mip 172.16.1.173 host 192.168.1.13 netmask 255.255.255.255 vr "trust-vr"
- set interface "ethernet0/0" mip 172.16.1.174 host 192.168.1.14 netmask 255.255.255.255 vr "trust-vr"
- set interface "ethernet0/0" mip 172.16.1.175 host 192.168.1.15 netmask 255.255.255.255 vr "trust-vr"
- set interface "ethernet0/0" mip 172.16.1.176 host 192.168.1.18 netmask 255.255.255.255 vr "trust-vr"

- set interface "ethernet0/0" mip 172.16.1.177 host 192.168.1.190 netmask 255.255.255.255 vr "trust-vr"
- set interface "ethernet0/0" mip 172.16.1.179 host 192.168.1.172 netmask 255.255.255.255 vr "trust-vr"
- set interface "ethernet0/0" mip 172.16.1.180 host 192.168.1.173 netmask 255.255.255.255 vr "trust-vr"
- set interface "ethernet0/0" mip 172.16.1.181 host 192.168.1.187 netmask 255.255.255.255 vr "trust-vr"
- set interface "ethernet0/0" mip 172.16.1.182 host 192.168.1.162 netmask 255.255.255.255 vr "trust-vr"

OPTIMIZACIÓN DE POLÍTICAS.

Para tener un mayor control, sobre el acceso y los privilegios que tiene cada usuario, se desarrollaron algunas políticas de seguridad para que se tenga mejor controlada y administrada la red.

Estas políticas pueden ser establecidas para acceder de una zona de seguridad a otra, es decir, se pueden establecer todas las reglas de acceso que se necesiten para que los usuarios puedan acensar a los recursos que requieran.

Las características más importantes de las políticas son: IP origen, IP Destino, Servicio y Acción.

El siguiente diagrama muestra lo descrito anteriormente, en la Empresa TECAPPS...

POLÍTICAS DMZ-UNTRUST

FIREWALL PERIMETRAL

Id Política	Zona Origen	Zona Destino	IP Origen	IP Destino	Servicio	Acción	NAT	Opciones
147	DMZ	Untrust	192.168.1.198/32	65.55.13.91/32	ANY	permit	NAT Origen	log
103	DMZ	Untrust	Exchange	Any	SMTP	deny	NAT Origen	log
105	DMZ	Untrust	192.168.1.19/32	Any	SMTP	permit	NAT Origen	log
106	DMZ	Untrust	192.168.1.20/32	Any	SMTP	permit	NAT Origen	log
2	DMZ	Untrust	Red_DMZ Red_Secure Access	ANY	ANY	permit	NAT Origen	log

TABLAS 17 POLÍTICAS DMZ-UNTRUST

POLÍTICAS DMZ-TRUST

Id Política	Zona Origen	Zona Destino	IP Origen	IP Destino	Servicio	Acción	NAT	Opciones
101	DMZ	Trust	192.168.1.19/32	Red_Jenner Red_Wireless	ANY	permit		log
42	DMZ	Trust	192.168.1.15/32	Red_Jenner Red_Wireless	ANY	permit		log
13	DMZ	Trust	Red_DMZ Red_Secure Access	Red_Jenner Red_Wireless	ANY	permit		log
93	DMZ	Trust	Red_DMZ Red_Secure Access	Red_Jenner Red_Wireless	ANY	permit	NAT Origen	log

TABLAS 18 POLÍTICAS DMZ-TRUST

POLÍTICAS TRUST-DEDICADO

FIREWALL PERIMETRAL

Id Política	Zona Origen	Zona Destino	IP Origen	IP Destino	Servicio	Acción	NAT	Opciones	VPN	Bidireccional Id
153	Trust	Dedicado	172.16.1.16 .7/24	Any	ANY	permit		log		
125	Trust	Dedicado	Red_Jenner	Dial-Up VPN	ANY	tunnel		log	VPN- Cliente_juniper	124-125
116	Trust	Dedicado	Red_Jenner	172.16.150.0/24	ANY	permit		Log		
90	Trust	Dedicado	Red_Jenner	Sucursal_Chicoloapan	ANY	permit		log		
84	Trust	Dedicado	Red_Jenner	Sucursal_AvMexico Sucursal_AvMexico- lab	ANY	permit		log		
82	Trust	Dedicado	Red_Jenner	Sucursal_Voca7	ANY	permit		Log		
77	Trust	Dedicado	Red_Jenner	Sucursal_Sur16	ANY	permit		Log		
74	Trust	Dedicado	Red_Jenner	Sucursal_Xochimilco	ANY	permit		Log		

96	Trust	Dedicado	Any	Any	SMTP	deny	NAT Origen	Log		
110	Trust	Dedicado	Any	Any	POP3	deny	NAT Origen	Log		
27	Trust	Dedicado	Red_Wireless Grupo_AccesoTotal	Any	ANY	permit antivirus	NAT Origen	log		
28	Trust	Dedicado	Red_Jenner	Any	HTTP HTTP- EXT HTTPS	Permit antivirus	NAT Origen	Log filtrado web		

69	Trust	Dedicado	Red_Jenner	Sucursal_Culhuacan	ANY	permit		Log		
66	Trust	Dedicado	Red_Jenner	Sucursal_Ermita	ANY	permit		Log		
61	Trust	Dedicado	Red_Jenner	Sucursal_Coyoacan	ANY	permit		Log		
58	Trust	Dedicado	Red_Jenner	Sucursal_Tezonco	ANY	permit		Log		
52	Trust	Dedicado	Red_Jenner	Sucursal_Tulyehualco	ANY	permit		log		
51	Trust	Dedicado	Red_Jenner	Sucursal_Tepozanes	ANY	permit		Log		
37	Trust	Dedicado	Red_Jenner	Sucursal_Estadio	ANY	permit		Log		
36	Trust	Dedicado	Red_Jenner	Sucursal_Viaducto	ANY	permit		Log		

TABLAS 19 POLÍTICAS TRUST-DEDICADO

POLÍTICAS DEDICADO- TRUST

FIREWALL PERIMETRAL

Id Política	Zona Origen	Zona Destino	IP Origen	IP Destino	Servicio	Acción	NAT	Opciones	VPN	Bidireccional Id
124	Dedicado	Trust	Dial-Up VPN	Red_Jenner	ANY	tunnel	NAT Origencon DIP	log	VPN-Cliente_juniper	124-125
113	Dedicado	Trust	Any	MIP(201.116.35.121)	Pto-SIP SIP	permit	MIP	log		
143	Dedicado	Trust	Any	MIP(201.116.35.121)	ANY	permit	MIP	log		
118	Dedicado	Trust	172.16.150.0/24	Red_Jenner	ANY	permit		log		
89	Dedicado	Trust	Sucursal_C hicoaloapan	Red_Jenner	ANY	permit		log		
86	Dedicado	Trust	Sucursal_A vMexico Sucursal_A vMexico-lab	Red_Jenner	ANY	permit		log		
81	Dedicado	Trust	Sucursal_V oca7	Red_Jenner	ANY	permit		log		
78	Dedicado	Trust	Sucursal_S ur16	Red_Jenner	ANY	permit		log		
72	Dedicado	Trust	Sucursal_X ochimilco	Red_Jenner	ANY	permit		log		
70	Dedicado	Trust	Sucursal_C ulhuacan	Red_Jenner	ANY	permit		log		
65	Dedicado	Trust	Sucursal_Er mita	Red_Jenner	ANY	permit		log		
62	Dedicado	Trust	Sucursal_C oyoacan	Red_Jenner	ANY	permit		log		
57	Dedicado	Trust	Sucursal_T ezonco	Red_Jenner	ANY	permit		log		
54	Dedicado	Trust	Sucursal_T ulyehualco	Red_Jenner	ANY	permit		log		
50	Dedicado	Trust	Sucursal_T epozanes	Red_Jenner	ANY	permit		log		
39	Dedicado	Trust	Sucursal_Vi aducto	Red_Jenner	ANY	permit		log		
38	Dedicado	Trust	Sucursal_Es tadio	Red_Jenner	ANY	permit		log		

TABLAS 20 POLÍTICAS DEDICADO- TRUST

POLÍTICAS TRUST-DMZ

Id Política	Zona Origen	Zona Destino	IP Origen	IP Destino	Servicio	Acción	NAT	Opciones
12	Trust	DMZ	Red_Jenner Red_Wireless	Red_DMZ Red_Secure Access	ANY	permit		Log
132	Trust	DMZ	172.16.1.77/32	MIP(172.16.1.176)	ANY	permit	MIP	Log
139	Trust	DMZ	172.16.1.77/32	MIP(172.16.1.182)	ANY	permit	MIP	Log
138	Trust	DMZ	172.16.1.77/32	MIP(172.16.1.181)	ANY	permit	MIP	log
137	Trust	DMZ	172.16.1.77/32	MIP(172.16.1.180)	ANY	permit	MIP	log
136	Trust	DMZ	172.16.1.77/32	MIP(172.16.1.179)	ANY	permit	MIP	log
133	Trust	DMZ	172.16.1.77/32	MIP(172.16.1.177)	ANY	permit	MIP	log
134	Trust	DMZ	172.16.1.77/32	MIP(172.16.1.176)	ANY	permit	MIP	log
131	Trust	DMZ	172.16.1.77/32	MIP(172.16.1.175)	ANY	permit	MIP	log
130	Trust	DMZ	172.16.1.77/32	MIP(172.16.1.174)	ANY	permit	MIP	log
129	Trust	DMZ	172.16.1.77/32	MIP(172.16.1.173)	ANY	permit	MIP	log
128	Trust	DMZ	172.16.1.77/32	MIP(172.16.1.172)	ANY	permit	MIP	log
127	Trust	DMZ	172.16.1.77/32	MIP(172.16.1.171)	ANY	permit	MIP	log
126	Trust	DMZ	172.16.1.77/32	MIP(172.16.1.170)	ANY	permit	MIP	log
141	Trust	DMZ	172.16.1.77/32	MIP(172.16.1.183)	ANY	permit	MIP	log

TABLAS 21 POLÍTICAS TRUST-DMZ

POLÍTICAS TRUST – INFINITUM

Id Política	Zona Origen	Zona Destino	IP Origen	IP Destino	Servicio	Acción	NAT	Opciones
120	Trust	Infinitem	Red_Jenner	10.30.30.0/24	ANY	permit		Log
97	Trust	Infinitem	Red_Jenner	Any	POP3	deny	NAT Origen	log
95	Trust	Infinitem	Red_Jenner	Any	SMTP	deny	NAT Origen	log
25	Trust	Infinitem	Red_Wireless Grupo_AccesoTotal	Any	HTTP HTTP- EXT HTTPS	permit antivirus	NAT Origen	log
46	Trust	Infinitem	Red_Jenner	Any	MS- MESSENGER MSN MSN	deny	NAT Origen	log
24	Trust	Infinitem	Red_Jenner	Any	HTTP HTTP- EXT HTTPS	permit antivirus	NAT Origen	log webfiltering
8	Trust	Infinitem	Red_Jenner	Any	ANY	permit deepinspect ion	NAT Origen	log

TABLAS 22 POLÍTICAS TRUST – INFINITUM

POLÍTICAS TRUST – UNTRUST

Id Política	Zona Origen	Zona Destino	IP Origen	IP Destino	Servicio	Acción	NAT	Opciones
98	Trust	Untrust	Red_Jenner	Any	POP3	Deny	NAT origen	log
94	Trust	Untrust	Red_Jenner	Any	SMTP	Deny	NAT origen	log
32	Trust	Untrust	Red_Wireless Grupo_AccesoTotal	Any	HTTP HTTP- EXT HTTPS	permit antivirus	NAT origen	log
23	Trust	Untrust	callcenter4	Any	HTTP HTTP- EXT HTTPS	permit	NAT origen	log
45	Trust	Untrust	Red_Jenner	Any	MS- MESSENGER MSN MSN	Deny	NAT origen	log
20	Trust	Untrust	Red_Jenner	Any	HTTP HTTP- EXT HTTPS	permit antivirus	NAT origen	log Web Filtering
1	Trust	Untrust	Red_Jenner	Any	Any	permit deepinspect ion	NAT origen	log

TABLAS 23 POLÍTICAS TRUST – UNTRUST

POLÍTICAS UNTRUST- TRUST

Id Política	Zona Origen	Zona Destino	IP Origen	IP Destino	Servicio	Acción	NAT	Opciones
112	Untrust	Trust	Any	MIP(201.116.35.121)	Pto-SIP	permit	MIP	Log

TABLAS 24 POLÍTICAS UNTRUST- TRUST

POLÍTICAS DMZ-INFINITUM

Id Política	Zona Origen	Zona Destino	IP Origen	IP Destino	Servicio	Acción	NAT	Opciones
9	DMZ	Infinitem	Red_DMZ Red_Secure Access	Any	Any	permit	NAT Origen	log

TABLAS 25 POLÍTICAS DMZ-INFINITUM

POLÍTICAS DMZ-DEDICADO

FIREWALL PERIMETRAL

Id Política	Zona Origen	Zona Destino	IP Origen	IP Destino	Servicio	Acción	NAT	Opciones
117	DMZ	Dedicado	Red_DMZ Red_Secure Access	172.16.150.0/24	Any	permit		log
91	DMZ	Dedicado	Red_DMZ Red_Secure Access	Sucursal_Chico oapan	Any	permit		log
85	DMZ	Dedicado	Red_DMZ Red_Secure Access	Sucursal_AvMexico Sucursal_AvMexico-lab	Any	permit		log
83	DMZ	Dedicado	Red_DMZ Red_Secure Access	Sucursal_Voca7	Any	permit		log
73	DMZ	Dedicado	Red_DMZ Red_Secure Access	Sucursal_Sur16	Any	permit		log
75	DMZ	Dedicado	Red_DMZ Red_Secure Access	Sucursal_Xochimilco	Any	permit		log
68	DMZ	Dedicado	Red_DMZ Red_Secure Access	Sucursal_Culhuacan	Any	permit		log
67	DMZ	Dedicado	Red_DMZ Red_Secure Access	Sucursal_Ermita	Any	permit		log
60	DMZ	Dedicado	Red_DMZ Red_Secure Access	Sucursal_Coyocan	Any	permit		log

FIREWALL PERIMETRAL

59	DMZ	Dedicado	Red_DMZ Red_Secure Access	Sucursal_Tezonco	Any	permit		log
53	DMZ	Dedicado	Red_DMZ Red_Secure Access	Sucursal_Tulyehualco	Any	permit		log
48	DMZ	Dedicado	Red_DMZ Red_Secure Access	Sucursal_Tepozanes	Any	permit		log
47	DMZ	Dedicado	Red_DMZ Red_Secure Access	Sucursal_Estadio	Any	permit		log
43	DMZ	Dedicado	Red_DMZ Red_Secure Access	Sucursal_Viaducto	Any	permit		log

102	DMZ	Dedicado	Exchange	Any	POP3	permit	NAT origen	Log
104	DMZ	Dedicado	192.168.1.19/32	Any	Any	permit	NAT origen	Log
152	DMZ	Dedicado	192.168.1.20/32	Any	Any	permit	NAT origen	Log
26	DMZ	Dedicado	192.168.1.20/32	Any	Any	permit	NAT origen	Log
34	DMZ	Dedicado	Visualab Web	Any	Any	permit	NAT origen	Log
11	DMZ	Dedicado	Red_DMZ Red_Secure Access	Any	Any	permit	NAT origen	log
151	DMZ	Dedicado	192.168.1.198/32	Any	HTTP	permit	NAT origen	Log

TABLAS 26 POLÍTICAS DMZ-DEDICADO

POLÍTICAS DEDICADO-INFINITUM

Id Política	Zona Origen	Zona Destino	IP Origen	IP Destino	Servicio	Acción	NAT	Opciones
122	Dedicado	Infinitem	Sucursal_AvMexico Sucursal_AvMexico-lab Sucursal_Chicoloapan Sucursal_Culhuacan Sucursal_Ermita Sucursal_Estadio Sucursal_Sur16 Sucursal_Tepozanes Sucursal_Tulyehualco Sucursal_Tezonco Sucursal_Viaducto Sucursal_Voca7	10.30.30.0/24	Any	permit		log

TABLAS 27 POLÍTICAS DEDICADO-INFINITUM

POLÍTICAS DEDICADO- DMZ

Id Política	Zona Origen	Zona Destino	IP Origen	IP Destino	Servicio	Acción	NAT	Opciones
145	Dedicado	DMZ	172.16.117.11/32	Stratix	stratix	permit		Log
144	Dedicado	DMZ	172.16.106.10/32	Stratix	stratix	permit		Log
119	Dedicado	DMZ	172.16.150.0/24	Red_Secure Access Red_DMZ	ANY	permit		log
88	Dedicado	DMZ	Sucursal_Chicoloapan	Red_DMZ Red_Secure Access	ANY	permit		log
87	Dedicado	DMZ	Sucursal_AvMexico Sucursal_AvMexico-lab	Red_DMZ Red_Secure Access	ANY	permit		log
80	Dedicado	DMZ	Sucursal_Voca7	Red_DMZ Red_Secure Access	ANY	permit		log
79	Dedicado	DMZ	Sucursal_Sur16	Red_DMZ Red_Secure Access	ANY	permit		log
73	Dedicado	DMZ	Sucursal_Xochimilco	Red_DMZ Red_Secure Access	ANY	permit		log
71	Dedicado	DMZ	Sucursal_Culhuacan	Red_DMZ Red_Secure Access	ANY	permit		log
64	Dedicado	DMZ	Sucursal_Ermita	Red_DMZ Red_Secure Access	ANY	permit		log

FIREWALL PERIMETRAL

63	Dedicado	DMZ	Sucursal_Coyoacan	Red_DMZ Red_Secure Access	ANY	permit		log
56	Dedicado	DMZ	Sucursal_Tezonco	Red_DMZ Red_Secure Access	ANY	permit		log
55	Dedicado	DMZ	Sucursal_Tulyehualco	Red_DMZ Red_Secure Access	ANY	permit		log
49	Dedicado	DMZ	Sucursal_Tepozanes	Red_DMZ Red_Secure Access	ANY	permit		log
41	Dedicado	DMZ	Sucursal_Viaducto	Red_DMZ Red_Secure Access	ANY	permit		log
40	Dedicado	DMZ	Sucursal_Estadio	Red_DMZ Red_Secure Access	ANY	permit		log
3	Dedicado	DMZ	Any	VIP(ethernet0/4)	ANY	permit	VIP	Log
16	Dedicado	DMZ	Any	MIP(201.116.35.114)	Pto_Visualab-1951	permit	MIP	Log
44	Dedicado	DMZ	Any	MIP(201.116.35.116)	HTTP	permit	MIP	Log
29	Dedicado	DMZ	Any	MIP(201.116.35.117)	Pto_Escritorio_remot o	permit	MIP	Log
22	Dedicado	DMZ	Any	MIP(201.116.35.118)	ANY	permit	MIP	Log
92	Dedicado	DMZ	Any	MIP(201.116.35.119)	HTTPS	permit	MIP	Log
142	Dedicado	DMZ	Any	MIP(201.116.35.120)	ANY	permit	MIP	Log

TABLAS 28 POLÍTICAS DEDICADO- DMZ

POLÍTICAS INFINITUM-DEDICADO

Id Política	Zona Origen	Zona Destino	IP Origen	IP Destino	Servicio	Acción	NAT	Opciones
123	infinitem	Dedicado	10.30.30.0/24	Sucursal_AvMexico Sucursal_AvMexico-lab Sucursal_Chicoloapan Sucursal_Coyoacan Sucursal_Culhuacan Sucursal_Ermita Sucursal_Estadio Sucursal_Sur16 Sucursal_Tepozanes Sucursal_Tezonco Sucursal_Tulyehualco Sucursal_Viaducto Sucursal_Voca7	ANY	permit		Log

TABLAS 29 POLÍTICAS INFINITUM-DEDICADO

POLÍTICAS INFINITUM-TRUST

Id Política	Zona Origen	Zona Destino	IP Origen	IP Destino	Servicio	Acción	NAT	Opciones
115	Infinitem	Trust	10.30.30.7/32	Red_Jenner	ANY	permit		log
33	Infinitem	Trust	Any	VIP(ethernet0/3)	Pto_Escritorio_remo to	permit	VIP	log
146	Infinitem	Trust	10.30.30.8/32	Red_Jenner	ANY	permit		log

TABLAS 30 POLÍTICAS INFINITUM-TRUST

POLÍTICAS INFINITUM-DMZ

Id Política	Zona Origen	Zona Destino	IP Origen	IP Destino	Servicio	Acción	NAT	Opciones
17	Infinitem	DMZ	Any	VIP(ethernet0/3)	ANY	permit	VIP	log

TABLAS 31 POLÍTICAS INFINITUM-DMZ

Línea de comando (CLI)

- set policy id 147 from "DMZ" to "Untrust" "192.168.1.198/32" "65.55.13.91/32"
"ANY" nat src permit log
- set policy id 147
- exit
- set policy id 12 from "Trust" to "DMZ" "Red_Tecapps" "Red_DMZ" "ANY"
permit log
- set policy id 12
- set src-address "Red_Wireless"
- set dst-address "Red_Secure Access"
- exit
- set policy id 132 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.176)"
"ANY" permit log
- set policy id 132
- exit
- set policy id 139 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.182)"
"ANY" permit log
- set policy id 139

- exit
- set policy id 138 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.181)"
"ANY" permit log
- set policy id 138
- exit
- set policy id 137 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.180)"
"ANY" permit log
- set policy id 137
- exit
- set policy id 136 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.179)"
"ANY" permit log
- set policy id 136
- exit
- set policy id 133 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.177)"
"ANY" permit log
- set policy id 133
- exit
- set policy id 134 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.176)"
"ANY" permit log
- set policy id 134
- exit
- set policy id 131 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.175)"
"ANY" permit log
- set policy id 131
- exit
- set policy id 130 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.174)"
"ANY" permit log
- set policy id 130
- exit
- set policy id 129 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.173)"
"ANY" permit log
- set policy id 129

- exit
- set policy id 128 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.172)"
"ANY" permit log
- set policy id 128
- exit
- set policy id 127 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.171)"
"ANY" permit log
- set policy id 127
- exit
- set policy id 126 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.170)"
"ANY" permit log
- set policy id 126
- exit
- set policy id 124 from "Dedicado" to "Trust" "Dial-Up VPN" "Red_Tecapps"
"ANY" nat src dip-id 6 tunnel vpn "VPN-Cliente_juniper" id 0x30 pair-policy 125 log
- set policy id 124
- exit
- set policy id 113 from "Dedicado" to "Trust" "Any" "MIP(201.116.35.121)"
"Pto-SIP" permit log
- set policy id 113 application "IGNORE"
- set policy id 113
- set service "SIP"
- exit
- set policy id 143 from "Dedicado" to "Trust" "Any" "MIP(201.116.35.121)"
"ANY" permit log
- set policy id 143
- exit
- set policy id 123 from "Infinitum" to "Dedicado" "10.30.30.0/24"
"Sucursal_AvMexico" "ANY" permit log
- set policy id 123
- set dst-address "Sucursal_AvMexico-lab"
- set dst-address "Sucursal_Chicoloapan"

- set dst-address "Sucursal_Coyoacan"
- set dst-address "Sucursal_Culhuacan"
- set dst-address "Sucursal_Ermita"
- set dst-address "Sucursal_Estadio"
- set dst-address "Sucursal_Sur16"
- set dst-address "Sucursal_Tepozanes"
- set dst-address "Sucursal_Tezonco"
- set dst-address "Sucursal_Tulyehualco"
- set dst-address "Sucursal_Viaducto"
- set dst-address "Sucursal_Voca7"
- set dst-address "Sucursal_Xochimilco"
- exit
- set policy id 122 from "Dedicado" to "Infinitum" "Sucursal_AvMexico"
"10.30.30.0/24" "ANY" permit log
- set policy id 122
- set src-address "Sucursal_AvMexico-lab"
- set src-address "Sucursal_Chicoloapan"
- set src-address "Sucursal_Culhuacan"
- set src-address "Sucursal_Ermita"
- set src-address "Sucursal_Estadio"
- set src-address "Sucursal_Sur16"
- set src-address "Sucursal_Tepozanes"
- set src-address "Sucursal_Tezonco"
- set src-address "Sucursal_Tulyehualco"
- set src-address "Sucursal_Viaducto"
- set src-address "Sucursal_Voca7"
- exit
- set policy id 120 from "Trust" to "Infinitum" "Red_Tecapps" "10.30.30.0/24"
"ANY" permit log
- set policy id 120
- exit

- set policy id 145 from "Dedicado" to "DMZ" "172.16.117.11/32" "Stratix"
"stratix" permit log
- set policy id 145
- exit
- set policy id 144 from "Dedicado" to "DMZ" "172.16.106.10/32" "Stratix"
"stratix" permit log
- set policy id 144
- exit
- set policy id 119 from "Dedicado" to "DMZ" "172.16.150.0/24" "Red_DMZ"
"ANY" permit log
- set policy id 119
- set dst-address "Red_Secure Access"
- exit
- set policy id 118 from "Dedicado" to "Trust" "172.16.150.0/24"
"Red_Tecapps" "ANY" permit log
- set policy id 118
- exit
- set policy id 117 from "DMZ" to "Dedicado" "Red_DMZ" "172.16.150.0/24"
"ANY" permit log
- set policy id 117
- set src-address "Red_Secure Access"
- exit
- set policy id 125 from "Trust" to "Dedicado" "Red_Tecapps" "Dial-Up VPN"
"ANY" tunnel vpn "VPNCliente_juniper" id 0x30 pair-policy 124 log
- set policy id 125
- exit
- set policy id 116 from "Trust" to "Dedicado" "Red_Tecapps"
"172.16.150.0/24" "ANY" permit log
- set policy id 116
- exit
- set policy id 112 from "Untrust" to "Trust" "Any" "MIP(201.116.35.121)" "Pto-
SIP" permit log

- set policy id 112
- exit
- set policy id 103 from "DMZ" to "Untrust" "Exchange" "Any" "SMTP" nat src deny log
- set policy id 103
- exit
- set policy id 105 from "DMZ" to "Untrust" "192.168.1.19/32" "Any" "SMTP" nat src permit log
- set policy id 105 disable
- set policy id 105
- exit
- set policy id 106 from "DMZ" to "Untrust" "192.168.1.20/32" "Any" "SMTP" nat src permit log
- set policy id 106 disable
- set policy id 106
- exit
- set policy id 101 from "DMZ" to "Trust" "192.168.1.19/32" "Red_Tecapps" "ANY" permit log
- set policy id 101
- set dst-address "Red_Wireless"
- exit
- set policy id 98 from "Trust" to "Untrust" "Red_Tecapps" "Any" "POP3" nat src deny log
- set policy id 98
- exit
- set policy id 97 from "Trust" to "Infinitum" "Red_Tecapps" "Any" "POP3" nat src deny log
- set policy id 97
- exit
- set policy id 95 from "Trust" to "Infinitum" "Red_Tecapps" "Any" "SMTP" nat src deny log
- set policy id 95

- exit
- set policy id 94 from "Trust" to "Untrust" " Red_Tecapps " "Any" "SMTP" nat src deny log
- set policy id 94
- exit
- set policy id 91 from "DMZ" to "Dedicado" "Red_DMZ" "Sucursal_Chicoloapan" "ANY" permit log
- set policy id 91
- set src-address "Red_Secure Access"
- exit
- set policy id 90 from "Trust" to "Dedicado" " Red_Tecapps " "Sucursal_Chicoloapan" "ANY" permit log
- set policy id 90
- exit
- set policy id 89 from "Dedicado" to "Trust" "Sucursal_Chicoloapan" " Red_Tecapps " "ANY" permit log
- set policy id 89
- exit
- set policy id 88 from "Dedicado" to "DMZ" "Sucursal_Chicoloapan" "Red_DMZ" "ANY" permit log
- set policy id 88
- set dst-address "Red_Secure Access"
- exit
- set policy id 87 from "Dedicado" to "DMZ" "Sucursal_AvMexico" "Red_DMZ" "ANY" permit log
- set policy id 87
- set src-address "Sucursal_AvMexico-lab"
- set dst-address "Red_Secure Access"
- exit
- set policy id 86 from "Dedicado" to "Trust" "Sucursal_AvMexico" " Red_Tecapps " "ANY" permit log
- set policy id 86

- set src-address "Sucursal_AvMexico-lab"
- exit
- set policy id 85 from "DMZ" to "Dedicado" "Red_DMZ" "Sucursal_AvMexico"
"ANY" permit log
- set policy id 85
- set src-address "Red_Secure Access"
- set dst-address "Sucursal_AvMexico-lab"
- exit
- set policy id 84 from "Trust" to "Dedicado" " Red_Tecapps "
"Sucursal_AvMexico" "ANY" permit log
- set policy id 84
- set dst-address "Sucursal_AvMexico-lab"
- exit
- set policy id 83 from "DMZ" to "Dedicado" "Red_DMZ" "Sucursal_Voca7"
"ANY" permit log
- set policy id 83
- set src-address "Red_Secure Access"
- exit
- set policy id 82 from "Trust" to "Dedicado" " Red_Tecapps" "Sucursal_Voca7"
"ANY" permit log
- set policy id 82
- exit
- set policy id 81 from "Dedicado" to "Trust" "Sucursal_Voca7" " Red_Tecapps "
"ANY" permit log
- set policy id 81
- exit
- set policy id 80 from "Dedicado" to "DMZ" "Sucursal_Voca7" "Red_DMZ"
"ANY" permit log
- set policy id 80
- set dst-address "Red_Secure Access"
- exit

- set policy id 79 from "Dedicado" to "DMZ" "Sucursal_Sur16" "Red_DMZ"
"ANY" permit log
- set policy id 79
- set dst-address "Red_Secure Access"
- exit
- set policy id 78 from "Dedicado" to "Trust" "Sucursal_Sur16" " Red_Tecapps"
"ANY" permit log
- set policy id 78
- exit
- set policy id 77 from "Trust" to "Dedicado" Red_Tecapps " "Sucursal_Sur16"
"ANY" permit log
- set policy id 77
- exit
- set policy id 76 from "DMZ" to "Dedicado" "Red_DMZ" "Sucursal_Sur16"
"ANY" permit log
- set policy id 76
- set src-address "Red_Secure Access"
- exit
- set policy id 74 from "Trust" to "Dedicado" " Red_Tecapps"
"Sucursal_Xochimilco" "ANY" permit log
- set policy id 74
- exit
- set policy id 73 from "Dedicado" to "DMZ" "Sucursal_Xochimilco" "Red_DMZ"
"ANY" permit log
- set policy id 73
- set dst-address "Red_Secure Access"
- exit
- set policy id 72 from "Dedicado" to "Trust" "Sucursal_Xochimilco" "
Red_Tecapps" "ANY" permit log
- set policy id 72
- exit

- set policy id 70 from "Dedicado" to "Trust" "Sucursal_Culhuacan" "Red_Tecapps" "ANY" permit log
- set policy id 70
- exit
- set policy id 69 from "Trust" to "Dedicado" "Red_Tecapps" "Sucursal_Culhuacan" "ANY" permit log
- set policy id 69
- exit
- set policy id 75 from "DMZ" to "Dedicado" "Red_DMZ" "Sucursal_Xochimilco" "ANY" permit log
- set policy id 75
- set src-address "Red_Secure Access"
- exit
- set policy id 68 from "DMZ" to "Dedicado" "Red_DMZ" "Sucursal_Culhuacan" "ANY" permit log
- set policy id 68
- set src-address "Red_Secure Access"
- exit
- set policy id 67 from "DMZ" to "Dedicado" "Red_DMZ" "Sucursal_Ermita" "ANY" permit log
- set policy id 67
- set src-address "Red_Secure Access"
- exit
- set policy id 66 from "Trust" to "Dedicado" "Red_Tecapps" "Sucursal_Ermita" "ANY" permit log
- set policy id 66
- exit
- set policy id 71 from "Dedicado" to "DMZ" "Sucursal_Culhuacan" "Red_DMZ" "ANY" permit log
- set policy id 71
- set dst-address "Red_Secure Access"
- exit

- set policy id 64 from "Dedicado" to "DMZ" "Sucursal_Ermita" "Red_DMZ"
"ANY" permit log
- set policy id 64
- set dst-address "Red_Secure Access"
- exit
- set policy id 63 from "Dedicado" to "DMZ" "Sucursal_Coyoacan" "Red_DMZ"
"ANY" permit log
- set policy id 63
- set dst-address "Red_Secure Access"
- exit
- set policy id 65 from "Dedicado" to "Trust" "Sucursal_Ermita" " Red_Tecapps"
"ANY" permit log
- set policy id 65
- exit
- set policy id 62 from "Dedicado" to "Trust" "Sucursal_Coyoacan"
Red_Tecapps" "ANY" permit log
- set policy id 62
- exit
- set policy id 61 from "Trust" to "Dedicado" Red_Tecapps"
"Sucursal_Coyoacan" "ANY" permit log
- set policy id 61
- exit
- set policy id 60 from "DMZ" to "Dedicado" "Red_DMZ" "Sucursal_Coyoacan"
"ANY" permit log
- set policy id 60
- set src-address "Red_Secure Access"
- exit
- set policy id 59 from "DMZ" to "Dedicado" "Red_DMZ" "Sucursal_Tezonco"
"ANY" permit log
- set policy id 59
- set src-address "Red_Secure Access"
- exit

- set policy id 58 from "Trust" to "Dedicado" " Red_Tecapps"
"Sucursal_Tezonco" "ANY" permit log
- set policy id 58
- exit
- set policy id 57 from "Dedicado" to "Trust" "Sucursal_Tezonco" "
Red_Tecapps" "ANY" permit log
- set policy id 57
- exit
- set policy id 56 from "Dedicado" to "DMZ" "Sucursal_Tezonco" "Red_DMZ"
"ANY" permit log
- set policy id 56
- set dst-address "Red_Secure Access"
- exit
- set policy id 55 from "Dedicado" to "DMZ" "Sucursal_Tulyehualco"
"Red_DMZ" "ANY" permit log
- set policy id 55
- set dst-address "Red_Secure Access"
- exit
- set policy id 54 from "Dedicado" to "Trust" "Sucursal_Tulyehualco" "
Red_Tecapps" "ANY" permit log
- set policy id 54
- exit
- set policy id 53 from "DMZ" to "Dedicado" "Red_DMZ"
"Sucursal_Tulyehualco" "ANY" permit log
- set policy id 53
- set src-address "Red_Secure Access"
- exit
- set policy id 52 from "Trust" to "Dedicado" " Red_Tecapps"
"Sucursal_Tulyehualco" "ANY" permit log
- set policy id 52
- exit

- set policy id 50 from "Dedicado" to "Trust" "Sucursal_Tepozanes" "Red_Tecapps" "ANY" permit log
- set policy id 50
- exit
- set policy id 49 from "Dedicado" to "DMZ" "Sucursal_Tepozanes" "Red_DMZ" "ANY" permit log
- set policy id 49
- set dst-address "Red_Secure Access"
- exit
- set policy id 48 from "DMZ" to "Dedicado" "Red_DMZ" "Sucursal_Tepozanes" "ANY" permit log
- set policy id 48
- set src-address "Red_Secure Access"
- exit
- set policy id 47 from "DMZ" to "Dedicado" "Red_DMZ" "Sucursal_Estadio" "ANY" permit log
- set policy id 47
- set src-address "Red_Secure Access"
- exit
- set policy id 43 from "DMZ" to "Dedicado" "Red_DMZ" "Sucursal_Viaducto" "ANY" permit log
- set policy id 43
- set src-address "Red_Secure Access"
- exit
- set policy id 102 from "DMZ" to "Dedicado" "Exchange" "Any" "POP3" nat src permit log
- set policy id 102
- exit
- set policy id 104 from "DMZ" to "Dedicado" "192.168.1.19/32" "Any" "ANY" nat src permit log
- set policy id 104
- exit

- set policy id 152 from "DMZ" to "Dedicado" "192.168.1.20/32" "Any" "ANY" nat src permit log
- set policy id 152
- exit
- set policy id 26 from "DMZ" to "Dedicado" "192.168.1.20/32" "Any" "ANY" nat src permit log
- set policy id 26 disable
- set policy id 26
- exit
- set policy id 42 from "DMZ" to "Trust" "192.168.1.15/32" " Red_Tecapps" "ANY" permit log
- set policy id 42
- set dst-address "Red_Wireless"
- exit
- set policy id 41 from "Dedicado" to "DMZ" "Sucursal_Viaducto" "Red_DMZ" "ANY" permit log
- set policy id 41
- set dst-address "Red_Secure Access"
- exit
- set policy id 40 from "Dedicado" to "DMZ" "Sucursal_Estadio" "Red_DMZ" "ANY" permit log
- set policy id 40
- set dst-address "Red_Secure Access"
- exit
- set policy id 3 from "Dedicado" to "DMZ" "Any" "VIP(ethernet0/4)" "ANY" permit log
- set policy id 3
- exit
- set policy id 16 from "Dedicado" to "DMZ" "Any" "MIP(201.116.35.114)" "Pto_Visualab-1951" permit log
- set policy id 16
- exit

- set policy id 44 from "Dedicado" to "DMZ" "Any" "MIP(201.116.35.116)" "HTTP" permit log
- set policy id 44
- exit
- set policy id 39 from "Dedicado" to "Trust" "Sucursal_Viaducto" " Red_Tecapps " "ANY" permit log
- set policy id 39
- exit
- set policy id 38 from "Dedicado" to "Trust" "Sucursal_Estadio" " Red_Tecapps " "ANY" permit log
- set policy id 38
- exit
- set policy id 51 from "Trust" to "Dedicado" " Red_Tecapps" "Sucursal_Tepozanes" "ANY" permit log
- set policy id 51
- exit
- set policy id 37 from "Trust" to "Dedicado" " Red_Tecapps" "Sucursal_Estadio" "ANY" permit log
- set policy id 37
- exit
- set policy id 36 from "Trust" to "Dedicado" " Red_Tecapps" "Sucursal_Viaducto" "ANY" permit log
- set policy id 36
- exit
- set policy id 96 from "Trust" to "Dedicado" "Any" "Any" "SMTP" nat src deny log
- set policy id 96
- exit
- set policy id 110 from "Trust" to "Dedicado" "Any" "Any" "POP3" nat src deny log
- set policy id 110
- exit

- policy id 34 from "DMZ" to "Dedicado" "Visualab" "Any" "ANY" nat src permit log
- set policy id 34
- set src-address "Web"
- exit
- set policy id 115 from "Infinitum" to "Trust" "10.30.30.7/32" "Red_Tecapps" "ANY" permit log
- set policy id 115
- exit
- set policy id 33 from "Infinitum" to "Trust" "Any" "VIP(ethernet0/3)" "Pto_Escritorio_remoto" permit log
- set policy id 33
- exit
- set policy id 32 from "Trust" to "Untrust" "Red_Wireless" "Any" "HTTP" nat src permit log count
- set policy id 32 av "AV-Tecapps"
- set policy id 32
- set src-address "Grupo_AccesoTotal"
- set service "HTTP-EXT"
- set service "HTTPS"
- exit
- set policy id 29 from "Dedicado" to "DMZ" "Any" "MIP(201.116.35.117)" "Pto_Escritorio_remoto" permit log
- set policy id 29
- exit
- set policy id 27 from "Trust" to "Dedicado" "Red_Wireless" "Any" "ANY" nat src permit log
- set policy id 27 av "AV-Tecapps"
- set policy id 27
- set src-address "Grupo_AccesoTotal"
- exit

- set policy id 28 from "Trust" to "Dedicado" "Red_Tecapps" "Any" "HTTP" nat src permit log url-filter
- set policy id 28 av "Av-Tecapps_Mortales"
- set policy id 28
- set service "HTTP-EXT"
- set service "HTTPS"
- set url protocol sc-cpa profile "Filtrado_Tecapps"
- exit
- set policy id 25 from "Trust" to "Infinitum" "Red_Wireless" "Any" "HTTP" nat src permit log
- set policy id 25 av "AV-Tecapps"
- set policy id 25
- set src-address "Grupo_AccesoTotal"
- set service "HTTP-EXT"
- set service "HTTPS"
- set url protocol sc-cpa profile "Filtrado_Tecapps"
- exit
- set policy id 46 from "Trust" to "Infinitum" "Red_Tecapps" "Any" "MS-MESSENGER" nat src deny log
- set policy id 46
- set service "MSN"
- set service "NSM"
- exit
- set policy id 24 from "Trust" to "Infinitum" "Red_Tecapps" "Any" "HTTP" nat src permit log url-filter
- set policy id 24 attack "HIGH:CHAT:SIGS" action drop ip-action "notify" target "serv" timeout 60
- set policy id 24
- set attack "INFO:CHAT:SIGS" action "drop" ip-action "notify" target "serv" timeout 60
- set attack "INFO:CHAT:ANOM" action "drop" ip-action "notify" target "serv" timeout 60

- exit
- set policy id 24 av "Av-Tecapps_Mortales"
- set policy id 24
- set service "HTTP-EXT"
- set service "HTTPS"
- set url protocol sc-cpa profile "Filtrado_Tecapps"
- exit
- set policy id 23 from "Trust" to "Untrust" "callcenter4" "Any" "HTTP" nat src permit log count
- set policy id 23
- set service "HTTP-EXT"
- set service "HTTPS"
- exit
- set policy id 45 from "Trust" to "Untrust" "Red_Tecapps" "Any" "MS-MESSENGER" nat src deny log count
- set policy id 45
- set service "MSN"
- set service "NSM"
- exit
- set policy id 2 from "DMZ" to "Untrust" "Red_DMZ" "Any" "ANY" nat src permit log
- set policy id 2
- set src-address "Red_Secure Access"
- exit
- set policy id 8 from "Trust" to "Infinitum" "Red_Tecapps" "Any" "ANY" nat src permit log
- set policy id 8 attack "HIGH:CHAT:SIGS" action drop ip-action "notify" target "serv" timeout 60
- set policy id 8
- set attack "INFO:CHAT:SIGS" action "drop" ip-action "notify" target "serv" timeout 60

- set attack "INFO:CHAT:ANOM" action "drop" ip-action "notify" target "serv" timeout 60
- exit
- set policy id 8
- exit
- set policy id 9 from "DMZ" to "Infinitum" "Red_DMZ" "Any" "ANY" nat src permit log
- set policy id 9
- set src-address "Red_Secure Access"
- exit
- set policy id 11 from "DMZ" to "Dedicado" "Red_DMZ" "Any" "ANY" nat src permit log
- set policy id 11
- set src-address "Red_Secure Access"
- exit
- set policy id 13 from "DMZ" to "Trust" "Red_DMZ" "Red_Tecapps" "ANY" permit log
- set policy id 13
- set src-address "Red_Secure Access"
- set dst-address "Red_Wireless"
- exit
- set policy id 93 from "DMZ" to "Trust" "Red_DMZ" "Red_Tecapps" "ANY" nat src permit log
- set policy id 93 disable
- set policy id 93
- set src-address "Red_Secure Access"
- set dst-address "Red_Wireless"
- exit
- set policy id 17 from "Infinitum" to "DMZ" "Any" "VIP(ethernet0/3)" "ANY" permit log
- set policy id 17
- exit

- set policy id 20 from "Trust" to "Untrust" "Red_Tecapps" "Any" "HTTP" nat src permit log count url-filter
- set policy id 20 attack "HIGH:CHAT:SIGS" action drop ip-action "notify" target "serv" timeout 60
- set policy id 20
- set attack "INFO:CHAT:SIGS" action "drop" ip-action "notify" target "serv" timeout 60
- set attack "INFO:CHAT:ANOM" action "drop" ip-action "notify" target "serv" timeout 60
- exit
- set policy id 20 av "Av-Tecapps_Mortales"
- set policy id 20
- set service "HTTP-EXT"
- set service "HTTPS"
- set url protocol sc-cpa profile "Filtrado_Tecapps"
- exit
- set policy id 1 from "Trust" to "Untrust" "Red_Tecapps" "Any" "ANY" nat src permit log
- set policy id 1 attack "HIGH:CHAT:SIGS" action drop ip-action "notify" target "serv" timeout 60
- set policy id 1
- set attack "INFO:CHAT:SIGS" action "drop" ip-action "notify" target "serv" timeout 60
- set attack "INFO:CHAT:ANOM" action "drop" ip-action "notify" target "serv" timeout 60
- exit
- set policy id 1
- exit
- set policy id 22 from "Dedicado" to "DMZ" "Any" "MIP(201.116.35.118)" "ANY" permit log
- set policy id 22
- exit

- set policy id 92 from "Dedicado" to "DMZ" "Any" "MIP(201.116.35.119)"
"HTTPS" permit log
- set policy id 92
- exit
- set policy id 141 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.183)"
"ANY" permit log
- set policy id 141
- exit
- set policy id 142 from "Dedicado" to "DMZ" "Any" "MIP(201.116.35.120)"
"ANY" permit log
- set policy id 142
- exit
- set policy id 146 from "Infinitum" to "Trust" "10.30.30.8/32" "Red_Tecapps"
"ANY" permit log
- set policy id 146
- exit
- set policy id 151 from "DMZ" to "Dedicado" "192.168.1.198/32" "Any" "HTTP"
nat src permit log
- set policy id 151
- exit

A continuación, se muestra la configuración final que tiene el firewall SSG 140, la cual contiene todo lo explicado anteriormente.

```
unset key protection enable
```

```
set clock timezone -6
```

```
set vrouter trust-vr sharable
```

```
set vrouter "untrust-vr"
```

```
exit

set vrouter "trust-vr"

unset auto-route-export

exit

set vrouter name "VR-Infinitem" id 1025 sharable

unset vrouter "VR-Infinitem" nsrp-config-sync

set vrouter "VR-Infinitem"

unset auto-route-export

set preference nhrp 100

set preference ospf-e2 254

exit

set service "Pto_Visualab-1951" protocol tcp src-port 0-65535 dst-port 1951-1951

set service "Pto_Escritorio_remoto" protocol tcp src-port 0-65535 dst-port 3389-3389

set service "Pto_Stratix-1672" protocol tcp src-port 0-65535 dst-port 1672-1672

set service "Puerto_Webmail" protocol tcp src-port 0-65535 dst-port 32000-32000

set service "Pto._OUTLOOK-6001" protocol tcp src-port 0-65535 dst-port 6001-6001

set service "Pto._OUTLOOK-6002" protocol tcp src-port 0-65535 dst-port 6002-6002

set service "Pto._OUTLOOK-6003" protocol tcp src-port 0-65535 dst-port 6003-6003

set service "Pto._OUTLOOK-6004" protocol tcp src-port 0-65535 dst-port 6004-6004

set service "Pto-2500" protocol tcp src-port 0-65535 dst-port 2500-2500

set service "Pto-SIP" protocol udp src-port 0-65535 dst-port 5004-5037

set service "Pto-SIP" + udp src-port 0-65535 dst-port 10001-20000
```

```
set service "Pto-SIP" + udp src-port 0-65535 dst-port 4569-4569

set service "Pto-SIP" + tcp src-port 0-65535 dst-port 800-800

set service "Pto-SIP" + tcp src-port 0-65535 dst-port 22-22

set service "Pto-SIP" + tcp src-port 0-65535 dst-port 80-80

set service "Pto-SIP" + udp src-port 0-65535 dst-port 5039-5082

set service "Pto-5038" protocol tcp src-port 0-65535 dst-port 5038-5038

set service "Pto-5038" + udp src-port 0-65535 dst-port 5038-5038

set service "Pto-5038" + tcp src-port 0-65535 dst-port 3306-3306

set service "Pto-5038" + udp src-port 0-65535 dst-port 3306-3306

set service "stratix" protocol tcp src-port 0-65535 dst-port 1672-1673

set service "stratix" + udp src-port 0-65535 dst-port 1672-1673

set alg applechat enable

unset alg applechat re-assembly enable

set alg sctp enable

set auth-server "Local" id 0

set auth-server "Local" server-name "Local"

set auth default auth server "Local"

set auth radius accounting port 1646

set admin name "AdminSystem"

set admin password "nM32MtrmPgKLc3CMCsHL6KCTsnFyJn"

set admin user "angelvalera" password "nLf/JQrzDXoCcULCus7EqHAtzzOPXn" privilege
'all"
```



```
set admin port 8080

set admin auth web timeout 10

set admin auth server "Local"

set admin format dos

set zone "Trust" vrouter "trust-vr"

set zone "Untrust" vrouter "trust-vr"

set zone "DMZ" vrouter "trust-vr"

set zone "VLAN" vrouter "trust-vr"

set zone id 100 "Dedicado"

set zone "Dedicado" vrouter "untrust-vr"

set zone id 101 "Infinitum"

set zone "Infinitum" vrouter "VR-Infinitum"

set zone "Untrust-Tun" vrouter "trust-vr"

set zone "Trust" tcp-rst

set zone "Untrust" block

unset zone "Untrust" tcp-rst

set zone "MGT" block

unset zone "V1-Trust" tcp-rst

unset zone "V1-Untrust" tcp-rst

set zone "DMZ" tcp-rst

unset zone "V1-DMZ" tcp-rst

unset zone "VLAN" tcp-rst
```

```
unset zone "Dedicado" tcp-rst
unset zone "Infinitum" tcp-rst
set zone "Trust" screen udp-flood
set zone "Trust" screen port-scan
set zone "Trust" screen ip-sweep
set zone "Trust" screen tear-drop
set zone "Trust" screen syn-flood
set zone "Trust" screen ping-death
set zone "Trust" screen icmp-fragment
set zone "Trust" screen icmp-large
set zone "Trust" screen icmp-id
set zone "Trust" screen tcp-sweep
set zone "Trust" screen udp-sweep
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ping-death
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land
set zone "V1-Untrust" screen tear-drop
set zone "V1-Untrust" screen syn-flood
set zone "V1-Untrust" screen ping-death
set zone "V1-Untrust" screen ip-filter-src
```

```
set zone "V1-Untrust" screen land
set zone "DMZ" screen icmp-flood
set zone "DMZ" screen udp-flood
set zone "DMZ" screen port-scan
set zone "DMZ" screen ip-sweep
set zone "DMZ" screen tear-drop
set zone "DMZ" screen syn-flood
set zone "DMZ" screen ip-spoofing
set zone "DMZ" screen ping-death
set zone "DMZ" screen icmp-fragment
set zone "DMZ" screen icmp-large
set zone "DMZ" screen icmp-id
set zone "DMZ" screen tcp-sweep
set zone "DMZ" screen udp-sweep
set interface "ethernet0/0" zone "Trust"
set interface "ethernet0/1" zone "DMZ"
set interface "ethernet0/2" zone "Untrust"
set interface "ethernet0/3" zone "Infinitum"
set interface "ethernet0/4" zone "Dedicado"
set interface "tunnel.1" zone "Dedicado"
set interface "tunnel.2" zone "Dedicado"
set interface "tunnel.3" zone "Dedicado"
```

```
set interface "tunnel.4" zone "Dedicado"
set interface "tunnel.5" zone "Dedicado"
set interface "tunnel.6" zone "Dedicado"
set interface "tunnel.7" zone "Dedicado"
interface "tunnel.8" zone "Dedicado"
set interface "tunnel.9" zone "Dedicado"
set interface "tunnel.10" zone "Dedicado"
set interface "tunnel.11" zone "Dedicado"
set interface "tunnel.12" zone "Dedicado"
set interface "tunnel.13" zone "Dedicado"
set interface "tunnel.14" zone "Infinitum"
set interface "tunnel.15" zone "Infinitum"
set interface ethernet0/0 ip 172.16.1.1/24
set interface ethernet0/0 route
unset interface vlan1 ip
set interface ethernet0/1 ip 192.168.1.1/24
set interface ethernet0/1 route
set interface ethernet0/2 ip 100.100.100.2/24
set interface ethernet0/2 route
set interface ethernet0/3 ip 200.67.204.204/32
set interface ethernet0/3 route
set interface ethernet0/4 ip 201.116.35.115/28
```

```
set interface ethernet0/4 route

set interface tunnel.1 ip unnumbered interface ethernet0/4

set interface tunnel.2 ip unnumbered interface ethernet0/4

set interface tunnel.3 ip unnumbered interface ethernet0/4

set interface tunnel.4 ip unnumbered interface ethernet0/4

set interface tunnel.5 ip unnumbered interface ethernet0/4

set interface tunnel.6 ip unnumbered interface ethernet0/4

set interface tunnel.7 ip unnumbered interface ethernet0/4

set interface tunnel.8 ip unnumbered interface ethernet0/4

set interface tunnel.9 ip unnumbered interface ethernet0/4

set interface tunnel.10 ip unnumbered interface ethernet0/4

set interface tunnel.11 ip unnumbered interface ethernet0/4

set interface tunnel.12 ip unnumbered interface ethernet0/4

set interface tunnel.13 ip unnumbered interface ethernet0/4

set interface tunnel.14 ip unnumbered interface ethernet0/3

set interface tunnel.15 ip unnumbered interface ethernet0/3

unset interface vlan1 bypass-others-ipsec

unset interface vlan1 bypass-non-ip

set interface ethernet0/0 ip manageable

set interface ethernet0/1 ip manageable

set interface ethernet0/2 ip manageable

set interface ethernet0/3 ip manageable
```

```
set interface ethernet0/4 ip manageable
set interface ethernet0/3 manage ping
set interface ethernet0/3 manage ssh
set interface ethernet0/3 manage telnet
set interface ethernet0/3 manage web
set interface ethernet0/4 manage ping
set interface ethernet0/4 manage ssh
set interface ethernet0/4 manage telnet
set interface ethernet0/4 manage web
set interface ethernet0/2 monitor track-ip ip
set interface ethernet0/2 monitor track-ip threshold 3
set interface ethernet0/2 monitor track-ip ip 4.2.2.2
unset interface ethernet0/2 monitor track-ip dynamic
set interface ethernet0/3 monitor track-ip ip
set interface ethernet0/3 monitor track-ip ip 4.2.2.2 interval 2
unset interface ethernet0/3 monitor track-ip dynamic
set interface ethernet0/4 vip interface-ip 80 "HTTP" 192.168.1.10 manual
set interface ethernet0/4 vip interface-ip 25 "MAIL" 192.168.1.19 manual
set interface ethernet0/4 vip interface-ip 53 "DNS" 192.168.1.10 manual
set interface ethernet0/4 vip interface-ip 6001 "Pto._OUTLOOK-6001" 192.168.1.11 manual
set interface ethernet0/4 vip interface-ip 443 "HTTPS" 192.168.1.11 manual
set interface ethernet0/4 vip interface-ip 6002 "Pto._OUTLOOK-6002" 192.168.1.11 manual
```

```
set interface ethernet0/4 vip interface-ip 6003 "Pto._OUTLOOK-6003" 192.168.1.11 manual
set interface ethernet0/4 vip interface-ip 6004 "Pto._OUTLOOK-6004" 192.168.1.11 manual
set interface ethernet0/4 vip interface-ip 3389 "Pto_Escritorio_remoto" 192.168.1.198
manual
set interface ethernet0/3 vip interface-ip 1672 "Pto_Stratix-1672" 192.168.1.12 manual
set interface ethernet0/3 vip interface-ip 1951 "Pto_Visualab-1951" 192.168.1.13 manual
set interface ethernet0/3 vip interface-ip 21 "FTP" 192.168.1.12 manual
set interface ethernet0/3 vip interface-ip 3389 "Pto_Escritorio_remoto" 172.16.1.74 manual
set interface ethernet0/0 dhcp server service
set interface ethernet0/0 dhcp server enable
set interface ethernet0/0 dhcp server option lease 1440000
set interface ethernet0/0 dhcp server option gateway 172.16.1.1
set interface ethernet0/0 dhcp server option netmask 255.255.255.0
set interface ethernet0/0 dhcp server option domainname laboratorioTecapps.com.mx
set interface ethernet0/0 dhcp server option dns1 192.168.1.198
set interface ethernet0/0 dhcp server option dns2 192.168.1.11
set interface ethernet0/0 dhcp server option wins1 192.168.1.198
set interface ethernet0/0 dhcp server ip 172.16.1.17 to 172.16.1.100
unset interface ethernet0/0 dhcp server config next-server-ip
set interface ethernet0/0 dip 4 172.16.1.178 172.16.1.178
set interface ethernet0/0 dip 6 172.16.1.77 172.16.1.77
set interface ethernet0/4 dip 5 201.116.35.113 201.116.35.113
```

set interface "ethernet0/0" mip 172.16.1.170 host 192.168.1.10 netmask 255.255.255.255
vr "trust-vr"

set interface "ethernet0/0" mip 172.16.1.171 host 192.168.1.11 netmask 255.255.255.255
vr "trust-vr"

set interface "ethernet0/0" mip 172.16.1.172 host 192.168.1.12 netmask 255.255.255.255
vr "trust-vr"

set interface "ethernet0/0" mip 172.16.1.173 host 192.168.1.13 netmask 255.255.255.255
vr "trust-vr"

set interface "ethernet0/0" mip 172.16.1.174 host 192.168.1.14 netmask 255.255.255.255
vr "trust-vr"

set interface "ethernet0/0" mip 172.16.1.175 host 192.168.1.15 netmask 255.255.255.255
vr "trust-vr"

set interface "ethernet0/0" mip 172.16.1.176 host 192.168.1.18 netmask 255.255.255.255
vr "trust-vr"

set interface "ethernet0/0" mip 172.16.1.177 host 192.168.1.190 netmask 255.255.255.255
vr "trust-vr"

set interface "ethernet0/0" mip 172.16.1.179 host 192.168.1.172 netmask 255.255.255.255
vr "trust-vr"

set interface "ethernet0/0" mip 172.16.1.180 host 192.168.1.173 netmask 255.255.255.255
vr "trust-vr"

set interface "ethernet0/0" mip 172.16.1.181 host 192.168.1.187 netmask 255.255.255.255
vr "trust-vr"

set interface "ethernet0/0" mip 172.16.1.182 host 192.168.1.162 netmask 255.255.255.255
vr "trust-vr"

set interface "ethernet0/0" mip 172.16.1.183 host 192.168.1.198 netmask 255.255.255.255
vr "trust-vr"


```
set interface "ethernet0/4" mip 201.116.35.117 host 192.168.1.12 netmask
255.255.255.255 vr "trust-vr"

set interface "ethernet0/4" mip 201.116.35.114 host 192.168.1.13 netmask
255.255.255.255 vr "trust-vr"

set interface "ethernet0/4" mip 201.116.35.118 host 192.168.1.15 netmask
255.255.255.255 vr "trust-vr"

set interface "ethernet0/4" mip 201.116.35.116 host 192.168.1.187 netmask
255.255.255.255 vr "trust-vr"

set interface "ethernet0/4" mip 201.116.35.119 host 192.168.1.16 netmask
255.255.255.255 vr "trust-vr"

set interface "ethernet0/4" mip 201.116.35.120 host 192.168.1.19 netmask
255.255.255.255 vr "trust-vr"

set interface "ethernet0/4" mip 201.116.35.121 host 172.16.1.90 netmask 255.255.255.255
vr "trust-vr"

set interface ethernet0/2 monitor interface ethernet0/3 weight 2

set interface ethernet0/2 monitor interface ethernet0/4 weight 3

set interface ethernet0/3 monitor interface ethernet0/2 weight 2

set interface ethernet0/3 monitor interface ethernet0/4 weight 3

set interface ethernet0/2 monitor zone "Dedicado" weight 3

set interface ethernet0/2 monitor zone "Infinitum" weight 2

set interface ethernet0/3 monitor zone "Untrust" weight 2

set interface ethernet0/3 monitor zone "Dedicado" weight 3

set flow all-tcp-mss 1304

unset flow no-tcp-seq-check
```

```
set flow tcp-syn-check

unset flow tcp-syn-bit-check

set flow reverse-route clear-text prefer

set flow reverse-route tunnel always

set domain laboratorioTecapps.com.mx

set hostname SSG140-Tecapps

set pki authority default scep mode "auto"

set pki x509 default cert-path partial

set dns host dns1 192.168.1.198 src-interface ethernet0/1

set dns host dns2 192.168.1.11 src-interface ethernet0/1

set dns host dns3 4.2.2.2

set dns host schedule 07:00 interval 4

set address "Trust" "0.0.0.0/0" 0.0.0.0 0.0.0.0

set address "Trust" "10.30.30.0/24" 10.30.30.0 255.255.255.0

set address "Trust" "172.16.0.0/16" 172.16.0.0 255.255.0.0

set address "Trust" "172.16.1.13/32" 172.16.1.13 255.255.255.255

set address "Trust" "172.16.1.135/32" 172.16.1.135 255.255.255.255

set address "Trust" "172.16.1.137/32" 172.16.1.137 255.255.255.255

set address "Trust" "172.16.1.14/32" 172.16.1.14 255.255.255.255

set address "Trust" "172.16.1.15/32" 172.16.1.15 255.255.255.255

set address "Trust" "172.16.1.7/32" 172.16.1.7 255.255.255.255

set address "Trust" "172.16.1.77/32" 172.16.1.77 255.255.255.255
```

set address "Trust" "192.168.125.0/24" 192.168.125.0 255.255.255.0

set address "Trust" "192.168.125.13/32" 192.168.125.14 255.255.255.255

set address "Trust" "Administrador" JNRCORP042.laboratorioTecapps.com.mx

set address "Trust" "Adriana Icelo" 172.16.1.4 255.255.255.255

set address "Trust" "Angel Valera" 172.16.1.8 255.255.255.255

set address "Trust" "ASISTGERENCIA" JNRCORP015.laboratorioTecapps.com.mx

set address "Trust" "AUDITORIA" JNRCORP004.laboratorioTecapps.com.mx

set address "Trust" "AUXILIAR" JNRCORP016.laboratorioTecapps.com.mx

set address "Trust" "BAN01" JNRCORP010.laboratorioTecapps.com.mx

set address "Trust" "BANCOS" JNRCORP033.laboratorioTecapps.com.mx

set address "Trust" "Call Center" 172.16.1.6 255.255.255.255

set address "Trust" "CALLCENTER3" JNRCORP018.laboratorioTecapps.com.mx

set address "Trust" "callcenter4" JNRCORP037.laboratorioTecapps.com.mx

set address "Trust" "CALLCENTERII" JNRCORP025.laboratorioTecapps.com.mx

set address "Trust" "CALLCENTERIII" JNRCORP023.laboratorioTecapps.com.mx

set address "Trust" "CAP02" JNRCORP040.laboratorioTecapps.com.mx

set address "Trust" "CCVT" JNRCORP008.laboratorioTecapps.com.mx

set address "Trust" "COMPRAS" JNRCORP029.laboratorioTecapps.com.mx

set address "Trust" "CONTA0102" JNRCORP005.laboratorioTecapps.com.mx

set address "Trust" "CONTABILIDAD" JNRCORP022.laboratorioTecapps.com.mx

set address "Trust" "CORP12" JNRCORP024.laboratorioTecapps.com.mx

set address "Trust" "DESARROLLO" JNRCORP013.laboratorioTecapps.com.mx

set address "Trust" "DH" 172.16.1.12 255.255.255.255

set address "Trust" "DH2" JNRCORP009.laboratorioTecapps.com.mx

set address "Trust" "DH3" JNRCORP035.laboratorioTecapps.com.mx

set address "Trust" "DIRECCION" JNRCORP001.laboratorioTecapps.com.mx

set address "Trust" "Dra Ana Sainez" 172.16.1.2 255.255.255.255

set address "Trust" "FACTURACION" JNRCORP011.laboratorioTecapps.com.mx

set address "Trust" "Fernando Ramirez" 172.16.1.5 255.255.255.255

set address "Trust" "FTP" JNRCORP007.laboratorioTecapps.com.mx

set address "Trust" "Gerardo Herrera" 172.16.1.12 255.255.255.255

set address "Trust" "HERRERA" JNRCORP014.laboratorioTecapps.com.mx

set address "Trust" "Jesus Ramirez" 172.16.1.9 255.255.255.255

set address "Trust" "JNRCORP038" JNRCORP038.laboratorioTecapps.com.mx

set address "Trust" "Mac" 172.16.1.105 255.255.255.255

set address "Trust" "MARISOL" JNRCORP036.laboratorioTecapps.com.mx

set address "Trust" "MKT" JNRCORP039.laboratorioTecapps.com.mx

set address "Trust" "MOVIL" JNRCORP021.laboratorioTecapps.com.mx

set address "Trust" "OPERACIONES" JNRCORP026.laboratorioTecapps.com.mx

set address "Trust" "OPERASISTENT" JNRCORP017.laboratorioTecapps.com.mx

set address "Trust" "PROMOCION" JNRCORP034.laboratorioTecapps.com.mx

set address "Trust" "prueba" JNRCORP043.laboratorioTecapps.com.mx

set address "Trust" "Raul Aguilar" 172.16.1.7 255.255.255.255

set address "Trust" "Red_Tecapps" 172.16.1.0 255.255.255.0

```
set address "Trust" "Red_Wireless" 172.16.1.128 255.255.255.240
set address "Trust" "SALA" JNRCORP027.laboratorioTecapps.com.mx
set address "Trust" "Sala de Juntas" 172.16.1.10 255.255.255.255
set address "Trust" "Salvador Vanegas" 172.16.1.3 255.255.255.255
set address "Trust" "SINCAL" JNRCORP006.laboratorioTecapps.com.mx
set address "Trust" "SIS0101" JNRCORP020.laboratorioTecapps.com.mx
set address "Trust" "SIS0102" JNRCORP019.laboratorioTecapps.com.mx
set address "Trust" "SISTEMAS001" JNRCORP002.laboratorioTecapps.com.mx
set address "Trust" "SISTEMASMARIO" JNRCORP030.laboratorioTecapps.com.mx
set address "Trust" "TRAMITES" JNRCORP032.laboratorioTecapps.com.mx
set address "Trust" "VENTAS" JNRCORP031.laboratorioTecapps.com.mx
set address "Trust" "Veronica Aguirre" 172.16.1.11 255.255.255.255
set address "Trust" "Wireless-129" 172.16.1.129 255.255.255.255
set address "Trust" "Wireless-130" 172.16.1.130 255.255.255.255
set address "Trust" "Wireless-131" 172.16.1.131 255.255.255.255
set address "Trust" "Wireless-132" 172.16.1.132 255.255.255.255
set address "Trust" "Wireless-133" 172.16.1.133 255.255.255.255
set address "Trust" "Wireless-134" 172.16.1.134 255.255.255.255
set address "Trust" "Wireless-135" 172.16.1.135 255.255.255.255
set address "Trust" "Wireless-136" 172.16.1.136 255.255.255.255
set address "Untrust" "224.0.0.1/32" 224.0.0.1 255.255.255.255
set address "Untrust" "65.55.13.91/32" 65.55.13.91 255.255.255.255
```

```
set address "DMZ" "192.168.1.15/32" 192.168.1.15 255.255.255.255
set address "DMZ" "192.168.1.16/32" 192.168.1.16 255.255.255.255
set address "DMZ" "192.168.1.19/32" 192.168.1.19 255.255.255.255
set address "DMZ" "192.168.1.198/32" 192.168.1.198 255.255.255.255
set address "DMZ" "192.168.1.20/32" 192.168.1.20 255.255.255.255
set address "DMZ" "Active_Directory" 192.168.1.198 255.255.255.255
set address "DMZ" "Exchange" 192.168.1.11 255.255.255.255
set address "DMZ" "FTP_Aspel" 192.168.1.18 255.255.255.255
set address "DMZ" "Red_DMZ" 192.168.1.0 255.255.255.0
set address "DMZ" "Red_Secure Access" 10.200.200.0 255.255.255.0
set address "DMZ" "Stratix" 192.168.1.12 255.255.255.255
set address "DMZ" "Visualab" 192.168.1.13 255.255.255.255
set address "DMZ" "Web" 192.168.1.10 255.255.255.255
set address "Dedicado" "172.16.106.10/32" 172.16.106.10 255.255.255.255
set address "Dedicado" "172.16.117.0/24" 172.16.117.0 255.255.255.0
set address "Dedicado" "172.16.117.11/32" 172.16.117.11 255.255.255.255
set address "Dedicado" "172.16.150.0/24" 172.16.150.0 255.255.255.0
set address "Dedicado" "224.0.0.1/32" 224.0.0.1 255.255.255.255
set address "Dedicado" "65.55.13.91/32" 65.55.13.91 255.255.255.255
set address "Dedicado" "correo_de_salida" 201.116.35.115 255.255.255.255
set address "Dedicado" "Sucursal_AvMexico" 172.16.123.0 255.255.255.0
set address "Dedicado" "Sucursal_AvMexico-lab" 172.16.100.0 255.255.255.0
```

```
set address "Dedicado" "Sucursal_Chicoloapan" 172.16.117.0 255.255.255.0
set address "Dedicado" "Sucursal_Coyoacan" 172.16.106.0 255.255.255.0
set address "Dedicado" "Sucursal_Culhuacan" 172.16.105.0 255.255.255.0
set address "Dedicado" "Sucursal_Ermita" 172.16.107.0 255.255.255.0
set address "Dedicado" "Sucursal_Estadio" 172.16.101.0 255.255.255.0
set address "Dedicado" "Sucursal_Sur16" 172.16.116.0 255.255.255.0
set address "Dedicado" "Sucursal_Tepozanes" 172.16.102.0 255.255.255.0
set address "Dedicado" "Sucursal_Tezonco" 172.16.104.0 255.255.255.0
set address "Dedicado" "Sucursal_Tulyehualco" 172.16.103.0 255.255.255.0
set address "Dedicado" "Sucursal_Viaducto" 172.16.125.0 255.255.255.0
set address "Dedicado" "Sucursal_Voca7" 172.16.121.0 255.255.255.0
set address "Dedicado" "Sucursal_Xochimilco" 172.16.114.0 255.255.255.0
set address "Infinitum" "10.30.30.0/24" 10.30.30.0 255.255.255.0
set address "Infinitum" "10.30.30.7/32" 10.30.30.7 255.255.255.255
set address "Infinitum" "10.30.30.8/32" 10.30.30.8 255.255.255.255
set address "Infinitum" "192.168.1.0/26" 192.168.1.0 255.255.255.192
set address "Infinitum" "192.168.1.145" 192.168.1.145 255.255.255.240
set address "Infinitum" "224.0.0.1/32" 224.0.0.1 255.255.255.255
set group address "Trust" "Grupo_AccesoTotal"
set group address "Trust" "Grupo_AccesoTotal" add "172.16.1.13/32"
set group address "Trust" "Grupo_AccesoTotal" add "172.16.1.14/32"
set group address "Trust" "Grupo_AccesoTotal" add "172.16.1.15/32"
```

```
set group address "Trust" "Grupo_AccesoTotal" add "Adriana Icelo"  
set group address "Trust" "Grupo_AccesoTotal" add "Angel Valera"  
set group address "Trust" "Grupo_AccesoTotal" add "Call Center"  
set group address "Trust" "Grupo_AccesoTotal" add "Dra Ana Sainez"  
set group address "Trust" "Grupo_AccesoTotal" add "Fernando Ramirez"  
set group address "Trust" "Grupo_AccesoTotal" add "Gerardo Herrera"  
set group address "Trust" "Grupo_AccesoTotal" add "Jesus Ramirez"  
set group address "Trust" "Grupo_AccesoTotal" add "Raul Aguilar"  
set group address "Trust" "Grupo_AccesoTotal" add "Sala de Juntas"  
set group address "Trust" "Grupo_AccesoTotal" add "Salvador Vanegas"  
set group address "Trust" "Grupo_AccesoTotal" add "Veronica Aguirre"  
set user "framirez" uid 2  
set user "framirez" ike-id u-fqdn "framirez@laboratorioTecapps.com.mx" share-limit 1  
set user "framirez" type ike  
set user "framirez" "enable"  
set user "gherrera" uid 5  
set user "gherrera" ike-id u-fqdn "gherrera@laboratorioTecapps.com.mx" share-limit 1  
set user "gherrera" type ike  
set user "gherrera" "enable"  
user "juniper" uid 6  
set user "juniper" ike-id u-fqdn "juniper@laboratorioTecapps.com.mx" share-limit 1  
set user "juniper" type ike
```



```
set user "juniper" "enable"

set user "mromero" uid 4

set user "mromero" ike-id u-fqdn "mromero@laboratorioTecapps.com.mx" share-limit 1

set user "mromero" type ike

set user "mromero" "enable"

set user-group "Usuario-Remotos" id 1

set user-group "Usuario-Remotos" user "framirez"

set user-group "Usuario-Remotos" user "gherrera"

set user-group "Usuario-Remotos" user "juniper"

set user-group "Usuario-Remotos" user "mromero"

set crypto-policy

exit

set ike gateway "Gw-Viaducto" address 0.0.0.0 id "sucursalviaducto" Aggr outgoing-
interface "ethernet0/4".

preshare      "gGcQQecWNcXMumsnPnCtZP9kFanpiRr2qG/e4g3tTz8Mjicq7PGMJzs="
proposal "pre-g2-3des-sha".

unset ike gateway "Gw-Viaducto" nat-traversal

set ike gateway "Gw-Estadio" address 0.0.0.0 id "sucestadio" Aggr outgoing-interface
"ethernet0/4"                                preshare
"JEaTZU3CNKGXCPsKVNCqHGCpZFnSmNBcZEVpQDwVeiQy5di/uxP4ml=" proposal
"pre-g2-3des-sha".

unset ike gateway "Gw-Estadio" nat-traversal udp-checksum

set ike gateway "Gw-Estadio" nat-traversal keepalive-frequency 0
```

```
set ike gateway "Gw-Chicoloapan" address 0.0.0.0 id "succhicoloapan" Aggr outgoing-  
interface "ethernet0/4" preshare  
"FjF4gH+jNlxLWEs5l0C76rrb0anlyPTjkF8EzHJ4A34/6zEpDWePKH0=" proposal "pre-g2-  
3des-sha".
```

```
set ike gateway "Gw-Chicoloapan" nat-traversal udp-checksum
```

```
set ike gateway "Gw-Chicoloapan" nat-traversal keepalive-frequency 0
```

```
set ike gateway "Gw-Tepozanes" address 0.0.0.0 id "suc-tepozanes" Aggr outgoing-interface  
"ethernet0/4" preshare  
"zPtA3e+qNQ2uBpsQ2DCK/dlCWgnXWnJXR3YJbabpQokIn0NBWMvow48=" proposal  
"pre-g2-3des-sha".
```

```
unset ike gateway "Gw-Tepozanes" nat-traversal
```

```
set ike gateway "Gw-Tezonco" address 0.0.0.0 id "suc-tezonco" Aggr outgoing-interface  
"ethernet0/4" preshare  
"C+bdvO9MNVtJBms0MuC2u+YVlrrnzHmTHUWbf7i//HPZwuJxnGnjeOc=" proposal "pre-  
g2-3des-sha".
```

```
unset ike gateway "Gw-Tezonco" nat-traversal
```

```
set ike gateway "Gw-Coyoacan" address 0.0.0.0 id "succoyoacan" Aggr outgoing-interface  
"ethernet0/4" preshare  
"cU5L2yFWN9SRr2sqjRCTctuYULnkmAH9lQHssYQDoDO3lAThsrFkCxl=" proposal "pre-  
g1-des-sha".
```

```
set ike gateway "Gw-Coyoacan" nat-traversal udp-checksum.
```

```
set ike gateway "Gw-Coyoacan" nat-traversal keepalive-frequency 0.
```

```
set ike gateway "Gw-Ermita" address 0.0.0.0 id "suc-ermita" Aggr outgoing-interface  
"ethernet0/4" preshare  
"asKiptV5NzitWZsZUVC4DCRUIGnx1/6QkePAhkOKOOXJIMK8OFU77ss=" proposal "pre-  
g2-3des-sha".
```

```
set ike gateway "Gw-Ermita" nat-traversal udp-checksum.
```

set ike gateway "Gw-Ermita" nat-traversal keepalive-frequency 0.

set ike gateway "Gw-Voca7" address 0.0.0.0 id "sucvoca7" Aggr outgoing-interface "ethernet0/4" preshare "qytoPYRtNLR4AsszfyCNfA+l34nYaa4pYKpJ7yz2rNiGfdAJ1tZX/qQ=" proposal "pre-g2-3des-sha".

unset ike gateway "Gw-Voca7" nat-traversal.

set ike gateway "Gw-Xochimilco" address 0.0.0.0 id "sucxochimilco" Aggr outgoing-interface "ethernet0/4" preshare "tj5hRQ3vNLcdo/sAy3C8ML0AYbnAqydiB8yZWh92YgnM4A5fbafj3Ps=" proposal "pre-g2-3des-sha".

unset ike gateway "Gw-Xochimilco" nat-traversal udp-checksum.

set ike gateway "Gw-Xochimilco" nat-traversal keepalive-frequency 0.

set ike gateway "Gw-Sur16" address 0.0.0.0 id "sucusur16" Aggr outgoing-interface "ethernet0/4" preshare "xV7NTknQNFq0m3sjLiC71+/PA0nwPui2wXFreZ//u8snqGxIVp9hW/s=" proposal "pre-g2-3des-sha".

set ike gateway "Gw-Sur16" nat-traversal udp-checksum.

set ike gateway "Gw-Sur16" nat-traversal keepalive-frequency 0.

set ike gateway "Gw-Culhuacan" address 0.0.0.0 id "sucocatepec" Aggr outgoing-interface "ethernet0/4" preshare

"LRxP756pNOViv8sngqC1rIVLafnJtoFVg8x/UL46ZpRhGVk+514SDH4=" proposal "pre-g2-3des-sha"

set ike gateway "Gw-Culhuacan" nat-traversal udp-checksum

set ike gateway "Gw-Culhuacan" nat-traversal keepalive-frequency 0

set ike gateway "Gw-Suc" address 200.67.250.192 Main outgoing-interface "ethernet0/3" preshare

```
"5H+f9vbINJ51MtsDEvCj8M9DYFnHqcaJ9g==" proposal "pre-g2-3des-sha"

set ike gateway "Cliente-Juniper" dialup "Usuario-Remotos" Aggr outgoing-interface
"ethernet0/4" preshare

"qR4CUkkNN4FVIHs+zLCgrrQdRani3UoGCQ==" proposal "pre-g2-3des-sha"

set ike gateway "Cliente-Juniper" nat-traversal udp-checksum

set ike gateway "Cliente-Juniper" nat-traversal keepalive-frequency 0

set ike gateway "GW-corporativo" address 0.0.0.0 id "sucpatito" Aggr outgoing-interface
"ethernet0/4" preshare

"sbkzJpkDNUofdrsvVCbi3o+5Inx/QJR7g==" proposal "pre-g2-3des-sha"

unset ike gateway "GW-corporativo" nat-traversal

set ike gateway "GW-Tulyehualco" address 0.0.0.0 id "suctulyehualco" Aggr outgoing-
interface "ethernet0/4"

preshare      "tVyvmM6SNf7D+OsiqtCF3UjvL0nKeBvmWkBNa3HVmnhroSYj6vZOZMU="
proposal "pre-g2-3des-sha"

set ike gateway "GW-Tulyehualco" nat-traversal udp-checksum

set ike gateway "GW-Tulyehualco" nat-traversal keepalive-frequency 5

set ike gateway "GW-Mexico-Infinitum" address 0.0.0.0 id "avmexico" Aggr outgoing-
interface "ethernet0/3"

preshare      "LVVtZ5C2NeKplgsJVcC3xUx0mqnHILJU1g/Jfcz30HPV35WKgi7GhNA="
proposal "pre-g2-3des-sha"

set ike gateway "GW-Mexico-Infinitum" nat-traversal udp-checksum

set ike gateway "GW-Mexico-Infinitum" nat-traversal keepalive-frequency 5

set ike gateway "GW-AV_Mexico" address 201.116.65.226 Main outgoing-interface
"ethernet0/4" preshare
```

"m7LFJUU/NWTi7AsQQPCpIUvgWAnUvS9urgVO9GDBytisYEindPwHL5Y=" proposal
"pre-g2-3des-sha"

set ike respond-bad-spi 1

set ike gateway "Gw-Viaducto" heartbeat hello 5

set ike gateway "Gw-Viaducto" heartbeat reconnect 60

set ike gateway "Gw-Estadio" heartbeat hello 5

set ike gateway "Gw-Estadio" heartbeat reconnect 60

set ike gateway "Gw-Chicoloapan" heartbeat hello 5

set ike gateway "Gw-Chicoloapan" heartbeat reconnect 60

set ike gateway "Gw-Tepozanes" heartbeat hello 5

set ike gateway "Gw-Tepozanes" heartbeat reconnect 60

set ike gateway "Gw-Tezonco" heartbeat hello 5

set ike gateway "Gw-Tezonco" heartbeat reconnect 60

set ike gateway "Gw-Coyoacan" heartbeat hello 5

set ike gateway "Gw-Coyoacan" heartbeat reconnect 60

set ike gateway "Gw-Ermita" heartbeat hello 5

set ike gateway "Gw-Ermita" heartbeat reconnect 60

set ike gateway "Gw-Voca7" heartbeat hello 5

set ike gateway "Gw-Voca7" heartbeat reconnect 60

set ike gateway "Gw-Xochimilco" heartbeat hello 5

set ike gateway "Gw-Xochimilco" heartbeat reconnect 60

set ike gateway "Gw-Sur16" heartbeat hello 5

```
set ike gateway "Gw-Sur16" heartbeat reconnect 60
set ike gateway "Gw-Culhuacan" heartbeat hello 5
set ike gateway "Gw-Culhuacan" heartbeat reconnect 60
set ike gateway "Gw-Suc" heartbeat hello 5
set ike gateway "Gw-Suc" heartbeat reconnect 60
set ike gateway "GW-Tulyehualco" heartbeat hello 5
set ike gateway "GW-Tulyehualco" heartbeat reconnect 60
set ike gateway "GW-Mexico-Infinitem" heartbeat hello 5
set ike gateway "GW-Mexico-Infinitem" heartbeat reconnect 60
set ike gateway "GW-AV_Mexico" heartbeat hello 5
set ike gateway "GW-AV_Mexico" heartbeat reconnect 60
set ike ikev2 ike-sa-soft-lifetime 60
unset ike ikeid-enumeration
unset ike dos-protection
unset ipsec access-session enable
set ipsec access-session maximum 5000
set ipsec access-session upper-threshold 0
set ipsec access-session lower-threshold 0
set ipsec access-session dead-p2-sa-timeout 0
unset ipsec access-session log-error
unset ipsec access-session info-exch-connected
unset ipsec access-session use-error-log
```

```
set vpn "VPN-Viaducto" gateway "Gw-Viaducto" replay tunnel idletime 0 proposal "g2-esp-3des-sha"
```

```
set vpn "VPN-Viaducto" monitor
```

```
set vpn "VPN-Viaducto" id 0x1 bind interface tunnel.1
```

```
set vpn "VPN-Estadio" gateway "Gw-Estadio" replay tunnel idletime 0 proposal "g2-esp-3des-sha"
```

```
set vpn "VPN-Estadio" monitor
```

```
set vpn "VPN-Estadio" id 0x2 bind interface tunnel.2
```

```
set vpn "VPN-Chicoloapan" gateway "Gw-Chicoloapan" replay tunnel idletime 0 proposal "g2-esp-3des-sha"
```

```
set vpn "VPN-Chicoloapan" monitor
```

```
set vpn "VPN-Chicoloapan" id 0xd bind interface tunnel.13
```

```
set vpn "VPN-Tepozanes" gateway "Gw-Tepozanes" replay tunnel idletime 0 proposal "g2-esp-3des-sha"
```

```
set vpn "VPN-Tepozanes" id 0xe bind interface tunnel.3
```

```
set vpn "VPN-Tezonco" gateway "Gw-Tezonco" replay tunnel idletime 0 proposal "g2-esp-3des-sha"
```

```
set vpn "VPN-Tezonco" monitor
```

```
set vpn "VPN-Tezonco" id 0xf bind interface tunnel.5
```

```
set vpn "VPN-Coyoacan" gateway "Gw-Coyoacan" replay tunnel idletime 0 proposal "g2-esp-des-sha"
```

```
set vpn "VPN-Coyoacan" monitor
```

```
set vpn "VPN-Coyoacan" id 0x17 bind interface tunnel.6
```

```
set vpn "VPN-Ermita" gateway "Gw-Ermita" replay tunnel idletime 0 proposal "g2-esp-3des-sha"
```

```
set vpn "VPN-Ermita" monitor
```

```
set vpn "VPN-Ermita" id 0x11 bind interface tunnel.7
```

```
set vpn "VPN-Voca7" gateway "Gw-Voca7" replay tunnel idletime 0 proposal "g2-esp-3des-sha"
```

```
set vpn "VPN-Voca7" monitor
```

```
set vpn "VPN-Voca7" id 0x32 bind interface tunnel.11
```

```
set vpn "VPN-Xochimilco" gateway "Gw-Xochimilco" replay tunnel idletime 0 proposal "g2-esp-3des-sha"
```

```
set vpn "VPN-Xochimilco" monitor
```

```
set vpn "VPN-Xochimilco" id 0x13 bind interface tunnel.9
```

```
set vpn "VPN-Sur16" gateway "Gw-Sur16" replay tunnel idletime 0 proposal "g2-esp-3des-sha"
```

```
set vpn "VPN-Sur16" monitor
```

```
set vpn "VPN-Sur16" id 0x14 bind interface tunnel.10
```

```
set vpn "VPN-Culhuacan" gateway "Gw-Culhuacan" replay tunnel idletime 0 proposal "g2-esp-3des-sha"
```

```
set vpn "VPN-Culhuacan" monitor
```

```
set vpn "VPN-Culhuacan" id 0x15 bind interface tunnel.8
```

```
set vpn "VPN-Suc" gateway "Gw-Suc" no-replay tunnel idletime 0 proposal "g2-esp-3des-sha"
```

```
set vpn "VPN-Suc" monitor
```

```
set vpn "VPN-Suc" id 0x16 bind interface tunnel.14
```



```
set vpn "VPN-Cliente_juniper" gateway "Cliente-Juniper" replay tunnel idletime 0 proposal
"g2-esp-3des-sha"

set vpn "VPN-Cliente_juniper" monitor

set vpn "VPN-Tulyehualco" gateway "GW-Tulyehualco" replay tunnel idletime 0 proposal
"g2-esp-3des-sha"

set vpn "VPN-Tulyehualco" monitor

set vpn "VPN-Tulyehualco" id 0x33 bind interface tunnel.4

set vpn "VPN-Mexico-Infinitum" gateway "GW-Mexico-Infinitum" replay tunnel idletime 0
proposal "g2-esp-3des-sha"

set vpn "VPN-Mexico-Infinitum" monitor

set vpn "VPN-Mexico-Infinitum" id 0x34 bind interface tunnel.15

set vpn "VPN_AvMexico" gateway "GW-AV_Mexico" replay tunnel idletime 0 proposal "g2-
esp-3des-sha"

set vpn "VPN_AvMexico" monitor

set vpn "VPN_AvMexico" id 0x35 bind interface tunnel.12

set vrouter "untrust-vr"

exit

set vrouter "trust-vr"

exit

set vrouter "VR-Infinitum"

exit

set attack db server "https://services.netscreen.com/restricted/sigupdates"

set av all fail-mode traffic permit
```

set av mime-list "Blok-mime" "audio;/video"

set av profile "AV-Tecapps"

set http decompress-layer 5

unset http skipmime mime-list

unset http skipmime mime-list

unset imap enable

unset pop3 enable

unset smtp enable

set aim-icq decompress-layer 5

set msnms decompress-layer 5

set ymsg decompress-layer 5

exit

set av profile "Av-Tecapps_Mortales"

set ftp decompress-layer 4

set http decompress-layer 5

unset http skipmime mime-list

set http skipmimemime-list "Blok-mime"

unset imap enable

unset pop3 enable

unset smtp enable

set aim-icq decompress-layer 5

exit

```
unset av scan-mgr max-content-size drop

unset av scan-mgr decompress-layer drop

unset av scan-mgr timeout drop

set url protocol type sc-cpa

set url protocol sc-cpa

set category "Paginas Permitidas" url "www.actinseguro.com/"

set category "Paginas_Bloqueadas" url "a.rad.msn.com/"

set category "Paginas_Bloqueadas" url "alfa913.mx/grc/gral.nsf/vwradio/esta-4z8tzb"

set category "Paginas_Bloqueadas" url "b.rad.msn.com/"

set category "Paginas_Bloqueadas" url "h.msn.com/"

set category "Paginas_Bloqueadas" url "rad.msn.com/"

set category "Paginas_Bloqueadas" url "radiocentro.com.mx/"

set category "Paginas_Bloqueadas" url "radiocentro.com.mx/estaciones"

set category "Paginas_Bloqueadas" url "www.alfa913.mx/"

set category "Paginas_Bloqueadas" url "www.alfaradio.com.mx/"

set category "Paginas_Bloqueadas" url "www.jetcast.com/em-popup-esplayer.phtml"

set category "Paginas_Bloqueadas" url "www.radiosintoniza.net/radio-alfa-radio-91.3-
fm_159.aspx"

set profile "Filtrado_Tecapps" "Paginas Permitidas" permit

set profile "Filtrado_Tecapps" "Paginas_Bloqueadas" block

set profile "Filtrado_Tecapps" "Adult/Sexually Explicit" block

set profile "Filtrado_Tecapps" "Advertisements" permit
```

set profile "Filtrado_Tecapps" "Arts & Entertainment" block

set profile "Filtrado_Tecapps" "Chat" block

set profile "Filtrado_Tecapps" "Computing & Internet" permit

set profile "Filtrado_Tecapps" "Criminal Skills" block

set profile "Filtrado_Tecapps" "Drugs, Alcohol & Tobacco" permit

set profile "Filtrado_Tecapps" "Education" permit

set profile "Filtrado_Tecapps" "Finance & Investment" permit

set profile "Filtrado_Tecapps" "Food & Drink" permit

set profile "Filtrado_Tecapps" "Gambling" permit

set profile "Filtrado_Tecapps" "Games" block

set profile "Filtrado_Tecapps" "Glamour & Intimate Apparel" permit

set profile "Filtrado_Tecapps" "Government & Politics" permit

set profile "Filtrado_Tecapps" "Hacking" block

set profile "Filtrado_Tecapps" "Hate Speech" permit

set profile "Filtrado_Tecapps" "Health & Medicine" permit

set profile "Filtrado_Tecapps" "Hobbies & Recreation" permit

set profile "Filtrado_Tecapps" "Hosting Sites" permit

set profile "Filtrado_Tecapps" "Job Search & Career Development" permit

set profile "Filtrado_Tecapps" "Kids Sites" permit

set profile "Filtrado_Tecapps" "Lifestyle & Culture" permit

set profile "Filtrado_Tecapps" "Motor Vehicles" permit

set profile "Filtrado_Tecapps" "News" permit

```
set profile "Filtrado_Tecapps" "Personals & Dating" block
set profile "Filtrado_Tecapps" "Photo Searches" permit
set profile "Filtrado_Tecapps" "Real Estate" permit
set profile "Filtrado_Tecapps" "Reference" permit
set profile "Filtrado_Tecapps" "Religion" permit
set profile "Filtrado_Tecapps" "Remote Proxies" block
set profile "Filtrado_Tecapps" "Search Engines" permit
set profile "Filtrado_Tecapps" "Sex Education" permit
set profile "Filtrado_Tecapps" "Shopping" permit
set profile "Filtrado_Tecapps" "Sports" block
set profile "Filtrado_Tecapps" "Streaming Media" block
set profile "Filtrado_Tecapps" "Travel" permit
set profile "Filtrado_Tecapps" "Usenet News" permit
set profile "Filtrado_Tecapps" "Violence" permit
set profile "Filtrado_Tecapps" "Weapons" permit
set profile "Filtrado_Tecapps" "Web-based Email" permit

set enable

set deny-message "Esta Pagina ha sido bloqueada de acuerdo a las politicas de seguridad
de Tecapps

$URL_CATEGORY"

exit

set vpn "VPN-Viaducto" proxy-id local-ip 172.16.1.0/24 remote-ip 172.16.125.0/24 "ANY"
```

```
set vpn "VPN-Estadio" proxy-id local-ip 172.16.1.0/24 remote-ip 172.16.101.0/24 "ANY"

set vpn "VPN-Chicoloapan" proxy-id local-ip 172.16.1.0/24 remote-ip 172.16.117.0/24
"ANY"

set vpn "VPN-Tepozanes" proxy-id local-ip 172.16.1.0/24 remote-ip 172.16.102.0/24 "ANY"

set vpn "VPN-Tezonco" proxy-id local-ip 172.16.1.0/24 remote-ip 172.16.104.0/24 "ANY"

set vpn "VPN-Coyoacan" proxy-id local-ip 172.16.1.0/24 remote-ip 172.16.106.0/24 "ANY"

set vpn "VPN-Ermita" proxy-id local-ip 172.16.1.0/24 remote-ip 172.16.107.0/24 "ANY"

set vpn "VPN-Voca7" proxy-id local-ip 172.16.1.0/24 remote-ip 172.16.121.0/24 "ANY"

set vpn "VPN-Xochimilco" proxy-id local-ip 172.16.1.0/24 remote-ip 172.16.114.0/24 "ANY"

set vpn "VPN-Sur16" proxy-id local-ip 172.16.1.0/24 remote-ip 172.16.116.0/24 "ANY"

set vpn "VPN-Culhuacan" proxy-id local-ip 172.16.1.0/24 remote-ip 172.16.105.0/24 "ANY"

set vpn "VPN-Suc" proxy-id local-ip 172.16.1.0/24 remote-ip 10.30.30.0/24 "ANY"

set vpn "VPN-Tulyehualco" proxy-id local-ip 172.16.1.0/24 remote-ip 172.16.103.0/24 "ANY"

set vpn "VPN-Mexico-Infinitem" proxy-id local-ip 172.16.1.0/24 remote-ip 172.16.123.0/24
"ANY"

set vpn "VPN_AvMexico" proxy-id local-ip 172.16.1.0/24 remote-ip 172.16.123.0/24 "ANY"

set policy id 147 from "DMZ" to "Untrust" "192.168.1.198/32" "65.55.13.91/32" "ANY" nat src
permit log

set policy id 147

exit

set policy id 12 from "Trust" to "DMZ" "Red_Tecapps" "Red_DMZ" "ANY" permit log

set policy id 12

set src-address "Red_Wireless"
```

```
set dst-address "Red_Secure Access"
```

```
exit
```

```
set policy id 132 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.176)" "ANY" permit  
log
```

```
set policy id 132
```

```
exit
```

```
set policy id 139 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.182)" "ANY" permit  
log
```

```
set policy id 139
```

```
exit
```

```
set policy id 138 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.181)" "ANY" permit  
log
```

```
set policy id 138
```

```
exit
```

```
set policy id 137 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.180)" "ANY" permit  
log
```

```
set policy id 137
```

```
exit
```

```
et policy id 136 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.179)" "ANY" permit  
log
```

```
set policy id 136
```

```
exit
```

```
set policy id 133 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.177)" "ANY" permit  
log
```

set policy id 133

exit

set policy id 134 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.176)" "ANY" permit
log

set policy id 134

exit

set policy id 131 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.175)" "ANY" permit
log

set policy id 131

exit

set policy id 130 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.174)" "ANY" permit
log

set policy id 130

exit

set policy id 129 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.173)" "ANY" permit
log

set policy id 129

exit

set policy id 128 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.172)" "ANY" permit
log

set policy id 128

exit

set policy id 127 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.171)" "ANY" permit
log

set policy id 127

exit

set policy id 126 from "Trust" to "DMZ" "172.16.1.77/32" "MIP(172.16.1.170)" "ANY" permit
log

set policy id 126

exit

set policy id 124 from "Dedicado" to "Trust" "Dial-Up VPN" "Red_Tecapps" "ANY" nat src
dip-id 6 tunnel vpn "VPNCliente_

juniper" id 0x30 pair-policy 125 log

set policy id 124

exit

set policy id 113 from "Dedicado" to "Trust" "Any" "MIP(201.116.35.121)" "Pto-SIP" permit
log

set policy id 113 application "IGNORE"

set policy id 113

set service "SIP"

exit

set policy id 143 from "Dedicado" to "Trust" "Any" "MIP(201.116.35.121)" "ANY" permit log

set policy id 143

exit

set policy id 123 from "Infinitum" to "Dedicado" "10.30.30.0/24" "Sucursal_AvMexico" "ANY"
permit log

set policy id 123

```
set dst-address "Sucursal_AvMexico-lab"

set dst-address "Sucursal_Chicoloapan"

set dst-address "Sucursal_Coyoacan"

set dst-address "Sucursal_Culhuacan"

set dst-address "Sucursal_Ermita"

set dst-address "Sucursal_Estadio"

set dst-address "Sucursal_Sur16"

set dst-address "Sucursal_Tepozanes"

set dst-address "Sucursal_Tezonco"

set dst-address "Sucursal_Tulyehualco"

set dst-address "Sucursal_Viaducto"

set dst-address "Sucursal_Voca7"

set dst-address "Sucursal_Xochimilco"

exit

set policy id 122 from "Dedicado" to "Infinitum" "Sucursal_AvMexico" "10.30.30.0/24" "ANY"
permit log

set policy id 122

set src-address "Sucursal_AvMexico-lab"

set src-address "Sucursal_Chicoloapan"

set src-address "Sucursal_Culhuacan"

set src-address "Sucursal_Ermita"

set src-address "Sucursal_Estadio"
```

set src-address "Sucursal_Sur16"

set src-address "Sucursal_Tepozanes"

set src-address "Sucursal_Tezonco"

set src-address "Sucursal_Tulyehualco"

set src-address "Sucursal_Viaducto"

set src-address "Sucursal_Voca7"

exit

set policy id 120 from "Trust" to "Infinitum" "Red_Tecapps" "10.30.30.0/24" "ANY" permit log

set policy id 120

exit

set policy id 145 from "Dedicado" to "DMZ" "172.16.117.11/32" "Stratix" "stratix" permit log

set policy id 145

exit

set policy id 144 from "Dedicado" to "DMZ" "172.16.106.10/32" "Stratix" "stratix" permit log

set policy id 144

exit

set policy id 119 from "Dedicado" to "DMZ" "172.16.150.0/24" "Red_DMZ" "ANY" permit log

set policy id 119

set dst-address "Red_Secure Access"

exit

set policy id 118 from "Dedicado" to "Trust" "172.16.150.0/24" "Red_Tecapps" "ANY" permit log

set policy id 118

exit

set policy id 117 from "DMZ" to "Dedicado" "Red_DMZ" "172.16.150.0/24" "ANY" permit log

set policy id 117

set src-address "Red_Secure Access"

exit

set policy id 125 from "Trust" to "Dedicado" "Red_Tecapps" "Dial-Up VPN" "ANY" tunnel
vpn "VPNCliente_

juniper" id 0x30 pair-policy 124 log

set policy id 125

exit

set policy id 116 from "Trust" to "Dedicado" "Red_Tecapps" "172.16.150.0/24" "ANY" permit
log

set policy id 116

exit

set policy id 112 from "Untrust" to "Trust" "Any" "MIP(201.116.35.121)" "Pto-SIP" permit log

set policy id 112

exit

set policy id 103 from "DMZ" to "Untrust" "Exchange" "Any" "SMTP" nat src deny log

set policy id 103

exit

set policy id 105 from "DMZ" to "Untrust" "192.168.1.19/32" "Any" "SMTP" nat src permit log

set policy id 105 disable

set policy id 105

exit

set policy id 106 from "DMZ" to "Untrust" "192.168.1.20/32" "Any" "SMTP" nat src permit log

set policy id 106 disable

set policy id 106

exit

set policy id 101 from "DMZ" to "Trust" "192.168.1.19/32" "Red_Tecapps" "ANY" permit log

set policy id 101

set dst-address "Red_Wireless"

exit

set policy id 98 from "Trust" to "Untrust" "Red_Tecapps" "Any" "POP3" nat src deny log

set policy id 98

exit

set policy id 97 from "Trust" to "Infinitum" "Red_Tecapps" "Any" "POP3" nat src deny log

set policy id 97

exit

set policy id 95 from "Trust" to "Infinitum" "Red_Tecapps" "Any" "SMTP" nat src deny log

set policy id 95

exit

set policy id 94 from "Trust" to "Untrust" "Red_Tecapps" "Any" "SMTP" nat src deny log

set policy id 94

exit

```
set policy id 91 from "DMZ" to "Dedicado" "Red_DMZ" "Sucursal_Chicoloapan" "ANY"  
permit log
```

```
set policy id 91
```

```
set src-address "Red_Secure Access"
```

exit

```
set policy id 90 from "Trust" to "Dedicado" "Red_Tecapps" "Sucursal_Chicoloapan" "ANY"  
permit log
```

```
set policy id 90
```

exit

```
set policy id 89 from "Dedicado" to "Trust" "Sucursal_Chicoloapan" "Red_Tecapps" "ANY"  
permit log
```

```
set policy id 89
```

exit

```
set policy id 88 from "Dedicado" to "DMZ" "Sucursal_Chicoloapan" "Red_DMZ" "ANY"  
permit log
```

```
set policy id 88
```

```
set dst-address "Red_Secure Access"
```

exit

```
set policy id 87 from "Dedicado" to "DMZ" "Sucursal_AvMexico" "Red_DMZ" "ANY" permit  
log
```

```
set policy id 87
```

```
set src-address "Sucursal_AvMexico-lab"
```

```
set dst-address "Red_Secure Access"
```

```
exit
```

```
set policy id 86 from "Dedicado" to "Trust" "Sucursal_AvMexico" "Red_Tecapps" "ANY"  
permit log
```

```
set policy id 86
```

```
set src-address "Sucursal_AvMexico-lab"
```

```
exit
```

```
set policy id 85 from "DMZ" to "Dedicado" "Red_DMZ" "Sucursal_AvMexico" "ANY" permit  
log
```

```
set policy id 85
```

```
set src-address "Red_Secure Access"
```

```
set dst-address "Sucursal_AvMexico-lab"
```

```
exit
```

```
set policy id 84 from "Trust" to "Dedicado" "Red_Tecapps" "Sucursal_AvMexico" "ANY"  
permit log
```

```
set policy id 84
```

```
set dst-address "Sucursal_AvMexico-lab"
```

```
exit
```

```
set policy id 83 from "DMZ" to "Dedicado" "Red_DMZ" "Sucursal_Voca7" "ANY" permit log
```

```
set policy id 83
```

```
set src-address "Red_Secure Access"
```

```
exit
```

set policy id 82 from "Trust" to "Dedicado" "Red_Tecapps" "Sucursal_Voca7" "ANY" permit
log

set policy id 82

exit

set policy id 81 from "Dedicado" to "Trust" "Sucursal_Voca7" "Red_Tecapps" "ANY" permit
log

set policy id 81

exit

set policy id 80 from "Dedicado" to "DMZ" "Sucursal_Voca7" "Red_DMZ" "ANY" permit log

set policy id 80

set dst-address "Red_Secure Access"

exit

set policy id 79 from "Dedicado" to "DMZ" "Sucursal_Sur16" "Red_DMZ" "ANY" permit log

set policy id 79

set dst-address "Red_Secure Access"

exit

set policy id 78 from "Dedicado" to "Trust" "Sucursal_Sur16" "Red_Tecapps" "ANY" permit
log

set policy id 78

exit

set policy id 77 from "Trust" to "Dedicado" "Red_Tecapps" "Sucursal_Sur16" "ANY" permit
log

set policy id 77

exit

set policy id 76 from "DMZ" to "Dedicado" "Red_DMZ" "Sucursal_Sur16" "ANY" permit log

set policy id 76

set src-address "Red_Secure Access"

exit

set policy id 74 from "Trust" to "Dedicado" "Red_Tecapps" "Sucursal_Xochimilco" "ANY"
permit log

set policy id 74

exit

set policy id 73 from "Dedicado" to "DMZ" "Sucursal_Xochimilco" "Red_DMZ" "ANY" permit
log

set policy id 73

set dst-address "Red_Secure Access"

exit

set policy id 72 from "Dedicado" to "Trust" "Sucursal_Xochimilco" "Red_Tecapps" "ANY"
permit log

set policy id 72

exit

set policy id 70 from "Dedicado" to "Trust" "Sucursal_Culhuacan" "Red_Tecapps" "ANY"
permit log

set policy id 70

exit

set policy id 69 from "Trust" to "Dedicado" "Red_Tecapps" "Sucursal_Culhuacan" "ANY"
permit log

set policy id 69

exit

set policy id 75 from "DMZ" to "Dedicado" "Red_DMZ" "Sucursal_Xochimilco" "ANY" permit
log

set policy id 75

set src-address "Red_Secure Access"

exit

set policy id 68 from "DMZ" to "Dedicado" "Red_DMZ" "Sucursal_Culhuacan" "ANY" permit
log

set policy id 68

set src-address "Red_Secure Access"

exit

set policy id 67 from "DMZ" to "Dedicado" "Red_DMZ" "Sucursal_Ermita" "ANY" permit log

set policy id 67

set src-address "Red_Secure Access"

exit

set policy id 66 from "Trust" to "Dedicado" "Red_Tecapps" "Sucursal_Ermita" "ANY" permit
log

set policy id 66

exit

set policy id 71 from "Dedicado" to "DMZ" "Sucursal_Culhuacan" "Red_DMZ" "ANY" permit log

set policy id 71

set dst-address "Red_Secure Access"

exit

set policy id 64 from "Dedicado" to "DMZ" "Sucursal_Ermita" "Red_DMZ" "ANY" permit log

set policy id 64

set dst-address "Red_Secure Access"

exit

set policy id 63 from "Dedicado" to "DMZ" "Sucursal_Coyoacan" "Red_DMZ" "ANY" permit log

set policy id 63

set dst-address "Red_Secure Access"

exit

set policy id 65 from "Dedicado" to "Trust" "Sucursal_Ermita" "Red_Tecapps" "ANY" permit log

set policy id 65

exit

set policy id 62 from "Dedicado" to "Trust" "Sucursal_Coyoacan" "Red_Tecapps" "ANY" permit log

set policy id 62

exit

set policy id 61 from "Trust" to "Dedicado" "Red_Tecapps" "Sucursal_Coyoacan" "ANY"
permit log

set policy id 61

exit

set policy id 60 from "DMZ" to "Dedicado" "Red_DMZ" "Sucursal_Coyoacan" "ANY" permit
log

set policy id 60

set src-address "Red_Secure Access"

exit

set policy id 59 from "DMZ" to "Dedicado" "Red_DMZ" "Sucursal_Tezonco" "ANY" permit
log

set policy id 59

set src-address "Red_Secure Access"

exit

set policy id 58 from "Trust" to "Dedicado" "Red_Tecapps" "Sucursal_Tezonco" "ANY"
permit log

set policy id 58

exit

set policy id 57 from "Dedicado" to "Trust" "Sucursal_Tezonco" "Red_Tecapps" "ANY"
permit log

set policy id 57

exit

set policy id 56 from "Dedicado" to "DMZ" "Sucursal_Tezonco" "Red_DMZ" "ANY" permit
log

set policy id 56

set dst-address "Red_Secure Access"

exit

set policy id 55 from "Dedicado" to "DMZ" "Sucursal_Tulyehualco" "Red_DMZ" "ANY" permit log

set policy id 55

set dst-address "Red_Secure Access"

exit

set policy id 54 from "Dedicado" to "Trust" "Sucursal_Tulyehualco" "Red_Tecapps" "ANY" permit log

set policy id 54

exit

set policy id 53 from "DMZ" to "Dedicado" "Red_DMZ" "Sucursal_Tulyehualco" "ANY" permit log

set policy id 53

set src-address "Red_Secure Access"

exit

set policy id 52 from "Trust" to "Dedicado" "Red_Tecapps" "Sucursal_Tulyehualco" "ANY" permit log

set policy id 52

exit

set policy id 50 from "Dedicado" to "Trust" "Sucursal_Tepozanes" "Red_Tecapps" "ANY" permit log

set policy id 50

exit

set policy id 49 from "Dedicado" to "DMZ" "Sucursal_Tepozanes" "Red_DMZ" "ANY" permit
log

set policy id 49

set dst-address "Red_Secure Access"

exit

set policy id 48 from "DMZ" to "Dedicado" "Red_DMZ" "Sucursal_Tepozanes" "ANY" permit
log

set policy id 48

set src-address "Red_Secure Access"

exit

set policy id 47 from "DMZ" to "Dedicado" "Red_DMZ" "Sucursal_Estadio" "ANY" permit log

set policy id 47

set src-address "Red_Secure Access"

exit

set policy id 43 from "DMZ" to "Dedicado" "Red_DMZ" "Sucursal_Viaducto" "ANY" permit
log

set policy id 43

set src-address "Red_Secure Access"

exit

set policy id 102 from "DMZ" to "Dedicado" "Exchange" "Any" "POP3" nat src permit log

set policy id 102

exit

set policy id 104 from "DMZ" to "Dedicado" "192.168.1.19/32" "Any" "ANY" nat src permit
log

set policy id 104

exit

set policy id 152 from "DMZ" to "Dedicado" "192.168.1.20/32" "Any" "ANY" nat src permit
log

set policy id 152

exit

set policy id 26 from "DMZ" to "Dedicado" "192.168.1.20/32" "Any" "ANY" nat src permit log

set policy id 26 disable

set policy id 26

exit

set policy id 42 from "DMZ" to "Trust" "192.168.1.15/32" "Red_Tecapps" "ANY" permit log

set policy id 42

set dst-address "Red_Wireless"

exit

set policy id 41 from "Dedicado" to "DMZ" "Sucursal_Viaducto" "Red_DMZ" "ANY" permit
log

set policy id 41

set dst-address "Red_Secure Access"

exit

set policy id 40 from "Dedicado" to "DMZ" "Sucursal_Estadio" "Red_DMZ" "ANY" permit log

set policy id 40

set dst-address "Red_Secure Access"

exit

set policy id 3 from "Dedicado" to "DMZ" "Any" "VIP(ethernet0/4)" "ANY" permit log

set policy id 3

exit

set policy id 16 from "Dedicado" to "DMZ" "Any" "MIP(201.116.35.114)" "Pto_Visualab-1951" permit log

set policy id 16

exit

set policy id 44 from "Dedicado" to "DMZ" "Any" "MIP(201.116.35.116)" "HTTP" permit log

set policy id 44

exit

set policy id 39 from "Dedicado" to "Trust" "Sucursal_Viaducto" "Red_Tecapps" "ANY" permit log

set policy id 39

exit

set policy id 38 from "Dedicado" to "Trust" "Sucursal_Estadio" "Red_Tecapps" "ANY" permit log

set policy id 38

exit

set policy id 51 from "Trust" to "Dedicado" "Red_Tecapps" "Sucursal_Tepozanes" "ANY" permit log

set policy id 51

exit

set policy id 37 from "Trust" to "Dedicado" "Red_Tecapps" "Sucursal_Estadio" "ANY" permit log

set policy id 37

exit

set policy id 36 from "Trust" to "Dedicado" "Red_Tecapps" "Sucursal_Viaducto" "ANY" permit log

set policy id 36

exit

set policy id 96 from "Trust" to "Dedicado" "Any" "Any" "SMTP" nat src deny log

set policy id 96

exit

set policy id 110 from "Trust" to "Dedicado" "Any" "Any" "POP3" nat src deny log

set policy id 110

exit

set policy id 34 from "DMZ" to "Dedicado" "Visualab" "Any" "ANY" nat src permit log

set policy id 34

set src-address "Web"

exit

set policy id 115 from "Infinitum" to "Trust" "10.30.30.7/32" "Red_Tecapps" "ANY" permit log

set policy id 115

exit

```
set policy id 33 from "Infinitum" to "Trust" "Any" "VIP(ethernet0/3)" "Pto_Escritorio_remoto"  
permit log
```

```
set policy id 33
```

exit

```
set policy id 32 from "Trust" to "Untrust" "Red_Wireless" "Any" "HTTP" nat src permit log  
count
```

```
set policy id 32 av "AV-Tecapps"
```

```
set policy id 32
```

```
set src-address "Grupo_AccesoTotal"
```

```
set service "HTTP-EXT"
```

```
set service "HTTPS"
```

exit

```
set policy id 29 from "Dedicado" to "DMZ" "Any" "MIP(201.116.35.117)"  
"Pto_Escritorio_remoto" permit log
```

```
set policy id 29
```

exit

```
set policy id 27 from "Trust" to "Dedicado" "Red_Wireless" "Any" "ANY" nat src permit log
```

```
set policy id 27 av "AV-Tecapps"
```

```
set policy id 27
```

```
set src-address "Grupo_AccesoTotal"
```

exit

```
set policy id 28 from "Trust" to "Dedicado" "Red_Tecapps" "Any" "HTTP" nat src permit log  
url-filter
```

```
set policy id 28 av "Av-Tecapps_Mortales"
```

```
set policy id 28
```

```
set service "HTTP-EXT"
```

```
set service "HTTPS"
```

```
set url protocol sc-cpa profile "Filtrado_Tecapps"
```

```
exit
```

```
set policy id 25 from "Trust" to "Infinitum" "Red_Wireless" "Any" "HTTP" nat src permit log
```

```
set policy id 25 av "AV-Tecapps"
```

```
set policy id 25
```

```
set src-address "Grupo_AccesoTotal"
```

```
set service "HTTP-EXT"
```

```
set service "HTTPS"
```

```
set url protocol sc-cpa profile "Filtrado_Tecapps"
```

```
exit
```

```
set policy id 46 from "Trust" to "Infinitum" "Red_Tecapps" "Any" "MS-MESSENGER" nat src  
deny log
```

```
set policy id 46
```

```
set service "MSN"
```

```
set service "NSM"
```

```
exit
```

set policy id 24 from "Trust" to "Infinitum" "Red_Tecapps" "Any" "HTTP" nat src permit log url-filter

set policy id 24 attack "HIGH:CHAT:SIGS" action drop ip-action "notify" target "serv" timeout 60

set policy id 24

set attack "INFO:CHAT:SIGS" action "drop" ip-action "notify" target "serv" timeout 60

set attack "INFO:CHAT:ANOM" action "drop" ip-action "notify" target "serv" timeout 60

exit

set policy id 24 av "Av-Tecapps_Mortales"

set policy id 24

set service "HTTP-EXT"

set service "HTTPS"

set url protocol sc-cpa profile "Filtrado_Tecapps"

exit

set policy id 23 from "Trust" to "Untrust" "callcenter4" "Any" "HTTP" nat src permit log count

set policy id 23

set service "HTTP-EXT"

set service "HTTPS"

exit

set policy id 45 from "Trust" to "Untrust" "Red_Tecapps" "Any" "MS-MESSENGER" nat src deny log count

set policy id 45

set service "MSN"

```
set service "NSM"
```

```
exit
```

```
set policy id 2 from "DMZ" to "Untrust" "Red_DMZ" "Any" "ANY" nat src permit log
```

```
set policy id 2
```

```
set src-address "Red_Secure Access"
```

```
exit
```

```
set policy id 8 from "Trust" to "Infinitum" "Red_Tecapps" "Any" "ANY" nat src permit log
```

```
set policy id 8 attack "HIGH:CHAT:SIGS" action drop ip-action "notify" target "serv" timeout  
60
```

```
set policy id 8
```

```
set attack "INFO:CHAT:SIGS" action "drop" ip-action "notify" target "serv" timeout 60
```

```
set attack "INFO:CHAT:ANOM" action "drop" ip-action "notify" target "serv" timeout 60
```

```
exit
```

```
set policy id 8
```

```
exit
```

```
set policy id 9 from "DMZ" to "Infinitum" "Red_DMZ" "Any" "ANY" nat src permit log
```

```
set policy id 9
```

```
set src-address "Red_Secure Access"
```

```
exit
```

```
set policy id 11 from "DMZ" to "Dedicado" "Red_DMZ" "Any" "ANY" nat src permit log
```

```
set policy id 11
```

```
set src-address "Red_Secure Access"
```

exit

set policy id 13 from "DMZ" to "Trust" "Red_DMZ" "Red_Tecapps" "ANY" permit log

NORMA 27001 SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACIÓN

Norma ISO 27001

Seguridad informática

La totalidad de los especialistas en seguridad basan sus conocimientos y experticias sobre el aspecto técnico tradicional de la seguridad, esto es en las áreas IT, aunque bastantes de ellos consideran las cuestiones propias como el nuevo aspecto en las comunicaciones y que hace que actualmente se hable de TIC.

Además de tener un enfoque técnico prácticamente, los especialistas únicamente se manejan con las vulnerabilidades y en parte con amenazas en forma de ataques, todo lo dicho no se considera suficiente para hablar de los riesgos correspondientes.

Con el fin de establecer una evaluación de riesgos, se necesita realizar una evaluación a los activos, además de identificar cualquier amenaza que pueda aprovechar y explotar las vulnerabilidades de estos activos. Expuesto lo anterior, sí podemos realizar la determinación de los riesgos teniendo como referencia:

Activos: con un rango de 5 a 8.

Vulnerabilidades: rango de 3.

Amenazas: rango de 3 a 5.

En el caso de que más tarde se pretenda determinar qué hacer con los distintos riesgos, en el mayor número de casos se persigue mitigar hasta conseguir un nivel aceptable, por lo que habrá que implantar las medidas de seguridad que se consideren oportunas para tal efecto.

Si encontramos riesgos con características técnicas, el enfoque más eficaz es llevar a cabo un análisis gracias a los estándares técnicos o bien gracias a las normas internacionales, como la ISO 27002, en la que se realizan todos los controles necesarios y se determina el nivel en que se tiene que implantar para minimizar los riesgos que se encuentren a niveles aceptables.

Hasta llegado este punto hablamos de seguridad informática. Este término es una traducción del inglés, information security, el sentido que recoge dicha problemática se aproxima más a términos como pueden ser “computer security” o network security”.

Seguridad de la información

Estamos ante un proceso en que se está produciendo modificaciones, por lo que el término Seguridad de la Información está tomando una traducción más acertada sobre information security. Aunque aún hay muchos especialistas que siguen nombrándolo según el enfoque técnico que hemos comentado anteriormente.

La Seguridad de la Información es muy extensa, por lo que no es sólo una cuestión técnica sino que supone una responsabilidad de la alta dirección de la empresa, así como de sus directivos.

Tenemos que tomar en cuenta que el ambiente TIC está orientado al servicio y a la actuación en función de los procesos de negocio. Se diferencia de los procesos centrales de la misma empresa que constituyen el núcleo de los negocios de la empresa.

En el caso de no involucrarse las unidades activas y los líderes de negocio, como podrían ser, ejecutivos, directivos, etc. de las entidades, no podrá existir un plan de Seguridad de la

Información, a partir de todos los riesgos determinados. Todo ello se lleva a cabo en el seno del sistema de dirección y control propio del gobierno corporativo.

Se tiene que considerar los sujetos, los procesos y las funciones de negocio, además de la protección de todos los activos/recursos de la entidad impulsora, propietaria y beneficiaria de la Seguridad de la Información, dentro de un marco de responsabilidades compartidas.

Se tienen que considerar la totalidad de los riesgos técnicos de TIC, además de que la seguridad se desarrolle por toda la empresa, es decir, son riesgos organizacionales, operacionales y físicos.

Los riesgos operacionales son hoy en día más cruciales en lo referente a Seguridad de la Información. Las vulnerabilidades de este tipo de riesgo se expanden durante una amplia gama de grises, en conexión con el comportamiento humano y los juicios subjetivos de las personas, la resistencia al cambio, la cultura empresarial, la forma de comunicarse, etc.

Establecer las distintas vulnerabilidades de una empresa es un proceso muy distinto a las mediciones o lecturas tomadas con los ordenadores, servidores, rúters, etc. como normalmente no se disponen de datos históricos suficientes, realizar un análisis exacto se hace muy complicado. El análisis es completado con información que se puede recabar y que corresponda con la información subjetiva surgida de las opiniones distintas. Dichas opiniones pueden ser identificadas y analizadas a través del método de investigación prospectiva, seguido muy de cerca por entrevistas personales que establecen el valor de estas opiniones.

La evaluación de los activos no se encuentra al alcance de la mayoría de los técnicos. Los propietarios de los procesos de negocio son quienes pueden determinar un valor correcto de los mismos y de allí derivar a los valores de los activos que se utilizan en las distintas funciones que componen cada caso.

Seguridad de la Información y Seguridad Informática

El desarrollo que se ha experimentado en cuanto a seguridad informática al de seguridad de la información, implica incrementar el campo de visión del marco de riesgos de negocio respecto a la perspectiva tradicional de seguridad técnica, fundamentada en las vulnerabilidades.

En el entorno de la seguridad de la información los riesgos de negocio incluyen, no sólo las vulnerabilidades y las amenazas, sino que incluyen también el conjunto de factores que determinan los riesgos:

Activos

Vulnerabilidades

Amenazas

Los riesgos de negocio que incluyen los riesgos organizacionales, operacionales, físicos y de sistemas TIC.

Podemos conseguir un enfoque completo de seguridad de la información en la parte en la cual se considera los recursos necesarios para minimizar los riesgos dentro de un plan de seguridad, no se puede considerar un gasto sino una inversión para la empresa. Solicita de un análisis y determinar de una manera cuantificable el retorno de las inversiones en seguridad.

Sistema de Gestión de Seguridad de la Información

La implantación de un Sistema de Gestión de Seguridad de la Información en las empresas supone un paso más para garantizar a los usuarios que la información manipulada por dicha empresa se realiza bajo la máxima seguridad.

RESULTADO

Cuando visite a la empresa TECAPPS detecte al inicio que había un ataque cibernético, esto que quiere decir, con esto capturaban información como la base de datos de la empresa y de los empleados como la nómina, sus registros, etc. se detectó mucho correo falso que robaban los elementos de su plataforma, también detecte accesos no permitidos lo cual no sabían quién estaba intentando entrar a los servidores donde se encuentran la información de los empleados por lo cual se llevó a cabo implementando un firewall para poder así restringir quien empleado tenía accesos a sus servidores y desde internet. Con esto podía validar y proteger a la empresa de todo ese tipo de información que tenía crítica. Ya que un firewall sirve como un cuello de botella por el que todo el tráfico de Internet entrante y saliente debe pasar, permitiendo controlar el tráfico y evita en gran medida que los hackers lo superen y

por supuesto te ayuda a mantener a salvo los datos confidenciales de tu empresa a la empresa TECAPPS sirvió mucho la implementación ya que Monitoriza y registra de los servicios utilizados para usar Internet, FTP y otros protocolos.

4.2 Trabajos Futuros

De acuerdo con el análisis de infraestructura y seguridad, TECAPPS recomienda tomar las siguientes medidas:

Utilización de un Next Generation Firewall, para el control a nivel de capa 7 en la red y análisis de tráfico SSL; asimismo poder generar reportes diarios, semanales o mensuales de la actividad y uso de la red.

4.3 Recomendaciones

Que cuente con al menos las siguientes características:

- Motor de clasificación del tráfico que permite identificar con precisión aplicaciones, independientemente de puerto.
- Motor de exploración basada en el flujo, inspección profunda de paquetes.
- Generación de informes y registros de la actividad y uso de la red y que pueda enviarlos de manera automática listos para su revisión.
- Que pueda generar alertas de seguridad y notificar

ANEXOS

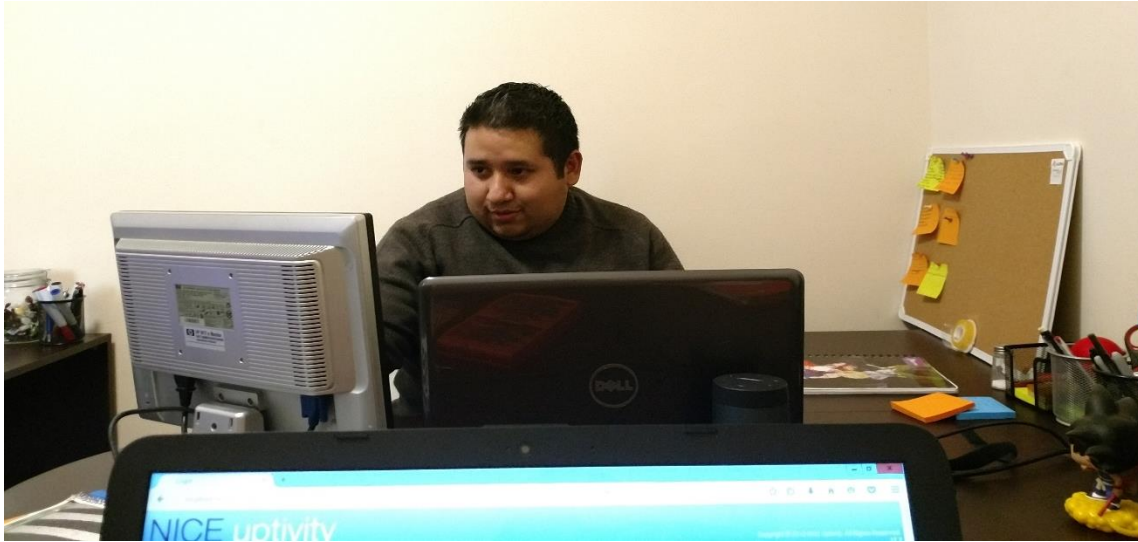


ILUSTRACIÓN 21 CONFIGURACION INICIAL

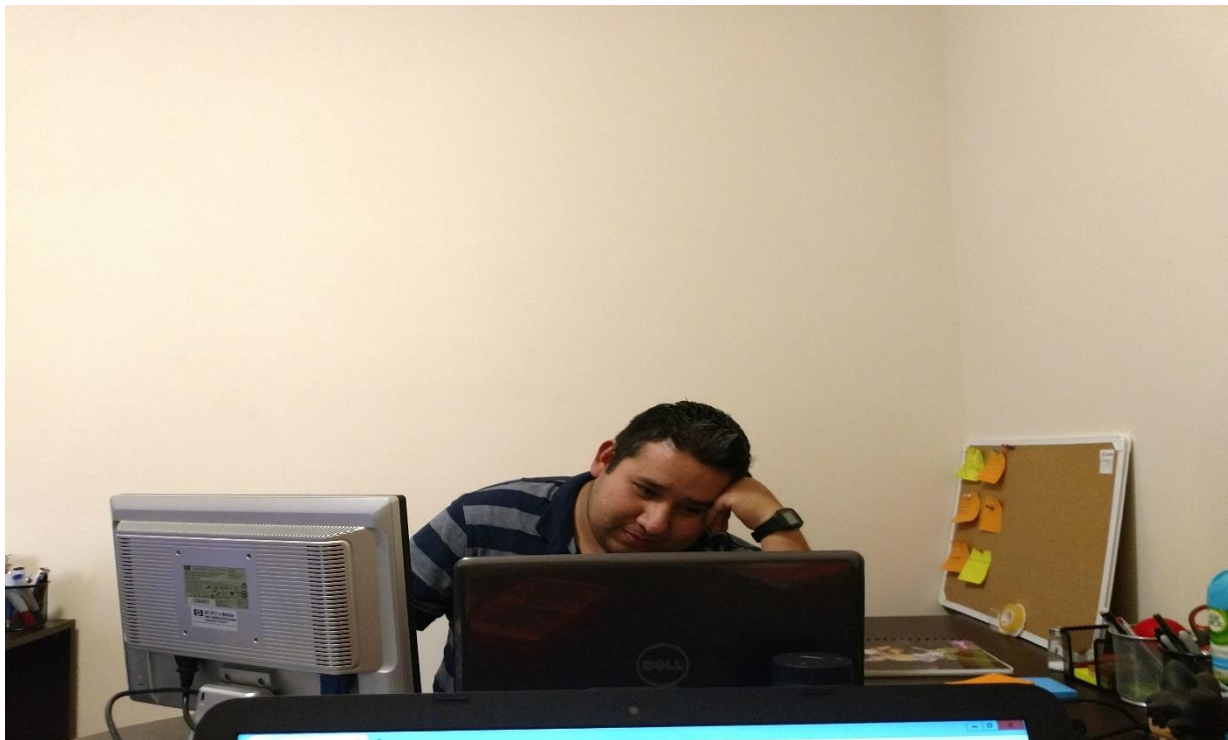




ILUSTRACIÓN 22 COMPAÑEROS DEL TRABAJO



ILUSTRACIÓN 23 ACCESS POINT



ILUSTRACIÓN 24 CAMARA DE SEGURIDAD



ILUSTRACIÓN 25 RACK

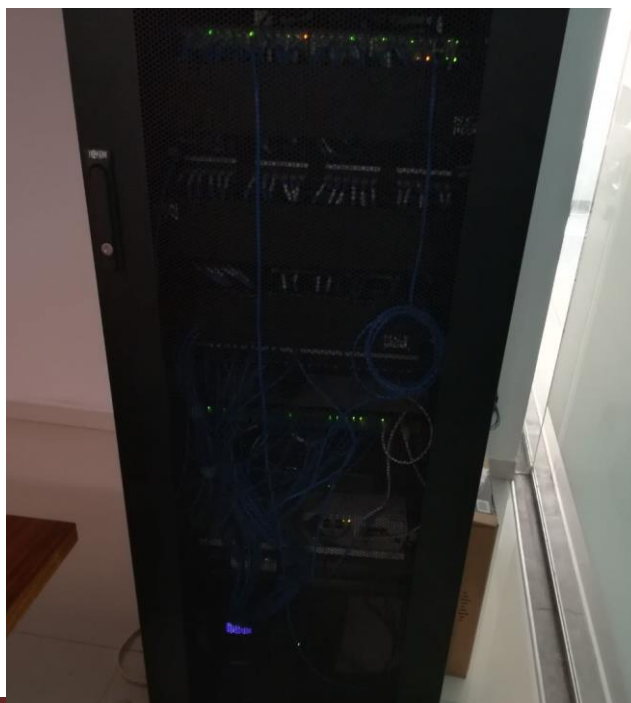
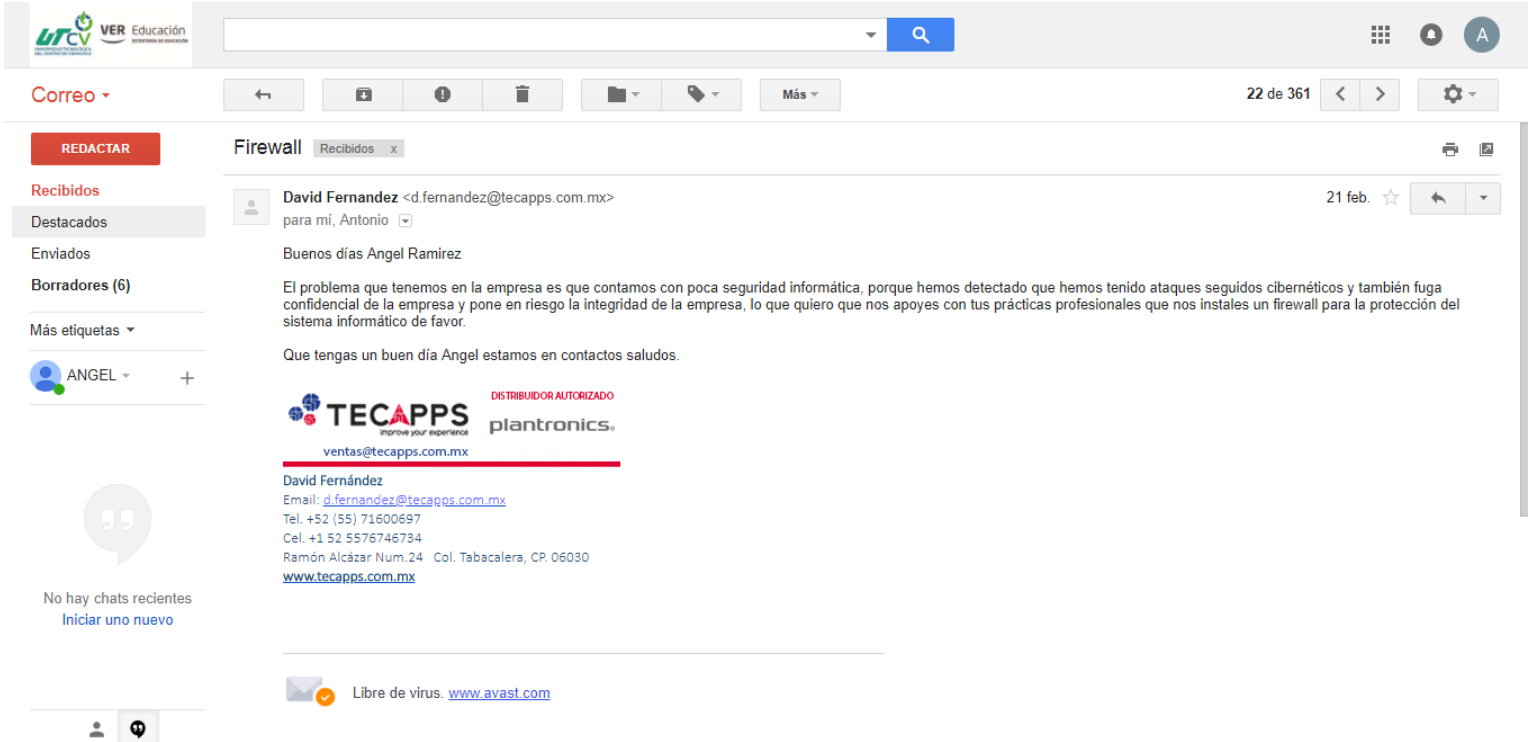


ILUSTRACIÓN 26 RACK



The screenshot shows an email client interface. At the top left is the UTCv logo and 'VER Educación'. The main header area contains a search bar, navigation icons, and '22 de 361' messages. The email is titled 'Firewall' and is from 'David Fernandez <d.fernandez@tecapps.com.mx>' dated '21 feb.'. The body of the email reads: 'Buenos días Angel Ramirez. El problema que tenemos en la empresa es que contamos con poca seguridad informática, porque hemos detectado que hemos tenido ataques seguidos cibernéticos y también fuga confidencial de la empresa y pone en riesgo la integridad de la empresa, lo que quiero que nos apoyes con tus prácticas profesionales que nos instales un firewall para la protección del sistema informático de favor. Que tengas un buen día Angel estamos en contactos saludos.' Below the text is a logo for 'TECAPPS' (Distribuidor Autorizado) and 'plantronics', with the website 'ventas@tecapps.com.mx'. Contact information for David Fernández is provided: Email: d.fernandez@tecapps.com.mx, Tel: +52 (55) 71600697, Cel: +1 52 5576746734, Ramón Alcázar Num.24 Col. Tabacalera, CP. 06030, www.tecapps.com.mx. At the bottom of the email, there is a virus scan notification: 'Libre de virus. www.avast.com'.

ILUSTRACIÓN 27 PRUEBA DEL PROBLEMA DE LA EMPRESA

BIBLIOGRAFÍA

- ALARCÓN, O. P. (2008). *blogspot*. Obtenido de <http://proyecto-de-redes.blogspot.mx/2008/01/seguridad-de-la-informacin.html>
- Avenue, N. M. (2006). *Juniper Networks, Inc*. Recuperado el 5 de febrero de 2018, de https://www.juniper.net/documentation/hardware/netscreen-appliances/translated/netscreen5x/5.4/SP_SSG5_HW.pdf
- Carballar, J. A. (2006). *RA-MA*. Recuperado el 17 de febrero de 2018, de <http://www.ra-ma.es/libros/FIREWALL-LA-SEGURIDAD-DE-LA-BANDA-ANCHA/194/978-84-7897-703-1>
- cisco*. (27 de diciembre de 2010). Obtenido de https://www.cisco.com/c/es_mx/support/docs/security/ios-firewall/98628-zone-design-guide.html
- González, J. N. (2005). *Cortafuegos*. Recuperado el 10 de febrero de 2018, de Arquitecturas de firewalls: <http://docplayer.es/1568874-Cortafuegos-firewall-arquitecturas-de-cortafuegos-juan-nieto-gonzalez-ies-a-carballeira.html>
- kaspersky*. (2018). *kaspersky*. Obtenido de <https://latam.kaspersky.com/resource-center/definitions/web-filter>
- Networks, J. (1999). *Juniper Networks*. Recuperado el 2 de febrero de 2018, de www.juniper.net/us/en/
- Networks, J. (1999-2010). *Juniper Networks*. Recuperado el 2018, de <https://www.juniper.net/documentation/software/screensos/screensos5.4.0/>
- Rouse, M. (2005-2018). *techtarget*. Recuperado el 2018
- scribd*. (2018). Obtenido de Juniper CLI: <https://es.scribd.com/doc/129847165/Juniper-CLI>