UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

"DISEÑO DE UNA RED DE DATOS PARA SEDE PRINCIPAL Y REMOTAS DEL SAT CON SEGURIDAD PERIMETRAL Y BANDWIDTH MANAGER CON ALTA DISPONIBILIDAD EN SU SEDE PRINCIPAL"

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

LIZANA SALAZAR, JIMMY ALEXANDER

Villa El Salvador

2016

DEDICATORIA

Dedico este trabajo de suficiencia a mis padres quienes me han apoyado incondicionalmente para poder llegar hasta estas instancias de mis estudios, ya que ellos siempre han estado presentes en los buenos y malos momentos.

A mis tías que siempre han formado parte muy importante de mi vida pues siempre me han brindado su apoyo, comprensión y me han dado el ejemplo de que todo es posible sin importar las condiciones.

AGRADECIMIENTO

Este proyecto, está dedicado a todas aquellas personas que me motivaron para su culminación.

Agradezco a mi familia por brindarme siempre su apoyo incondicional.

ÍNDICE

LISTADO DE FIGURAS

Capítulo 2

Capítulo 3

LISTADO DE TABLAS

INTRODUCCIÓN

Actualmente nos encontramos ante una de las eras informáticas más importantes, sobre todo en lo referente a internet y redes de datos.

La globalización del internet ha sido más rápida de lo que se esperaba, por lo que hemos tenido que aprender, aplicar y actualizar conceptos que hasta hace muy poco eran impensables para la mayoría de las personas, esto nos ha llevado a aprender las redes para nuestras relaciones sociales, comerciales y políticas.

La finalidad de este proyecto es ofrecer una solución integrada a través del diseño de una red de datos que esté basado en una alta disponibilidad y control del ancho de banda en la sede principal del SAT (Sistema de Administración Tributaria), además de permitir una conectividad con sus sedes remotas. Para ello se cuenta con un diseño y estructuras lógicas de red teniendo en cuenta los host, vlans, anchos de banda y cada servicio, para así poder mejorar el servicio hacia los diferentes usuarios que cuenta el Sistema de Administración Tributaria (SAT).

CAPÍTULO I. PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción de la Realidad Problemática

En la actualidad el SAT cuenta con una sede principal y 5 sedes remotas, las sedes remotas salen por un internet independiente es decir no están en la misma red que la principal, debido a la gran demanda de usuarios y para una mejor atención, se ve con la necesidad de contar con un sistema de datos que integre su sede principal con las sedes remotas, además de un equipo que garantice la seguridad en la información de manera rápida y eficiente de manera que pueda satisfacer la demanda de los diversos usuarios.

Actualmente si un firewall de alta capacidad, sin un control y visualización de su ancho de banda hacen que la red se perciba lenta e ineficientes, por ende la productividad se ve afectada. Es por ello que ve la necesidad de contar con un sistema pueda cubrir estas necesidades; además que contribuya a la eficiencia y que sus procesos se lleven de una manera confiable.

1.2 Justificación del Problema

Debido a que la función principal del SAT es ejercer la administración del régimen tributario y cada vez dicha labor va en aumento la entidad no cuenta con un firewall que asegure la seguridad en los procesos e información, además de no tener con un Bandwidth Manager para poder controlar el ancho de banda con la que se cuenta y así tener una mejor optimización de la red que beneficie tanto a los clientes como a los trabajadores.

Es por esta razón que este proyecto propone una solución a este problema que existe en el manejo de la información, con el diseño de una red de datos que tenga un seguridad perimetral de alta disponibilidad en su sede principal además de la interconexión con sus sedes remotas por medio de RPV; la cual se ajusta a las necesidades del SAT, además de poder asignar un determinado ancho de banda para cada servicio ,el objetivo es que tanto la sedes remotas y la principal puedan compartir información en tiempo real para poder tener una mayor rapidez en los procesos y servicios de la entidad.

1.3 Delimitación del Proyecto

Limitación teórica

- Red de datos con alta disponibilidad mediante Firewall
- Red Privada Virtual (4 o 6CoS)
- Bandwidth Manager

Limitación temporal

Este proyecto está realizado desde el diseño de red, en cuanto a la topología, software y hardware respectivamente, tanto un diagrama lógico como físico, se realiza durante el período de febrero a agosto del año 2016.

Limitación espacial

Este proyecto se realiza para el Sistema de Administración Tributaria (SAT) con sedes ubicadas en los distritos de Lima como cercado, San juan, Miraflores y Jesús María.

1.4 Formulación del Problema

1.4.1 Problema Principal

¿Es posible realizar un diseño para una red de datos con alta disponibilidad en su seguridad perimetral y administración de su ancho de banda e interconexión con sus sedes remotas a través de un RPV para el Sistema de Administración Tributaria (SAT)?

1.4.2 Problemas Específicos

- ¿Cómo determinar las necesidades actuales del SAT y los beneficios que esto podría brindar a los trabajadores y usuarios?

- ¿Cuál sería el mejor hardware y software para el diseño e implementación de la red de datos para el SAT?

¿Cómo definir las aplicaciones que consumen mayor ancho de banda para poder asignarle un determinado valor y tener una visualización y control total del tráfico de la red?

1.5 Objetivos

1.5.1 Objetivo General

- Diseñar una red de datos – Alta disponibilidad en su seguridad perimetral de la sede principal con un Bandwidth Manager e interconexión con sus sedes remotas por RPV.

1.5.2 Objetivos específicos

- Estudiar las necesidades de interconexión entre las sedes del SAT y los beneficios que se darían.

- Tener en cuenta el modelo y marca del hardware versión del software para la implementación de la red de datos para el SAT.

- Definir las aplicaciones que tengan mayor consumo del ancho de banda y ocasiones mayor tráfico en la red, para definir sus respectivos valores dentro de la red.

- Crear y definir zonas de seguridad en la red del SAT, para que se defina los servicios y dar mayor seguridad.

CAPÍTULO II: MARCO TEÓRICO

2.1 Antecedentes de la Investigación

- El ingeniero **Diego Eduardo Cortés Robles** (Universidad Andres Bello – Colombia - 2011), en su tesis: RED PERIMETRAL SEGURA DE LA CAMARA NACIONAL DEL COMERCIO. Concluye lo siguiente:

"El siguiente Trabajo de Título, aborda el tema de la seguridad perimetral en redes empresariales, la cual hoy en día es importante desarrollar. La seguridad perimetral consiste en entregar algunos parámetros de seguridad como lo es, bloqueo de URL, paquetes, conexiones o aplicaciones, Anti-malware, anti-spam, o mantener vigilada nuestra red por medio de IPS. Cada uno de estos puntos son implementados según las amenazas detectadas en la Cámara Nacional de Comercio. Generando pruebas y recolectando información del funcionamiento de la red, se implementa un cortafuegos o más bien conocido en inglés como Firewa11, el cual fue elegido previo contrato existente antes de la realización de este proyecto, el cual realizará las funcionalidades que se necesitan para poder tener una red segura perimetralmente. Este dispositivo es un cortafuego

WatchGuard, el cual posee las características necesarias para dar la solución de seguridad perimetral. Este dispositivo tiene la capacidad de generar registros y con estos a su vez generar reportes entendibles para cualquier usuario que los desee revisar. Con esto podemos estar revisando la red y encontrar ciertas vulnerabilidades en algunos puntos de la red. Con esta red segura los usuarios pudieron aumentar su calidad de trabajo, ya que los sistemas mejoraron en tiempos de respuesta, al igual que los enlaces de intemet. Esto ayudo en mejorar el uso del ancho de banda hacia la nube".

- El ingeniero **David Mayorga Polo** (Universidad Internacional SEK – Quito - 2008), en su tesis: ANALISIS, DISEÑO E IMPLEMENTACION DEL ESQUEMA DE SEGURIDAD PERIMETRAL PARA LA RED DE DATOS DE LA UISEK. Concluye lo siguiente:

"Las Instituciones educativas universitarias, además de perseguir el noble fin de educar a la gente, también tienen su parte administrativa, en la que se persiguen otros objetivos que vayan de la mano con el principal, que es educar. Las Universidades también son empresas, como cualquier otra, y necesitan proteger sus activos críticos de cualquier eventualidad que pueda suceder y afectar a su negocio. En la UISEK Ecuador Campus Miguel de Cervantes se consideran parte de los activos críticos los sistemas informáticos, no solo porque alojen información sensible, sino también porque son parte importante del proceso de educación de los alumnos y actualmente no se les da el suficiente resguardo, por lo que la presente investigación propone un esquema de seguridad perimetral para la red de datos del Campus; además del desarrollo de un manual de políticas de seguridad, así como un plan de contingencia ante posibles desastres y un esquema de monitoreo proactivo de la seguridad perimetral establecida".

- El ingeniero **Jorge Luis Valenzuela Gonzales** (Pontificia Universidad Católica del Perú – Lima. Perú - 2012), en su tesis: DISEÑO DE UNA ARQUITECTURA DE SEGURIDAD PERIMETRAL DE UNA RED DE COMPUTADORAS PARA UNA PEQUEÑA EMPRESA. Concluye lo siguiente:

"En el trabajo realizado se presenta una solución de seguridad perimétrica que cubra los requerimientos de una red de computadoras de una empresa pequeña. Se muestra además una simulación del diseño propuesto en un ambiente de pruebas controlado. En el primer capítulo se presenta el estado actual y riesgos de la información, y la importancia de la misma. Se presenta además la seguridad perimetral de la red de datos como parte de una problemática mayor. La seguridad de la información. En el segundo capítulo se muestra en detalle y de manera técnica, los riesgos, amenazas contra la integridad de una red de computadoras de una empresa pequeña y las contramedidas que pueden ser adoptadas. En el tercer capítulo se explica el escenario de trabajo, sus requerimientos y sus necesidades sin especificar aun producto alguno, sea software o hardware. En el cuarto capítulo se presentan los criterios que fueron tomados en consideración para la selección de la solución más idónea para el escenario planteado en el tercer capítulo. En el quinto capítulo, se desarrollan la política de seguridad que debe ser aplicada en la solución seleccionada en el cuarto capítulo, se plasma en los componentes que la conforman y se evalúa su desempeño en un ambiente de pruebas. Finalmente se presenta las conclusiones que se desprenden del análisis del escenario planteado, así como las recomendaciones para mantener un nivel de seguridad adecuado".

- El Ingeniero **Rodolfo Sirilo Córdova Gálvez,** (UniversidadPolitécnica Católica del Ecuador - Ecuador – 2009), en su tesis: ANALISIS Y PROPUESTA DE MEJORAS PARA LA SEGURIDAD DE REDES INTERNAS LAN Y REDES PERIMETRALES (DMZ)

UTILIZANDO TCP/IP Y GNU/LINUX EN PEQUEÑAS Y MEDIANAS EMPRESAS (PYMES) DEL ECUADOR. Concluye lo siguiente:

"Luego de las pruebas y evaluaciones realizadas, se determinó que ninguna de las herramientas libres por sí solas ofrece el 100% de seguridad, ni aun agregándoles todos los adicionales disponibles, cabe señalar que las herramientas propietarias tampoco ofrecen el 100% de seguridad, ya que encontramos vulnerabilidades de las mismas publicadas en el Internet. Agregando algunos adicionales a IPCOP (UrlFilter y CopFilter) se logra una seguridad del 89% en nuestra escala. De acuerdo al puntaje obtenido por IPCOP se concluye que si existe una solución adecuada para los problemas relacionados con la seguridad perimetral en las redes DMZ y LAN de las pymes del Ecuador, y es la utilización de software libre basado en GNU/LINUX. La seguridad perimetral debe realizarse a nivel de red para prevenir ataques de hackers, las intrusiones o el robo de información en las conexiones remotas y a nivel de contenidos para prevenir el ingreso de código malicioso, spam y los contenidos web no deseados por las empresas. El nivel de seguridad implementado está directamente relacionado con las políticas y planes de seguridad que dispongan las empresas ya que la seguridad no es un producto final, si no, es un proceso continuo".

- Los bachilleres **Manuel Fernando DefazCalvopiña y David Omar Guevara Aulestia,** (Universidad Técnica de Ambato – Guayaquil. Ecuador – 2015), en su tesis: LA SEGURIDAD PERIMETRAL Y SU INCIDENCIA EN SU CALIDAD DE SERVICIO DE LA RED INFORMATICA PARA EL GOBIERNO AUTONOMO DESCENTRALIZADO DE LA PROVINCIA DE COTOPAXI. Concluyen lo siguiente:

“La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad etc., en la presentación de sus servicios los gobiernos autónomos descentralizados emprenderán un proceso progresivo de aplicación de los sistemas de gobierno y democracia digital, aprovechando de las tecnologías disponibles. De esta manera poder brindar un mejor servicio a la ciudadanía en general. Tomando en cuenta factores esenciales como los avances en la tecnología, creación de redes informáticas, intercambio de información, vulnerabilidad de las redes, se pone en manifiesto la necesidad de implementar un sistema seguridad perimetral que cubra los requerimientos del GADPC. En la investigación realizada se presenta una solución de seguridad perimetral, que en su primera parte se describe el estado actual de la institución, los riesgos, amenazas contra la integridad de los activos del sistema informático y las contramedidas que pueden ser adoptadas. En segunda instancia se explica el escenario de trabajo, sus requerimientos y sus necesidades de seguridad presentando los criterios que fueron tomados en consideración para la selección de la solución más idónea, se desarrollan los controles de acceso lógico y las política de seguridad que debe ser aplicada en la solución seleccionada, para finalmente presentar las conclusiones que se desprenden del esquema de seguridad perimetral planteado, así como las recomendaciones para mantener un nivel de seguridad adecuado”.

2.2 Bases Teóricas

2.2.1 Fundamentos de Seguridad Perimetral.

La evolución de la tecnología y la constante demanda de seguridad han permitido que los sistemas de seguridad perimetral en redes evolucionen para ofrecer una mayor confiabilidad a los usuarios tanto internos como externos sobre la transparencia y protección de su información para el acceso de diferentes servicios, hoy en día existen un sin número de personas que usan sus

conocimientos y ética profesional de una forma incorrecta al ingresar a redes informáticas restringidas ocasionado pérdidas multimillonarias alrededor del mundo. Éste artículo tiene como objetivo realizar un análisis de los pasos y requerimientos necesarios para el diseño de un sistema de Seguridad Perimetral para una red de Datos.

La seguridad perimetral es un método de defensa de las redes informáticas, en el que consiste instalar equipos de comunicaciones en los que se establece las políticas de seguridad necesarias para su óptimo funcionamiento; estos equipos se los coloca entre la red externa y la red interna, permitiendo o denegando el acceso a los usuarios internos y externos a los diferentes servicios de la red.

La seguridad perimetral basa su filosofía en la protección de todo sistema informático de una empresa desde "fuera" es decir componer una coraza que proteja todos los elementos sensibles de ser atacados dentro de un sistema informático. Esto implica que cada paquete de tráfico transmitido debe ser diseccionado, analizado y aceptado o rechazado en función de su potencial riesgo de seguridad para nuestra red.

Para el diseño del sistema de seguridad perimetral es indispensable realizar un análisis a la situación actual de la red logrando así saber cuál de los segmentos de red de datos necesitan más protección, es decir que segmento de red debe tener o no permisos para acceder a los servicios de red o internet.

También cabe destacar la clasificación dependiendo del medio de detección. En esta se clasificarían en:

Sistemas Perimetrales Abiertos: Los que dependen de las condiciones ambientales para detectar. Como ejemplo de estos son video vigilancia, las barreras infrarrojas, las barreras de microondas. Esta característica provoca falsas alarmas o falta de sensibilidad en condiciones ambientales adversas.

Sistemas Perimetrales Cerrados: Los que no dependen del medio ambiente y controlan exclusivamente el parámetro de control. Como ejemplo de estos son los antiguos cables microfónicos, la fibra óptica y los sensores.

2.2.2 Perímetros de la red.

La seguridad perimetral es uno de los métodos posibles de defensa de una red, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles. Esto nos permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

La seguridad perimetral:

- No es un componente aislado: es una estrategia para proteger los recursos de una organización conectada a la red.

- Es la realización práctica de la política de seguridad de una organización. Sin una política de seguridad, la seguridad perimetral no sirve de nada.

- Condiciona la credibilidad de una organización en Internet.

Ejemplos de la seguridad perimetral:

- Rechazar conexiones a servicios comprometidos

- Permitir sólo ciertos tipos de tráfico (p. ej. correo electrónico) o entre ciertos nodos.

- Proporcionar un único punto de interconexión con el exterior - Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet

- Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet

- Auditar el tráfico entre el exterior y el interior.

- Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red, cuentas de usuarios internos.

Objetivos de la seguridad perimetral.

Los objetivos de la seguridad perimetral son:

• Proteger el perímetro de la red privada ante amenazas externas.

• Filtrar eficientemente los accesos solicitados hacia la red privada.

• Tomar acción ante cualquier amenaza antes de que acceda a la red privada.

Componentes de la seguridad perimetral

Los componentes esenciales que pueden existir en el perímetro de una red son:

a. **Ruteadores de perímetro.**

   Los ruteadores direccionan el tráfico de red hacía, desde y dentro de la red. Los ruteadores de perímetro (también se los conoce como ruteadores de frontera o límite) son los últimos ruteadores que están justo antes de una red no confiable, como el Internet. Debido a que todo el tráfico de Internet de una Organización pasa por estos ruteadores, se lo utiliza como un primer y último filtro, por eso se los considera críticos para la defensa.

b. **Firewall.**

   El firewall es un dispositivo que protege de amenazas externas a uno o varios equipos dentro de una red

Existen 2 tipos de firewall, los personales que protegen a un solo equipo en el cual está instalado, o los de red que protegen a los equipos de toda una red de datos.

Firewall de red

Existen 3 tipos de firewalls de red, los filtros de paquetes, los stateful y los deep-packetinspection.

Los filtros de paquetes son los firewall de más simple tipo y sirven para controlar el acceso a determinados segmentos de red definiendo que tipo de tráfico es permitido y que otro tipo no es permitido. Los filtros de paquete analizan el tráfico en la capa 4 del modelo OSI (Transporte):

• Dirección de origen

• Dirección de destino

• Puerto de origen

• Puerto de destino

• Protocolo

Los firewall analizan toda conexión que pasa por su interfaz de red, además de analizar los campos del encabezado del paquete (filtro de paquetes) también analiza el estado de la conexión (establecida, cerrada, reset, negociando), que sirve para detectar otros tipo de ataques que se basan en el estado de la conexión de los paquetes.

Los firewall deep-packetinspection o de inspección profunda de paquetes analizan la información en la Capa 7 (Aplicación).

Existen aplicaciones que requieren un manejo especial de los paquetes de datos cuando pasan por un firewall. Estos incluyen aplicaciones y protocolos que tienen embebidos información de direccionamiento IP en sus paquetes de datos o abren canales secundarios en puertos asignados dinámicamente (P2P). Usando inspección de aplicaciones se puede identificar los puertos asignados dinámicamente por la misma y permitir o denegar el intercambio de datos por esos puertos en una conexión específica.

NAT (Network Address Traslation)

La mayoría de firewalls existentes ofrecen el servicio de NAT, que consiste en enmascarar o disfrazar la dirección IP de los hosts protegidos o que están detrás del firewall a una dirección IP pública, por ejemplo, una red corporativa con 30 hosts con diferentes IP privadas dentro de la red interna, saldrán a navegar por Internet con una sola dirección IP pública.

IDS (Intrusion Detection Systems)

El funcionamiento de este tipo de herramientas se basa en el análisis del tráfico de red, el cual al entrar en contacto con el IDS es comparado con firmas de ataques conocidos o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes malformados, etc… y no solo se analiza que tipo de tráfico es sino también su contenido y su comportamiento.

Normalmente esta herramienta se integra con un firewall y al trabajar conjuntamente pueden convertirse es una herramienta muy poderosa de seguridad.

En un sistema pasivo, el sensor detecta la posible intrusión, almacena la información y envía una señal de alerta al administrador de la red, en cambio en sistemas reactivos el IDS responde a la actividad sospechosa reprogramando el firewall para que bloquee el tráfico de donde proviene el posible ataque.

IPS (Intrusion Prevention Systems)

Un IPS es un sistema que establece políticas de seguridad para proteger un equipo o una red. A diferencia con un IDS que se ocupa de alertar al administrador sobre actividad sospechosa o toma acción ante la detección de una posible intrusión, un IPS ya tiene preestablecidas políticas de seguridad que no dejarían acceder cierto tipo de tráfico o a ciertos patrones que se detecten dentro de los paquetes, a la red privada, es un tipo de protección proactiva a diferencia del IDS que es reactiva.

VPN (Virtual Prívate Networks)

Una VPN es una sesión de red protegida formada a través de un canal no protegido como es el Internet. Las Organizaciones crean VPN's para ofrecer integridad de datos, autenticación y encriptación de datos para asegurar la confidencialidad de los paquetes enviados sobre una red no protegida. Una VPN permite a un usuario externo unirse a una red privada a que participe en ésta sin estar conectado físicamente o internamente a la misma. El uso de este tipo de conexiones está diseñado también para ahorrar costos en líneas dedicadas externas.

Clasificación de las VPN:

a. **Site–to–Site:**

   Permiten a las Organizaciones establecer túneles VPN entre 2 o más ubicaciones (por ejemplo, oficina principal y sucursal) para que los usuarios se comuniquen mediante un medio compartido como el Internet.

b. **Remote-access:**

   Permite a los usuarios trabajar desde ubicaciones remotas (casa, hotel, etc…) como si estuvieran físicamente conectados a la red privada de la Organización.

SSL VPNs

Las VPN's basadas en SSL (Secure Socket Layer) están teniendo bastante demanda hoy en día, debido a su facilidad de uso. La característica más popular de éste tipo de VPN's es que el usuario solo necesita ejecutar un browser y conectarse a la dirección de la VPN, ésta facilidad de uso es debido a que la mayoría de firewalls aceptan conexión a SLL (Puerto 443) y no es necesario abrir otros puertos para establecer la comunicación.

Arquitectura de software

La arquitectura de software consiste en un conjunto de patrones definidos que proporcionan el marco de referencia para guiar la construcción de un software. Existen varios tipos de arquitecturas:

• **Monolítica:** El software se compone de un solo módulo donde se encuentra todo el código, es poco organizado.

• **Cliente-Servidor:** El software realiza todo el cómputo en un solo computador (Servidor) y entrega datos ya procesados a los clientes conectados, para que estos no realicen ningún proceso de datos.

• **Arquitectura de 3 niveles:** El computo se divide en 3 niveles, persistencia (Almacenamiento de datos), negocio (procesamiento de datos) y presentación (interfaz de usuario).

La arquitectura de software tiene un papel importante cuando se habla de una infraestructura segura porque el primer objetivo de la seguridad perimetral es proteger los datos y servicios de los sistemas de información.

DMZ (Zona Desmilitarizadas) y subredes monitoreadas.

Una DMZ es un área insegura, en el caso de una red es todo lo que está antes del firewall, y una subred monitoreada es una red pequeña que está aislada de la red interna pero también tiene la protección del firewall, éste tipo de redes se usan para separar servidores que necesitan ser accesibles desde Internet de los servidores que contienen sistemas que se usan solo internamente en la Organización.

Seguridad a nivel de aplicación: Secure Shell (SSH).

SSH es un programa de login remoto que nos permite realizar una transmisión segura de cualquier tipo de datos: passwords, sesión de login, ficheros, etc, sustituyendo a las habituales formas de acceso (Telnet, FTP…).

Su seguridad reside en el uso de criptografía fuerte, de manera que toda la comunicación es encriptado y autentificada de forma transparente para el usuario.

Este protocolo fue diseñado para dar seguridad al acceso a ordenadores de forma remota.

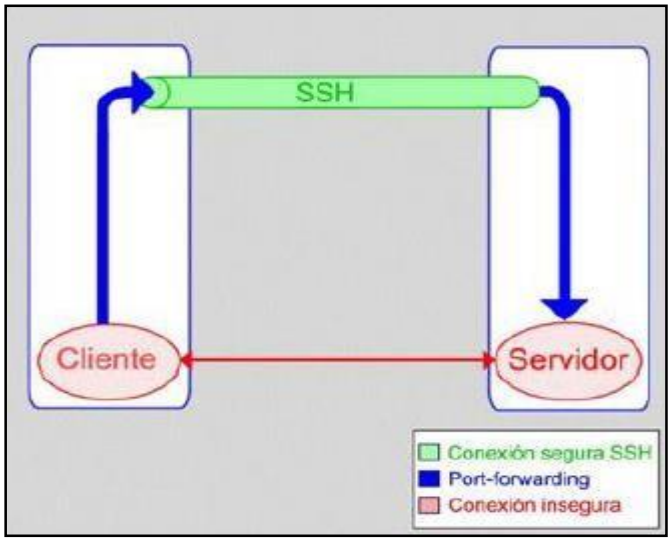


Figura 2.1: Esquema del funcionamiento del SSH
Fuente: juniper

SSH trabaja de forma similar a como se hace con telnet. La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible y ninguna tercera persona pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión.

2.2.3 Equipo firewall de seguridad (Juniper)

Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cuál de los servicios pueden ser aceptados por la red, es decir quién puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración. Lamentablemente, este sistema no puede ofrecer protección alguna una vez que el atacante pasa esta barrera o permanece en ella.

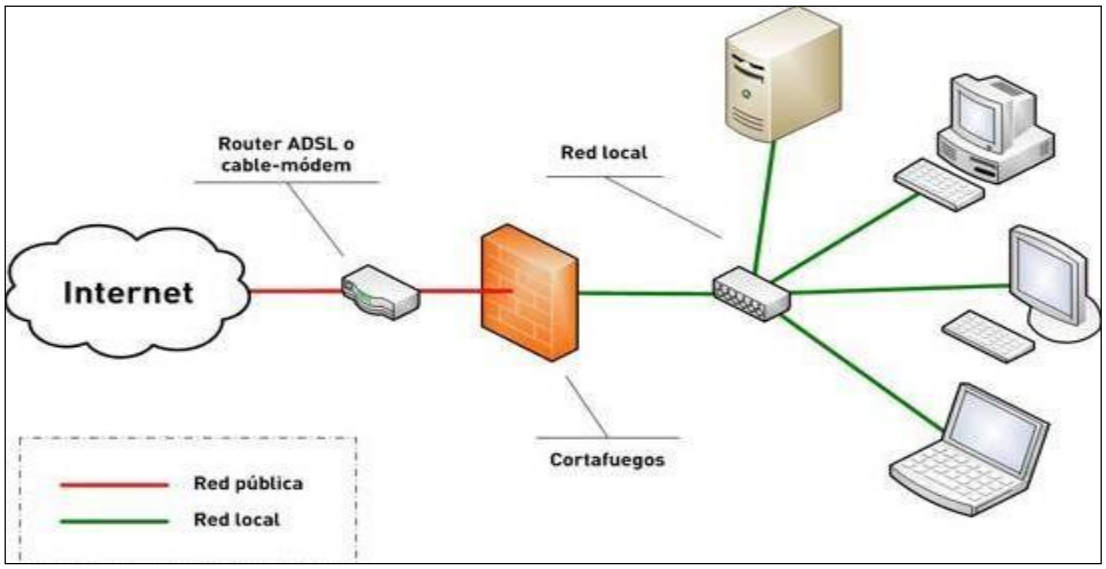


Figura 2.2: Esquema de una red protegida por un firewall
Fuente: juniper

Objetivos del Firewall

El firewall se encarga de controlar puertos y conexiones, es decir, de permitir el paso y el flujo de datos entre los puertos, ya sean clientes o servidores. Es como un semáforo que, en función de la dirección IP y el puerto (entre otras opciones), dejará establecer la conexión o no siguiendo unas reglas establecidas.

De este modo, el firewall controla qué combinaciones "IP Cliente: puerto + IP Servidor: puerto" son válidas o no. Por ejemplo podemos apreciar un esquema en la **figura 2.3**, si el administrador del servidor 222.222.222.222 decide que no quiere que el cliente con dirección IP 111.111.111.111 vea su página web desde casa, podría indicarle a su firewall en el servidor que bloquee esa dirección IP y no le permita acceder a su puerto 80.

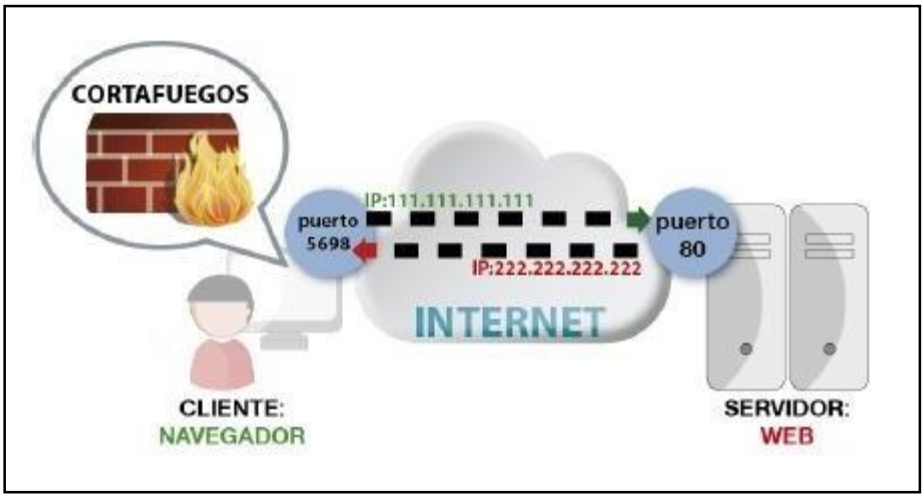


Figura 2.3: Esquema de protección a un servidor
Fuente: juniper

Zona de Seguridad

Una zona es una colección de uno o más segmentos de la red que comparten los requisitos de seguridad idénticos. Para los segmentos de red del grupo dentro de una zona, debe asignar interfaces lógicas desde el dispositivo a una zona.

Las zonas permiten la segregación de seguridad de red. Las políticas de seguridad se aplican entre las zonas para regular el tráfico a través de la seguridad plataforma que ejecuta el sistema operativo Junos. Por defecto, todas las interfaces de red pertenecen a la zona nula definida por el sistema. Todo el tráfico hacia o desde la zona nula se rechaza. Interfaces especiales, incluyendo la gestión de la interfaz Ethernet presente en fxp0 algunas plataformas SRX Series, interfaces de tela clúster de chasis, y las interfaces del sistema em0 internos no pueden ser asignados a una zona.

Zonas e Interfaces

Puede asignar una o más interfaces lógicas a una zona. También puede asignar una o más interfaces de lógicas a una instancia de enrutamiento.

No se puede asignar una interfaz lógica a múltiples zonas o múltiples instancias de enrutamiento. También debe asegurarse de que todos los de una zona es interfaces lógicas están en una sola instancia de enrutamiento.

Tipos de zona de seguridad

Las zonas dentro del sistema operativo Junos se pueden subdividir en dos categorías definidas por el usuario y definida por el sistema. Puede configurar zonas definidas por el usuario, pero no se puede configurar zonas definidas por el sistema. Se puede subdividir la categoría definida por el usuario en la seguridad y zonas funcionales. Este grafico lo podemos observar en la **figura 2.3**

Security zones

Las zonas de seguridad son una colección de uno o más segmentos de red que requiere regulación del tráfico entrante y saliente a través del uso de políticas. La seguridad en las zonas se aplica al tráfico de tránsito, así como el tráfico destinado a cualquier interfaz perteneciente a la zona de seguridad. Son necesario una o más políticas de seguridad para regular la intra-zona y el tráfico interzonal.

Functional zones

Las zonas funcionales son zonas de propósito especial que no se pueden especificar en las políticas de seguridad. Tenga en cuenta que el tráfico en tránsito no utiliza zonas funcionales. Mientras que la interfaz Ethernet gestión fxp0 está fuera de banda por defecto, la zona de gestión que permite asignar otras interfaces de red el mismo comportamiento de aislar el tráfico de gestión del tráfico de tránsito.

ZoneNull

Actualmente existe una sola zona definida por el sistema, la zona Null. Por defecto, todas las interfaces pertenecen a la zona Null. No se puede configurar dicha zona. Cuando se elimina una interfaz de una zona, el software asigna de nuevo a la zona Null. El sistema operativo Junos rechaza todo el tráfico hacia y desde las interfaces que pertenece a la zona Null.

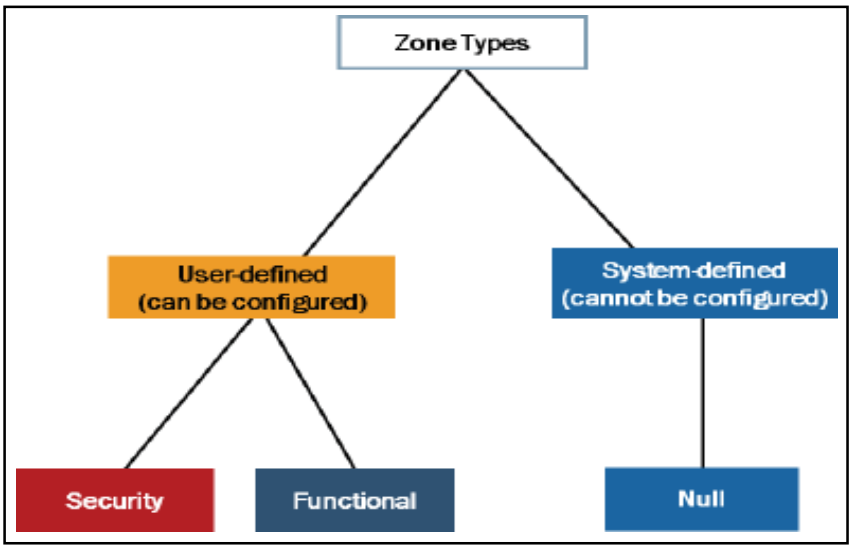


Figura 2.4: Esquema de los tipos de zona
Fuente: juniper jncis-sec

Políticas de Seguridad

Una política de seguridad es un conjunto de instrucciones que controla el tráfico de una fuente específico a un destino específico utilizando un determinado Servicio. Si llega un paquete que coincida con esas especificaciones, el dispositivo de la serie SRX realiza la acción en la póliza. Las políticas de seguridad de la red son de gran valor para la funcionalidad de red segura. Las políticas de seguridad de red contorno de toda la red recursos dentro de una empresa y el nivel de seguridad requerido para cada recurso. El sistema operativo Junos proporciona un conjunto de herramientas para poner en práctica una política de seguridad de la red dentro de su organización. Hace cumplir las políticas de seguridad de un conjunto de reglas para el tráfico de tránsito, identificar las que el tráfico puede pasar a través del servidor de seguridad y las medidas tomadas en el tráfico a medida que pasa a través del firewall.

El sistema operativo Junos para las plataformas de seguridad siempre se examina el tráfico de tránsito mediante el uso de políticas de seguridad. Como se ilustra en el gráfico, en caso de

Ningún resultado existe en la política de seguridad, la política de seguridad predeterminada se aplica al paquete como podemos apreciar en la **figura 2.5**.

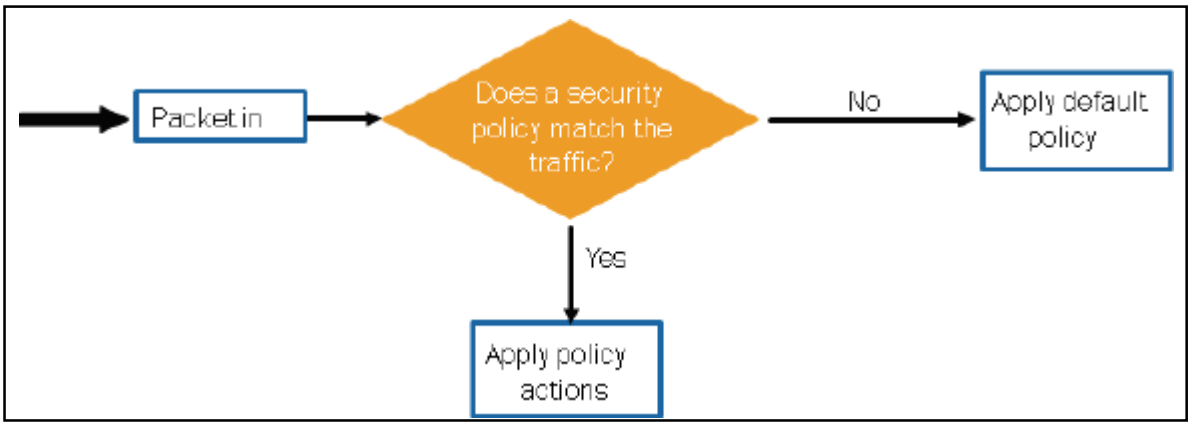


Figura 2.5: Esquema de la exanimación del paquete
Fuente juniper jncis-sec

Políticas de seguridad por defecto.

En la configuración por defecto de fábrica en las plataformas tiene tres políticas de seguridad pre configuradas las cuales son:

1. *Trust-to-trust zonepolicy*: Permite todo el tráfico intra-zona dentro de la zona de confianza;

2. *Trust-to-untrustzonepolicy*: Permisos de todo el tráfico de la zona Trust a la zona Untrust; y

3. *Untrust-to-trust zonepolicy*: niega todo el tráfico de la zona Untrust a la zona Trust.

Contextos de políticas de seguridad.

Al definir una política, debe asociarlo con una zona de origen, cuyo nombre este en la zona. Además, debe definir una zona de destino. Dentro de una dirección de las zonas de origen y de destino, puede definir más de una póliza, se refiere como un conjunto ordenado de las políticas, que el sistema operativo Junos se ejecuta en el orden de su configuración.

Recordemos que una zona es una colección de múltiples interfaces lógicas con los requisitos de seguridad idénticos. El sistema operativo Junos siempre comprueba todo el tráfico de tránsito intra-zona-y-interzona mediante el uso de políticas de seguridad.

Componentes de una política de seguridad.

Dentro del título del contexto definido, cada política está marcada con un nombre definido por el usuario, el nombre definido por el usuario es una lista de coinciden con los criterios y las acciones especificadas, similar a un Junos política de enrutamiento. Una diferencia importante es que cada política de seguridad debe contener una dirección de origen coincidente, dirección de destino y aplicación. Acciones para tráfico que coincide con los criterios especificados incluir permiso, negar, rechazar, registro, o contar.

El sistema operativo Junos también utiliza la política para invocar la aplicación de políticas de prevención y detección de intrusión (IDP).

Gestión de características (UTM) para dispositivos de rama y la autenticación de servidor de seguridad.

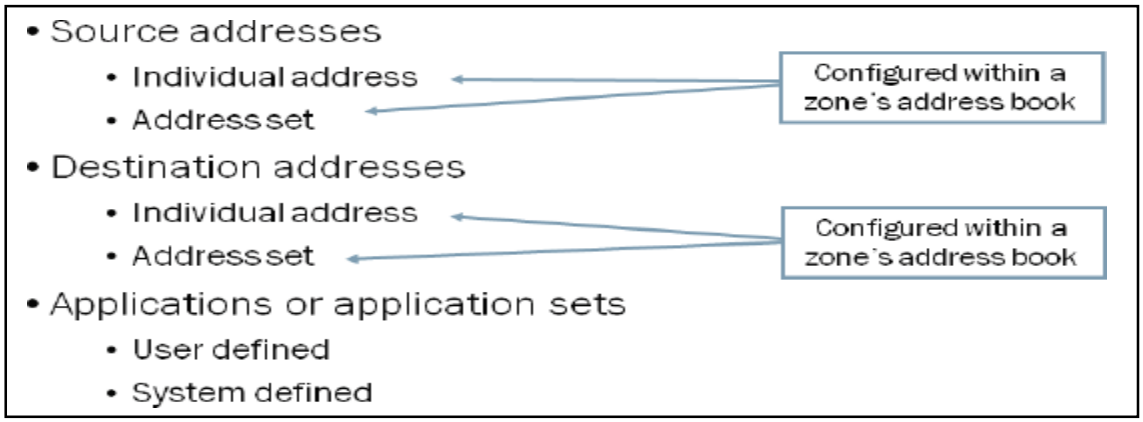


Figura 2.6: Componentes de una política
Fuente: juniper jncis-sec

Cada una de las políticas definidas debe incluir los siguientes criterios:

• Direcciones de origen: Este criterio puede ser en forma de conjunto de direcciones o direcciones individuales. Puede agrupar direcciones individuales en conjuntos de direcciones.

• Direcciones de destino: Este criterio puede ser en forma de conjunto de direcciones o direcciones individuales. Puede agrupar direcciones individuales en conjuntos de direcciones.

• Las aplicaciones o conjuntos de aplicaciones: Este criterio puede ser definida por el usuario o por el sistema. Los soportes del sistema operativo Junos de aplicaciones por defecto y los conjuntos de aplicaciones, se hace referencia con el formato junos-aplicación, donde la aplicación es el nombre de la aplicación real. También podemos definir nuestras propias aplicaciones.

Acciones básicas de una política.

Cada política tiene una lista de acciones básicas asociadas con ella. Las acciones son las siguientes:

• Permit: Permite que el flujo de tráfico;

• deny: Resultados en una caída de paquetes.

• reject: Resultados en una gota de paquetes y el envío de un mensaje de control de Internet Protocolo (ICMP) inalcanzable mensaje para el tráfico UDP y el mensaje de un tiempo de opresión de registro TCP reset (RST) para el tráfico TCP.

Programación de una política.

Es un método para programar una ejecución de políticas para una duración especificada o un conjunto de duraciones.

Un planificador de la política es opcional y puede ser compatible con la hora del sistema actualizaciones ya sea a través de una configuración manual o mediante el Protocolo (NTP) con sincronización en sí con los cambios de tiempo.

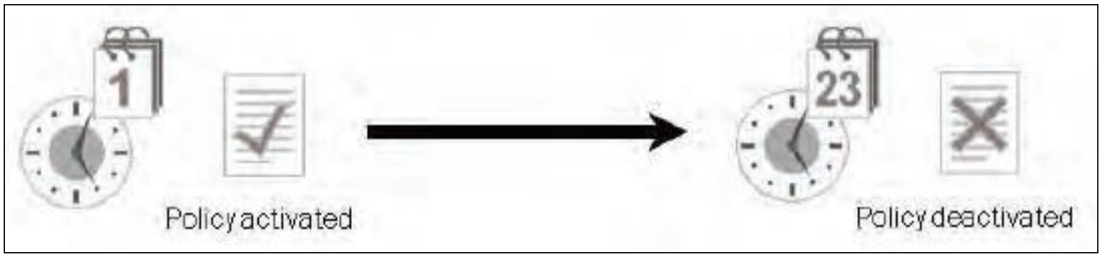


Figura 2.7: Esquema de tiempo en una política
Fuente: juniper jncis-sec

Autenticación de usuarios en el firewall.

La autenticación de usuario en el Firewall proporciona otra capa de protección en la red en la parte superior de las zonas de seguridad, políticas y pantallas.

Con la autenticación de servidor de seguridad, puede restringir o permitir a los usuarios de forma individual o en grupos que intentan acceder a una red

Recibirá una pregunta recursos del sistema operativo Junos un nombre de usuario y contraseña, incluso si una política de seguridad está en su lugar permitiendo el tráfico.

Los usuarios pueden ser autenticados con una base de datos local de contraseñas o el uso de una base de datos de contraseña externa. Los soportes del sistema operativo Junos RADIUS, Lightweight Directory Access Protocol (LDAP) o servidores de autenticación SecurID.

El ejemplo de la **figura 2.7** ilustra un usuario (host A) intentar acceder a un recurso de red que pertenece a la zona pública. Con autenticación de usuario firewall configurado, el usuario debe

autenticarse en primer lugar con la plataforma de seguridad antes de acceder al recursojunos. En este ejemplo, el dispositivo puede consultar un servidor de autenticación externo para determinar el resultado de la autenticación. Las políticas de seguridad también debe permitir el flujo de tráfico. Una vez que el usuario recibe la autenticación, sesiones posteriores de la misma fuente dirección IP de derivación de autenticación de usuario del firewall. Este comportamiento es especialmente importante cuando se considera el uso del firewall de autenticación tiene su origen basado en el Network AddressTranslation (NAT) empleado.

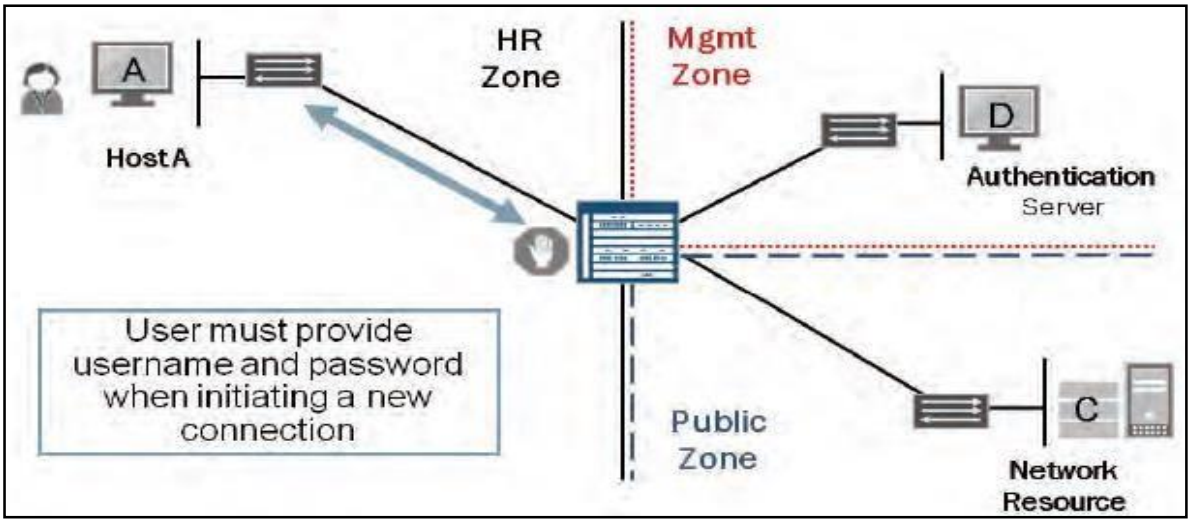


Figura 2.8: Esquema del proceso de autenticación
Fuente: juniper jncis-sec

Pasos a través de la autenticación.

Hay dos tipos de autenticación de firewall disponibles; a través de pasos o autenticación Web. El primero es provocado por el tráfico de Telnet, FTP o protocolo de transferencia de hipertexto (HTTP). En este tipo de autenticación de servidor de seguridad, el usuario inicia una sesión en un dispositivo de red remoto o recurso. Si el tráfico coincide con la política de seguridad configurado para de paso a través la autenticación, la puerta de enlace de servicios de la serie

SRX intercepta la sesión. El usuario recibe una solicitud de un nombre de usuario y contraseña. Si la autenticación es satisfactoria, el tráfico subsiguiente de la misma dirección IP de origen se le permite que automáticamente pase a través del dispositivo, siempre que coincida con la política de seguridad aplicada.

Autenticación web.

La autenticación Web es válido para todos los tipos de tráfico. Con la autenticación Web configurado, los usuarios deben acceder directamente a la plataforma de seguridad a través de HTTP. El usuario introduce la dirección o el nombre de host del dispositivo en un navegador Web y luego pedirá un nombre de usuario y contraseña. Si la autenticación es satisfactoria, el usuario puede tener acceso al recurso restringido directamente. El tráfico subsiguiente de la misma dirección IP de origen se le permite automáticamente el acceso al recurso restringido, siempre y cuando política de seguridad lo permite.

Autenticación local.

El sistema operativo Junos soporta la autenticación local en la misma plataforma de seguridad de Junos, así como RADIUS, LDAP y servidores de autenticaciónexternos SecurID. La base de datos de contraseñas local es compatible con la autenticación y autorización.

Autenticación RADIUS.

El sistema operativo Junos soporta RADIUS para la autenticación y la autorización. La plataforma de seguridad Junos actúa como un cliente RADIUS y utiliza la comunicación UDP. RADIUS utiliza una clave secreta compartida para cifrar la información del usuario durante el intercambio.

Autenticación LDAP.

Un servidor LDAP es otra forma de servidor de autenticación externo. El sistema operativo Junos sólo es compatible con la autenticación cuando se utiliza un servidor LDAP. El sistema operativo Junos es compatible con la versión 3 de LDAP y Microsoft Active Directory de Windows.

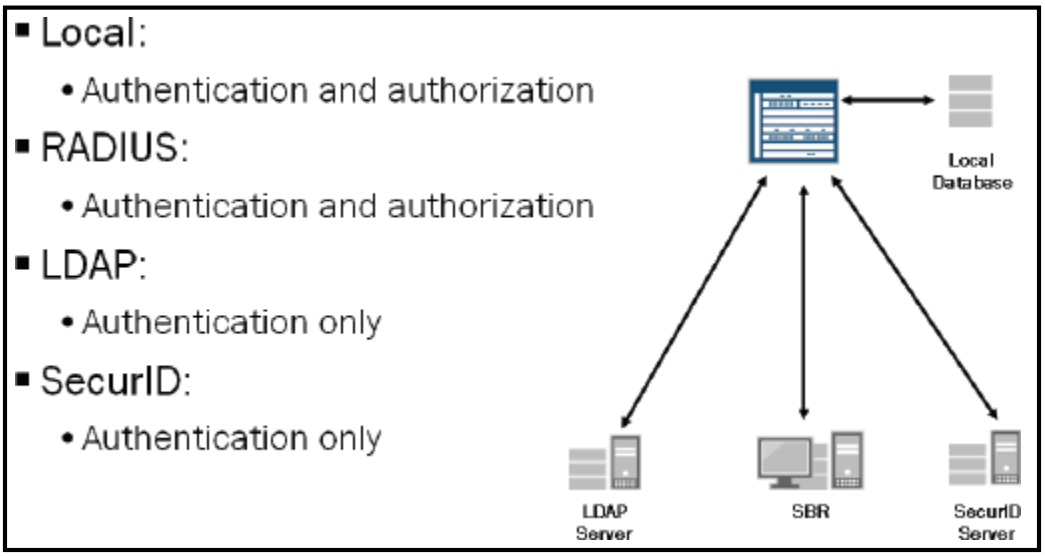


Figura 2.9: Esquema de tipos de autenticación
Fuente: juniper jncis-sec

Alta disponibilidad (Clustering).

El sistema operativo Junos (HA) proporciona una alta disponibilidad de conmutación por error de sesión. Esta capacidad se aplica a las sesiones TCP y UDP de aquellos que despliegan Network AddressTranslation (NAT), seguridad IP (IPsec), o la autenticación, así como aquellos que no lo hacen.

La alta disponibilidad incluye la sincronización de los archivos de configuración y las dinámicas de los estados de sesión de tiempo de ejecución entre plataformas Junos de seguridad

implementados. La aplicación Junos de clustering de alta disponibilidad es compatible actualmente con una activa-pasiva redundancia para el plano de control y una redundancia activa-activa para el plano de datos.

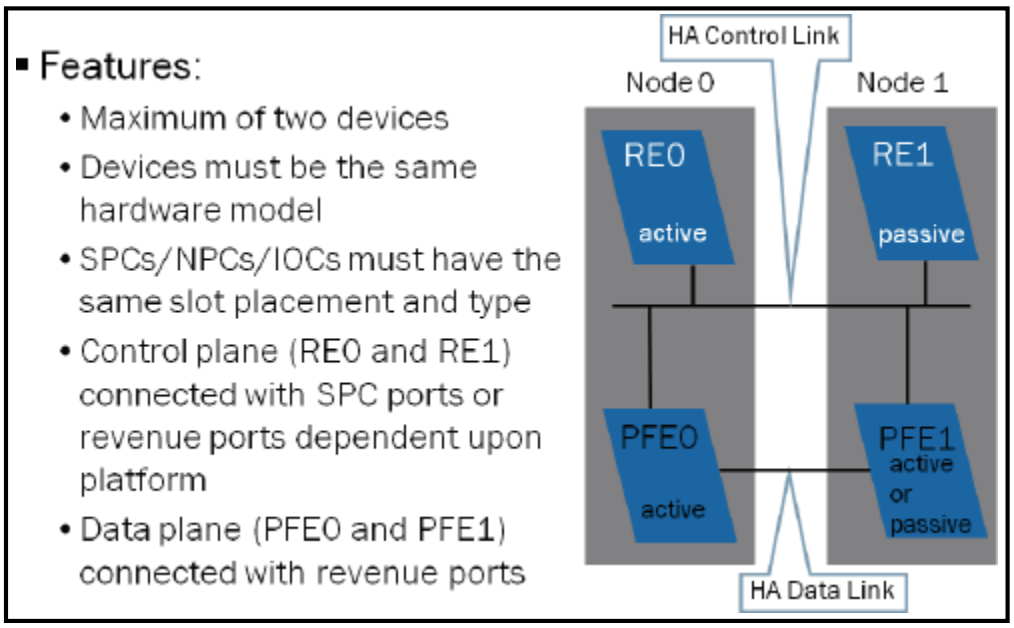


Figura 2.10: Diseño lógico de un clúster
Fuente: juniper jncis-sec

Componentes de un cluster.

Un chasis clúster se compone de los siguientes componentes:

• Identificación de clústeres, incluyendo la ID de clúster-id e Identificación del nodo;

• Los grupos de redundancia (RGs); y

• Interfaces de cluster:

- Fxp1: La interfaz de plano de control;

- Fxp0: El fuera de la banda de la interfaz de gestión;

- Fab: La interfaz de plano de datos;

- Swfab: La interfaz de plano de datos de conmutación; y

- Reth: Una interfaz de redundancia.

Conjunto UTM.

Una red actual contribuye de manera significativa a la línea de fondo y es fundamental para una organización de éxito. Las sucursales incluyen normalmente un número relativamente pequeño de los recursos informáticos en comparación con el centro instalaciones o sedes. Las sucursales se encuentran normalmente en donde se producen interacciones con los clientes, lo que significa que es la creciente demanda de aplicaciones de soporte y asegurar el rendimiento de aplicaciones, un aumento de la demanda de seguridad.

Existen vulnerabilidades de seguridad generales para cada red de oficinas. Estas vulnerabilidades incluyen ataques de spam y phishing, virus, troyanos y spyware, archivos infectados de acceso web no aprobado, y de contenido no autorizado.

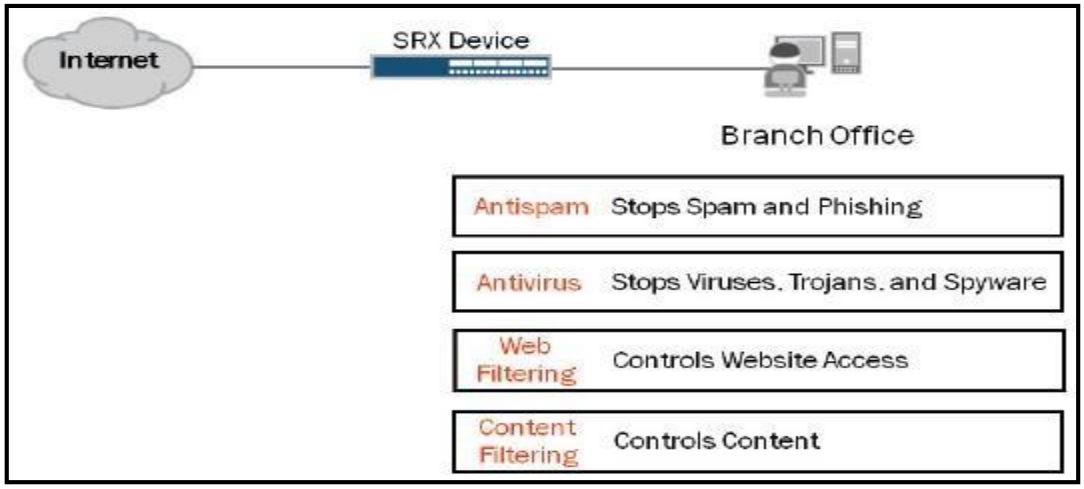


Figura 2.11: Esquema del contenido UTM
Fuente: juniper jncis-sec

La característica del UTM es que proporcionan seguridad en los dispositivos de la gama SRX, lo que permite a una empresa para protegerse de correo no deseado, virus, gusanos, software espía, troyanos, y malware. Con UTM, se puede implementar un conjunto completo de características de seguridad que incluyen antispam, antivirus, filtrado Web y protección de filtrado de contenido. Estas características UTM proporcionan la capacidad de prevenir las amenazas a la puerta de entrada de los SRX antes que estas amenazas ingresen a la red.

2.2.4 Administrador de Ancho de Banda (Allot).

En los últimos años la creación de servicios en la Nube, la masificación de la telefonía y colaboración basadas en IP, han repercutido seriamente en el modo de trabajo y cambiado la forma en que utilizamos la red. De este modo, el concepto que conocemos como Ancho de Banda pasa a ser un recurso escaso por el cual compiten usuarios, servicios y aplicaciones.

Entendiendo que el protocolo TCP/IP se refiere al tránsito desordenado de múltiples paquetes a través de una autopista limitada en la cual, sólo un paquete puede ser transportado a la vez. Se hace importante determinar el orden en que éstos son transmitidos y dar prioridad a aquellos más importantes para el que hacer de la empresa.

Un dispositivo de Control de ancho de banda se encargará de gestionar estos paquetes, ordenándolos según una serie de reglas y parámetros definidos, de manera de asegurar la calidad de servicio a las aplicaciones que más lo necesiten. Podemos por ejemplo, asignar un ancho de banda fijo a la telefonía con el fin de asegurar la calidad de la voz, y a la vez garantizar el acceso a las aplicaciones corporativas. Además de limitar el uso del ancho de banda para el uso de aplicaciones no productivas como redes sociales u otros contenidos.

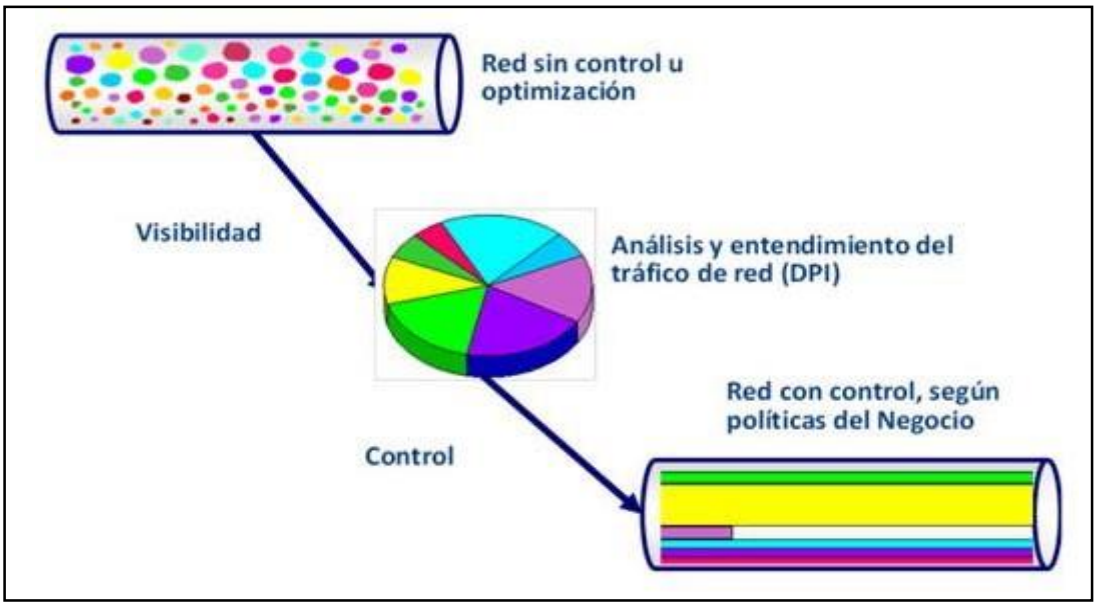


Figura 2.12: Esquema de un optimizador de ancho de banda
Fuente: Pagina allot-oficial

Definición del NetEnforcer.

Un bandwidth manager que recopila las estadísticas y tráfico de la red.

Conjuntamente con el NetXplorer habilita las siguientes características:

- Visualización del tráfico en tiempo real
- Recopilación de la información a largo plazo para la representación de reportes.
- Aplicación de policías.

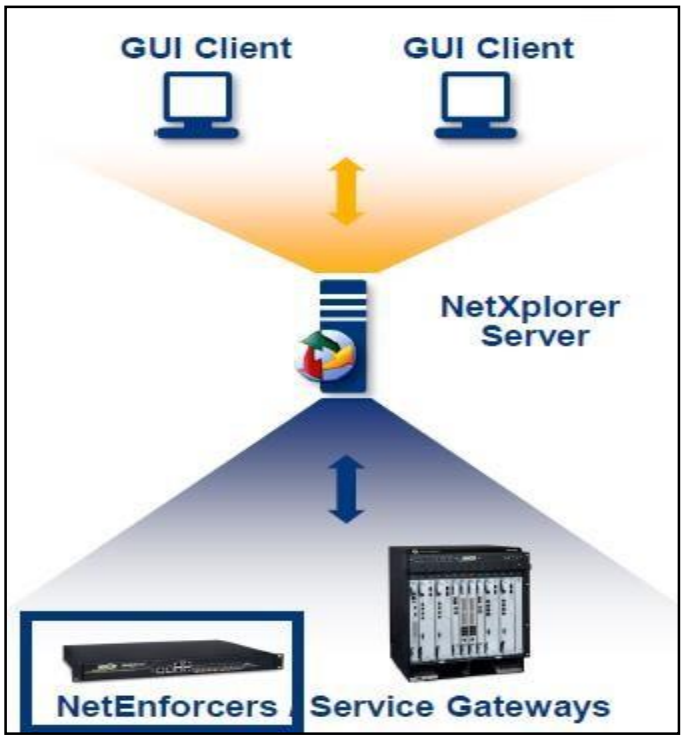


Figura 2.13: Esquema del NetEnforcer
Fuente: Pagina allot-oficial

Definición del NetXplorer.

El NetXplorer te permite lo siguiente:

- Configuración de las políticas de ancho de banda
- Reportes de planificación a largo plazo para el análisis y solución de problemas en la red.
- Monitoreo en tiempo real para la solución inmediata en la red.
- Alertas del tráfico y del sistema.
- Recopilación de la información y exportación para efectos de mejoras.

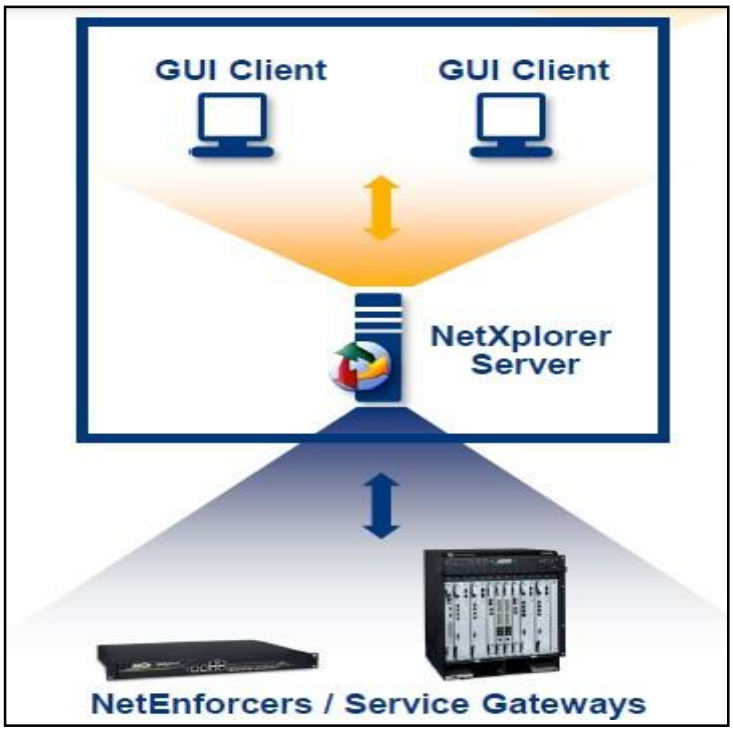


Figura 2.14: Esquema del NetXplorer
Fuente: Pagina allot-oficial

Funcionalidades de Bandwidth Manager

Visibilidad e Inteligencia de Red

- Troubleshooting de red y análisis de tendencias.
- Completo control de aplicaciones.
- Firmas definidas por el usuario en HTTP.
- Monitorización y filtrado de URLs.
- Gestión de ancho de banda (QoS).
- Reglas dinámicas adaptativas.

Solución del Bandwidth Manager en la Red

Único producto de alto rendimiento que no se degrada con el número de conexiones

- Líder en control de P2P.
- Sistema muy potente de informes.
- Control de tráfico no deseado.
- Control de número de conexiones por IP y ancho de banda.

2.2.5 Equipos a implementar.

Media Converter.

RC512-FE 10 / 100M convertidor de medios es diseñada para acceder a suscriptores de banda ancha en el borde de la red troncal IP. Es un puente la brecha de ancho de banda entre TDM tradicional circuitos y núcleo IP al proporcionar a medida ancho de banda de 32 K a 100 Mbps. Gracias al despliegue de tales convertidor de medios de comunicación, servicios de ancho de banda-sed como IPTV y Video Conferencia fueron posibles.

RC512 convertidor de medios de la serie realiza la conversión de medios entre el 10 / 100M de cobre líneas y enlaces de fibra 100M, que se extiende de manera efectiva una distancia de transmisión de Ethernet de 100 metros 120 km (necesidad de personalización).

Su robustez y fiabilidad ha hecho muy bien acogida y popular con los transportistas e ISPs.

En la **tabla 2.1** tenemos los diferentes tipos de tarjetas raisecom (media converter) que se emplean para la transmisión de datos, internet y telefonía respectivamente, además en dicha tabla

encontramos parámetros principales como al potencia, longitud de onda, tipo de fibra con la que funcionan, entre otras características.

Figura 2.15: Equipo Media Converter Raisecom
Fuente: Claro Perú

TARJETAS RAISECOM							
TARJETA	DESCRIPCION	CONECTOR	LONG ONDA	DISTANCIA	POT TX	POT RX	Caracteristicas
RC001-NMS1	administracion						
RC001-NMS2	administracion						
RC001-1AC	Chasis remoto para MC 1 slot						
RC001-1D-AC	Chasis remoto para MC 2 slot						
RC512-FE-M	MC FastEthernet MM, hasta 2 Km	SC, MM	1310	0 - 2 km	-18 / -14	-29 / -14	No DyingGasp, 2 hilos, POP/Cliente
RC512-FE-S1	MC FastEthernet SM, hasta 25 Km	SC, SM	1310	0 - 25 km	-15 / -8	-34 / -8	No DyingGasp, 2 hilos, POP/Cliente
RC512-FE-SS15	MC FastEthernetmonofibra 1550, hasta 25 Km	SC, SM	TX 1550 / RX 1310	0 - 25 km	-5 / -0	-30 / -8	No Dying Gasp, 1 hilo, POP
RC512-FE-C-SS13	MC FastEthernetmonofibra 1310, hasta 25 Km	SC, SM	TX 1310 / RX 1550	0 - 25 km	-12 / -3	-30 / -8	No DyingGasp, 1 hilo, Cliente
RC512-FE-SS25	MC FastEthernetmonofibra 1550, hasta 50 Km	SC, SM	TX 1550 / RX 1310	10 - 50 km	-5 / -0	-32 / -10	No Dying Gasp, 1 hilo, POP
RC512-FE-C-SS23	MC FastEthernetmonofibra 1310, hasta 50 Km	SC, SM	TX 1310 / RX 1550	10 - 50 km	-12 / -3	-32 / -10	No DyingGasp, 1 hilo, Cliente
RC602-GE-S1	MC GigaEthernet SM, hasta 25 Km	SC, SM	1310	0 - 25 km	-10 / -3	<-23	No DyingGasp, 2 hilos, POP/Cliente
RC602-GE-SS13	MC GigaEthernetmonofibra 1550, hasta 25 Km	SC, SM	TX 1310 / RX 1550	0 - 25 km	-5 / -0	<-20	No DyingGasp, 1 hilo, Cliente
RC602-GE-SS15	MC GigaEthernetmonofibra 1310, hasta 25 Km	SC, SM	TX 1550 / RX 1310	0 - 25 km	-5 / -0	<-20	No Dying Gasp, 1 hilo, POP
RC602-GE-SS24	MC FastEthernetmonofibra 1550, hasta 50 Km	SC, SM	TX 1550 / RX 1310	10-50 km	-3 / -2	<-20	No DyingGasp, 1 hilo, Cliente
RC602-GE-SS25	MC FastEthernetmonofibra 1310, hasta 50 Km	SC, SM	TX 1310 / RX 1550	10-50 km	-3 / -2	<-20	No Dying Gasp, 1 hilo, POP
RC832-30-BL-M	MC E1 120ohm, MM hasta 2 Km	SC, MM	1310	0 - 2 km	-20 / -14	-28 / -14	DyingGasp, POP/Cliente
RC832-30-BL-S1	MC E1 120ohm, SM hasta 25 Km	SC, SM	1310	0 - 25 km	-15 / -8	-34 / -8	DyingGasp, POP/Cliente
RC832-30-BL-SS15	MC E1 120 ohm, monofibra 1550, hasta 25 Km	SC, SM	TX 1550 / RX 1310	0 - 25 km	-12 / -3	-30 / -8	DyingGasp, POP/Cliente
RC832-30-BL-SS13	MC E1 120 ohm, monofibra 1310, hasta 25 Km	SC, SM	TX 1310 / RX 1550	0 - 25 km	-12 / -3	-30 / -8	DyingGasp, POP/POP
RC832-30-BL-SS25	MC E1 120 ohm, monofibra 1550, hasta 50 Km	SC, SM	TX 1550 / RX 1310	10 - 50 km	-5 / -0	<-32	DyingGasp, POP
RC832-30-BL-SS23	MC E1 120 ohm, monofibra 1310, hasta 50 Km	SC, SM	TX 1310 / RX 1550	10 - 50 km	-12 / -3	<-32	DyingGasp, Cliente
RCMS2802-120LFE-BL-M	MC 4E1&FE, MM, hasta 2 Km	SC, MM	1310	0 - 2 km	-20 / -14	-28 / -14	DyingGasp, POP/Cliente
RCMS2802-120LFE-BL-S1	MC 4E1&FE, SM, hasta 25 Km	SC, SM	1310	0 - 25 km	-15 / -8	-34 / -8	DyingGasp, POP/Cliente

Tabla 2.1: Tarjetas Raisecom y características principales
Fuente: Claro Perú

Router Juniper SRX 220.

El SRX220 Services Gateway consolida seguridad, enrutamiento, switching y conectividad WAN en un dispositivo compatible hasta 950 Mbps firewall, sistema de prevención de intrusiones (IPS) de 100 Mbps y de 100 Mbps IPsec VPN.

La familia de productos de Juniper Networks SRX Series servicios Gateways puede ofrecer protección de firewall de próxima generación con controles de aplicación conocimiento y usuario basada en funciones, además de opciones de administración (UTM) mejor en su clase unificada de amenazas para proteger y controlar los activos de su empresa.

El SRX220 Services Gateway es ideal para la seguridad de empresas pequeñas y medianas y empresas distribuidas localidades.

Figura 2.16: Equipo Juniper SRX 220
Fuente: Datasheet de juniper

CARACTERISTICAS	METRICA
Versión Junos OS Software probado	Junos OS 12.1
Rendimiento Firewall (max)	950 Mbps
Rendimiento IPS	80 Mbps
AES256 + SHA-1 / 3DES + SHA-1 El rendimiento de VPN	100 Mbps
Máximo de sesiones simultáneas	96000
Nuevas sesiones / segundo (sostenido, TCP, de 3 vías)	2800
Políticas de máxima seguridad	2048

Tabla 2.2: Características técnicas de router SRX 220 de Juniper
Fuente Datasheet de juniper

Firewall Juniper SRX-550 Juniper.

Los equipos Juniper SRX550 Gateway es un todo en uno. Se presenta en forma de un dispositivo con dos unidades de rack integrado de seguridad, enrutamiento, conmutación y conectividad WAN. Es compatible con un firewall para un rendimiento máximo de 5,5 Gbit/s, un rendimiento de VPN IPSec de hasta 1 Gb/s e IPS con un rendimiento de hasta 800 Mbit /s.

Figura 2.17: Equipo Juniper SRX-550
Fuente Datasheet de juniper

También incluye la función UnifiedThreat Management (UTM) que consiste en: antivirus, seguridad de aplicaciones, IPS, filtrado Web anti-spam y avanzado. Los Servicios SRX550 Gateway es ideal para asegurar las medianas y grandes filiales.

CARACTERISTICAS	METRICA
Versión Junos OS Software probado	Junos OS 12.1
Rendimiento Firewall (max)	5.5 Gbps
Rendimiento IPS (NSS 4.2.1)	800 Mbps
AES256 + SHA-1 / 3DES + SHA-1 El rendimiento de VPN	1.0 Gbps
Máximo de sesiones simultáneas	375000
Nuevas sesiones / segundo (sostenido, TCP, de 3 vías)	27000
Políticas de máxima seguridad	7256

Tabla 2.3: Características técnicas del firewall SRX 550 de Juniper
Fuente: Datasheet de juniper

Administrador de Ancho de Banda AC-1400 (ALLOT).

AllotNetEnforcer® AC-1400 gestiona el tráfico de Internet en varios enlaces Ethernet a velocidades de hasta 1 Gbps. Este dispositivo flexible proporciona análisis en tiempo real, la aplicación de políticas y de direccionamiento del tráfico para ayudar a la utilización de ancho de banda de control de los operadores y los costes a la vez que garantiza la calidad de experiencia (QoE) para todos los usuarios de la red.

Figura 2.18: Equipo Administrador de ancho de banda SRX-550
Fuente: Datasheet de allot

NetEnforcer Series		Max Throughput	Max Connections	Max Pipes/VCs
400		100 Mbps (Full Duplex)	96,000 (192,000 flows)	1,024 4,096
1400		1Gbps (Full Duplex)	2,000,000 (4,000,000 flows)	40,000 80,000
3000		4 Gbps (Full Duplex)	2,000,000 (4,000,000 flows)	40,000 80,000
5000		7.5 Gbps (Full Duplex)	5,000,000 (10,000,000 flows)	100,000 200,000
10000		15 Gbps (Full Duplex)	10,000,000 (20,000,000 flows)	200,000 400,000

Tabla 2.4: Características técnicas de los NetEnforcer de
Allot Fuente: Allot datasheep

Switch EX2200-24T (Juniper).

Cuenta con capa 2 completa y básica de capa 3, conmutación de capacidades. La línea EX2200 de switches Ethernet de configuración fija con tecnología de Virtual chasis satisface la rama y requerimientos de conectividad además de cableado de baja densidad de hoy para

negocios de alto rendimiento. Cuatro configuraciones de la plataforma están disponibles con 24y puertos 48 10/100/1000BASE-T con o sin Powerover Ethernet (PoE).Los modelos EX2200 incluyen un presupuesto máximo de 405 W para proporcionar hasta 15,4vatios de basados en estándares 802.3af clase PoE 3 o 30 vatios de basados en estándares 802.3atPoE + para apoyar los dispositivos en red tales como teléfonos, cámaras de vídeo, wireless LAN (WLAN) acceder a puntos y teléfonos de video en redes convergentes.

Figura 2.19: Equipo Switch juniper EX2200
Fuente: Datasheet de switch juniper

CARACTERISTICAS	METRICA
Compatibilidad con estándares	Auto MDI/MDIX, Alimentación a Través de Ethernet, con tramas Jumbo
Puerto USB	si
Puerto de consola	si
Número de puertos en el conmutador	48 x Ethernet 10/100/1000 Mbit/s
Número de VLANs	1024

Tabla 2.5: Características técnicas del equipos EX2200 de Juniper
Fuente: Datasheet de switch juniper

2.3 Marco Conceptual

Cluster.

Termino que se utiliza para la alta disponibilidad de los equipos Firewall, se puede utilizar máximo 2 equipos, si hubiera una caída del primer equipo automáticamente pasa el funcionamiento el segundo, con las mismas características del equipo caído. Es un sistema a prueba de fallas, con la finalidad de no perder el servicio hacia internet.

Nodo 0 (Master).

Se le llama así al equipo principal de un clúster, es decir en donde está corriendo todos los servicios y políticas actuales de la red.

Nodo 1 (Backup).

Es el equipo secundario de un cluster, se pone en funcionamiento cuando hay alguna falla o caída del nodo 0, pasando a ser el equipo principal.

Enlace Principal

Es aquel enlace en donde se encuentra el router, es decir por donde actualmente pasa el tráfico de datos en condiciones normales, es decir mientras la red no tenga ningún inconveniente físico o lógico en dicho equipo.

Enlace de Contingencia

Es aquel enlace en donde se encuentra el router de contingencia por donde pasa el tráfico de datos cuando en el enlace principal sufre algún inconveniente de tipo lógico o físico.

Políticas.

Es la parte más importante en la configuración del equipo ya que definimos exactamente el tráfico que queremos de zona a zona, además de los puertos que se quieren habilitar, en esta parte podemos permitir el acceso a un determinado servicio o por el contrario negarlo.

Zonas de Seguridad.

Las zonas de seguridad se definen dependiendo de lo requerido por la entidad , es decir cuántas zonas actualmente maneja por ejemplo las principales son la zona WAN y la zona LAN, aparte de ello tememos la zona DMZ que es de servidores, la zona VPN entre otras.

Address Book.

Este término hace referencia a las direcciones IPs de las diferentes zonas, es decir para poder crear una política de seguridad tenemos que tener la lista de IPspertenecientes a cada zona, estas IPs serán públicas o privadas dependiendo a la zona en la que se llame. Una vez creada la lista de IPs podemos llamarla en la política de seguridad.

BGP (BorderGatweyProtocol)

En comunicaciones, BGP (del inglés *Border Gateway Protocol*), es un protocolo mediante el cual se intercambia información deencaminamiento o ruteo entre sistemas autónomos. Por ejemplo, los proveedores de servicio registrados en internet suelen componerse de varios sistemas autónomos y para este caso es necesario un protocolo como BGP.

Entre los sistemas autónomos de los ISP se intercambian sus tablas de rutas a través del protocolo BGP. Este intercambio de información de encaminamiento se hace entre los routers externos de cada sistema autónomo, los cuales deben soportar BGP. Se trata del protocolo más utilizado para redes con intención de configurar un Exterior Gateway Protocol.

RPVL.

El servicio ofrece a los clientes la posibilidad única de elegir la Clase de Servicio ideal para sus aplicaciones de voz o video y datos, obteniendo así la capacidad de administrar sus recursos de manera eficiente y a la medida de sus necesidades, y por consiguiente la mejor relación coste/beneficio por su inversión en servicios de telecomunicaciones.

Red Privada Virtual proporciona el transporte de cualquier tipo de información en una plataforma única y convergente, donde se puede transmitir voz, video, datos críticos, datos transaccionales y datos generales.

QoS - CoS

Sigla de Quality of Service (Calidad de servicio) es el conjunto de tecnologías que garantiza la transmisión de cierta cantidad de información en un tiempo determinado a uno o varios dispositivos, además que dicha información ocupe cierto ancho de banda designado para tal propósito

ITEM	CoS3	CoS2	CoS1
Tipo de Datos	Voz y Video	Datos Críticos	Datos No críticos
Prioridad	Máxima	Media	Normal
Precedencia / IP DSCP	P5 / IP DSCP 40	P2 / IP DSCP 16	P1 / IP DSCP 8
Política aplicable al tráfico excedente	Se descarta	Se Remarca como P1	No aplica
Aplicaciones	Aplicaciones en Tiempo Real como	Aplicaciones de Datos sensibles al retardo y	Aplicaciones tradicionales como:

	VoIP, Video conferencia	críticas para el negocio como SNA, SAP, ERP.	FTP, E-mail, HTTP.

Tabla 2.6: Clasificación de datos para calidad de servicio
Fuente: Elaboración propia

Bandwith

Es una medida de la capacidad de un canal de comunicaciones en la transmisión del espectro. La medida de capacidad de la línea de un teléfono análogo es medida en Hertz, para canales digitales es medida en bits por segundo (bps).

Line.

Es la política general que se crea en el administrador de ancho de banda, es decir todo el tráfico que viene de la red del cliente, pasa primero por ese filtro la cual se le asocia reglas y ciertas características.

Pipe.

Este término es utilizado en el administrador de ancho de banda (allot), para segmentar el tráficoproveniente del LINE, podemos crear varios Pipe dentro de un Line dependiendo de lo requerido por la entidad, además de asignar un determinado ancho de banda a cada Pipe.

Virtual Channel (VC).

Este término es utilizado en el administrador de ancho de banda (allot), la cual nos indica las aplicaciones o servicios que queremos limitar y están dentro de los Pipe, cada VC creado tiene un determinado valor de QoS que se le asigna en base a lo requerido por la entidad.

CAPÍTULO 3. DISEÑO DE LA TOPOLOGIA DE RED DE DATOS

3.1 ANÁLISIS DEL MODELO DE LA RED DE DATOS.

Actualmente la mayoría de las empresas y entidades poseen una seguridad perimetral con alta disponibilidad, es por ello que se ofrece esta solución en la Superintendencia de Administración Tributaria (SAT), debido a la demanda de usuarios que actualmente posee y a su crecimiento a futuro, además de las necesidades de los clientes que se conectan a los servicios publicados, el diseño de red incluye además el bandwidth Manager que hace una correcta administración de ancho de banda contratado por la entidad, además el diseño incluye una conexión de la sedes remotas del SAT a través de un RPVL, hacia la sede Principal.

En esta topología de red diseñada para el SAT, nos basaremos principalmente en la trasmisión de datos tanto en la sede principal como en sus sedes remotas.

3.1.1 ANALISIS DE LA SOLUCION.

Esta sección detalla el funcionamiento de la solución, La topología que se implementó está basada en la redundancia la cual es fundamental en una red, ya que permite que las redes sean tolerantes a fallas, estas topologías proporcionan protección contra el tiempo de inactividad, o no disponibilidad que puede deberse a la falla de algún enlace.

En la topología implementada para el SAT, la cual se observa en la Figura 3.1 cada equipo dependiendo de la conexión y configuración cumple funcionalidades específicas.

Además se realiza el protocolo de pruebas para poder verificar por donde sale el tráfico ante la caída física o lógica de un equipo.

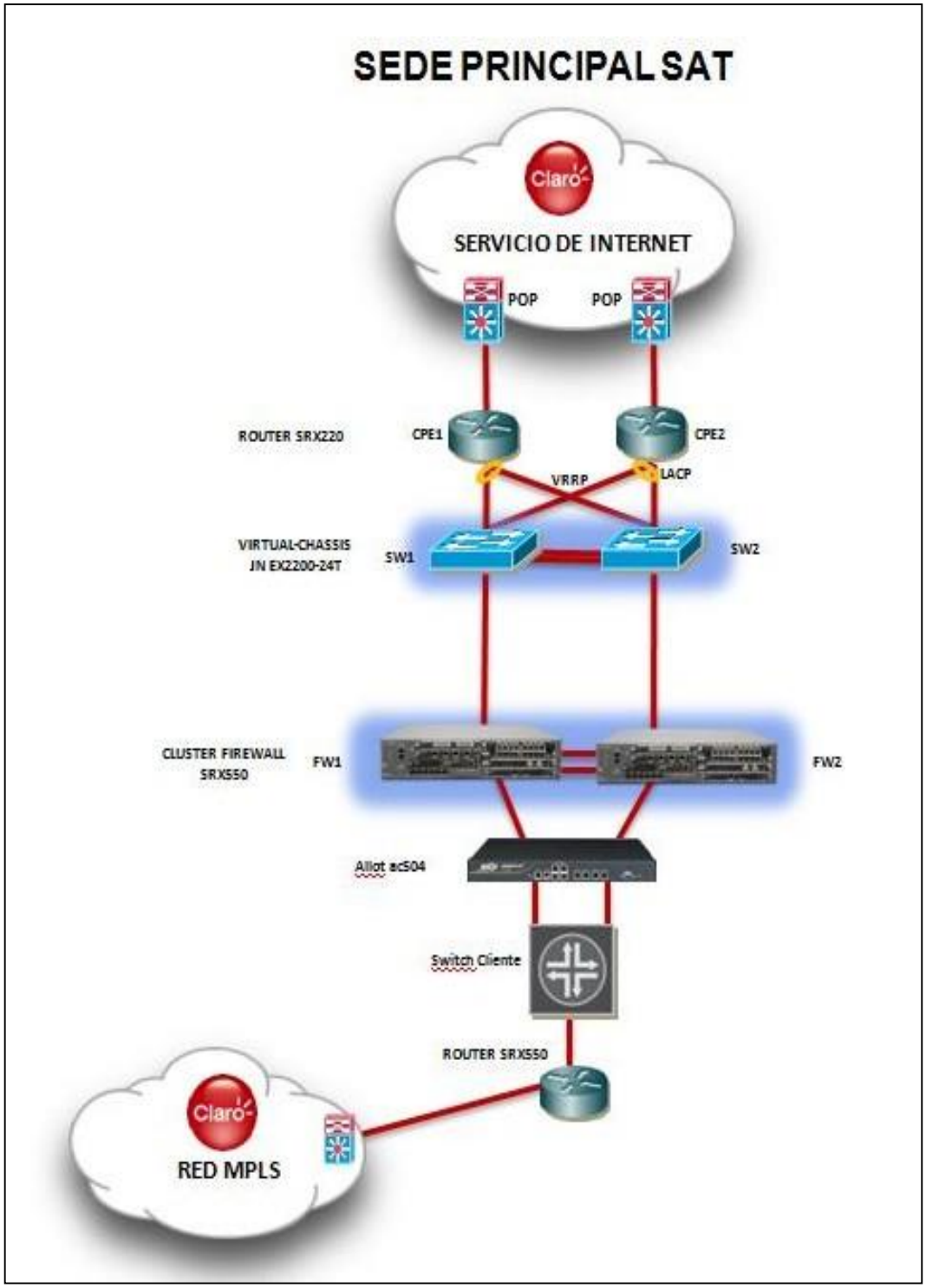


Figura 3.1: Diagrama de la seguridad perimetral en la sede principal
Fuente: Elaboración propia

3.1.2 INTERFACES CONECTADAS EN LOS EQUIPOS.

Todas las interfaces conectada en los equipos son giga Ethernet y están configuradas en una velocidad de auto negociación, para no tener problemas en la comunicación entre los equipos.

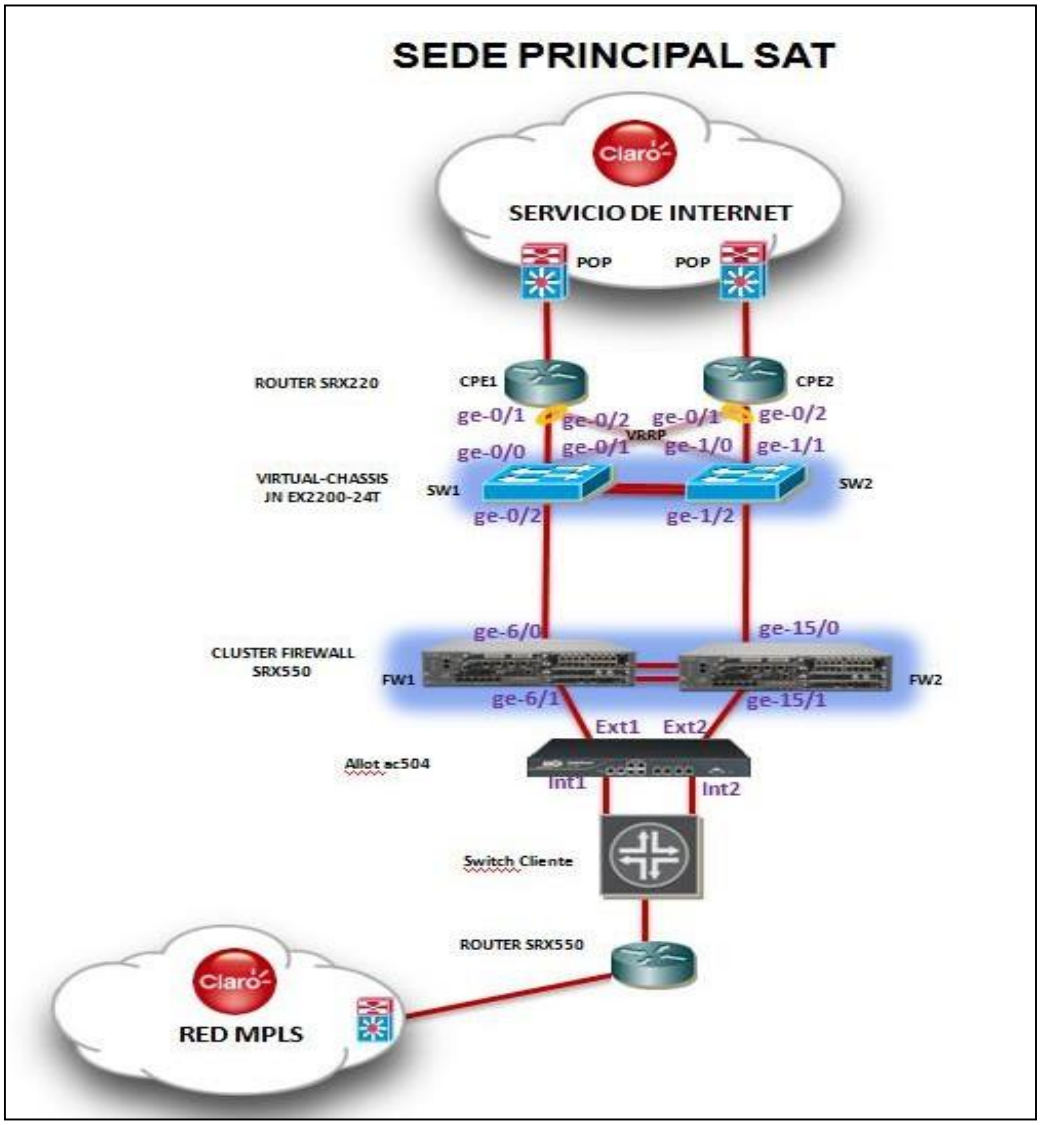


Figura 3.2: Diagrama de las interfaces conectada a los equipos
Fuente: Elaboración propia

3.1.3PROTOCOLO DE PRUEBA DE LOS EQUIPOS INSTALADOS.

Se han configurado los equipos de tal manera que el tráfico valla por el enlace señalado en la figura 3.3.

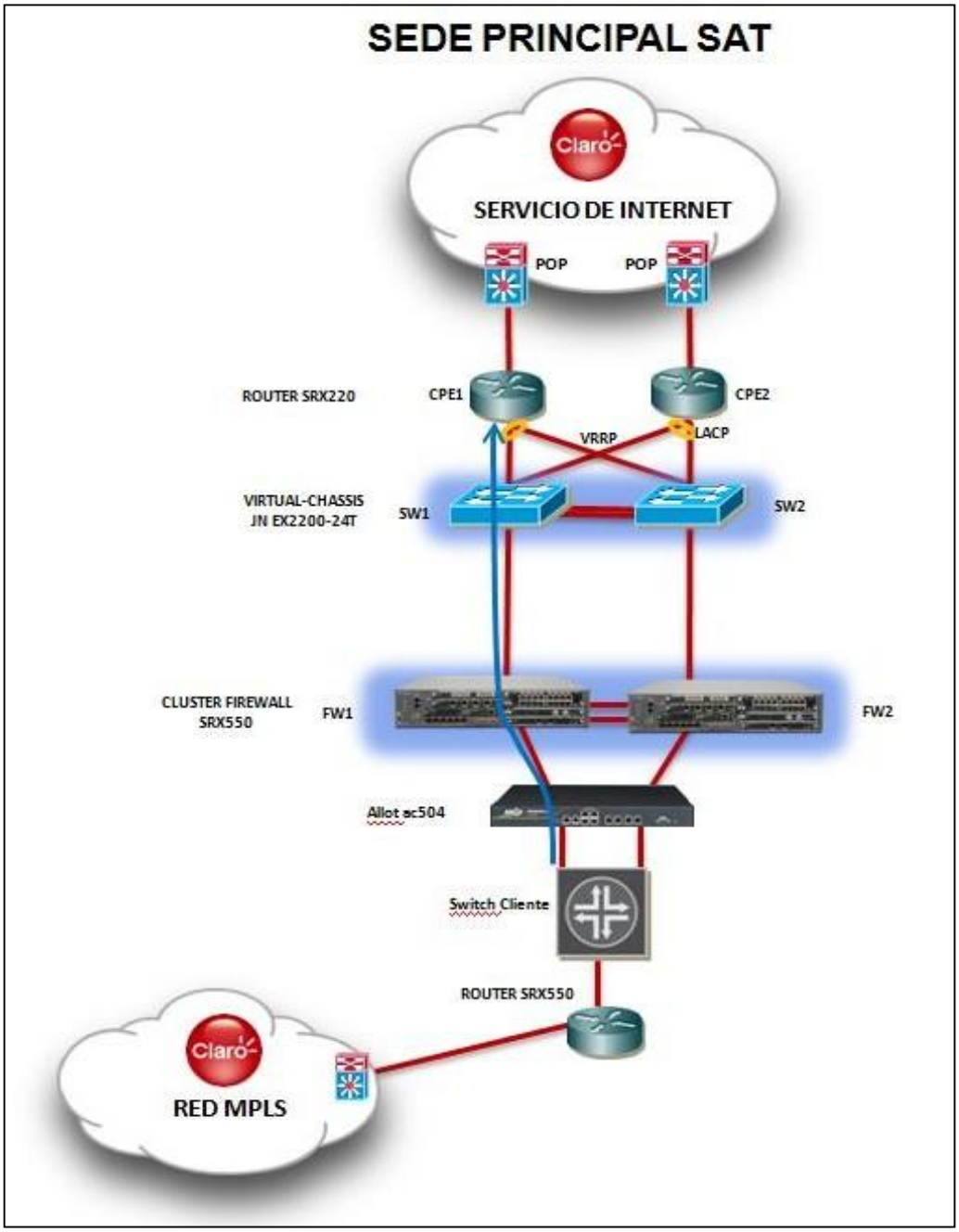


Figura 3.3: Diagrama del tráfico en sede principal
Fuente: Elaboración propia

En caso falle el enlace principal el tráfico es redirigido hacia el otro enlace como se observa en la figura 3.4.

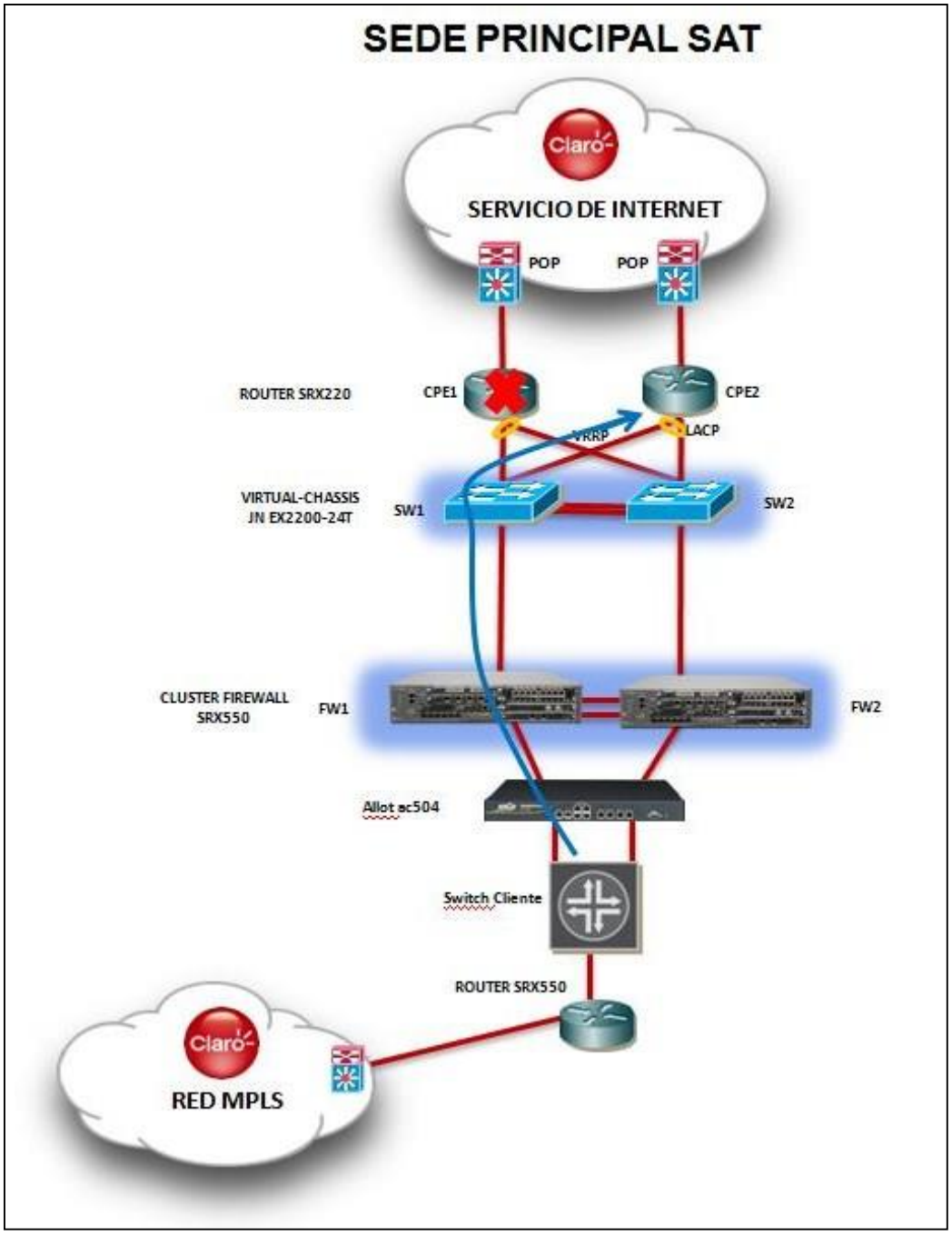


Figura 3.4: Diagrama de caída en el router principal.
Fuente: Elaboración propia

En caso falle uno de los Switches del Virtual Chassis, el Firewall Secundario pasa a tomar el papel de máster haciendo q redirija el tráfico hacia el otro enlace.

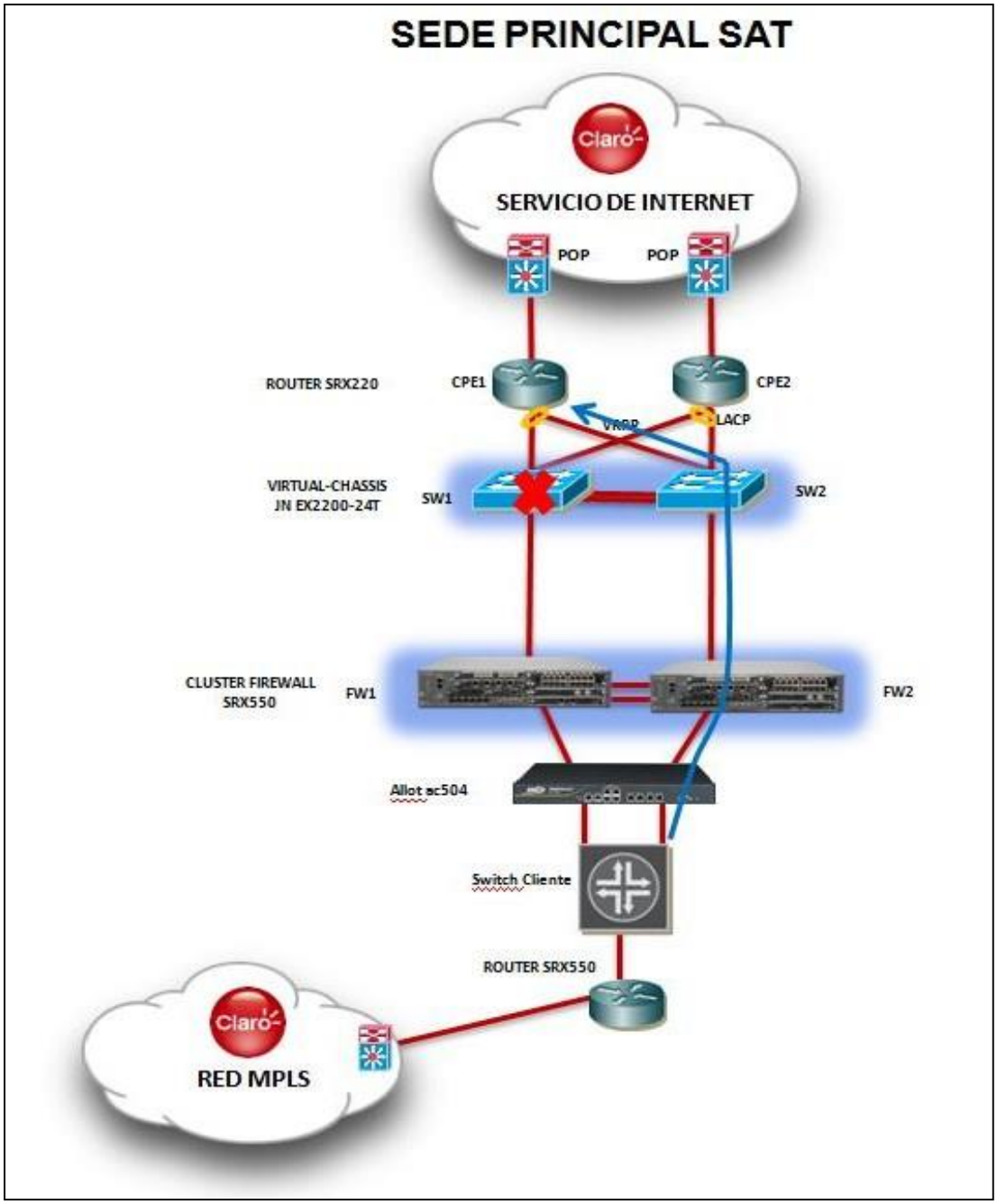


Figura 3.5: Diagrama de caída del SW- Virtual Chassis
Fuente: Elaboración propia.

En caso falle el Firewall Principal, todo el tráfico saldrá por el Firewall Secundario ya que los equipos están en Cluster, haciendo que el flujo hacia internet no se vea interrumpido.

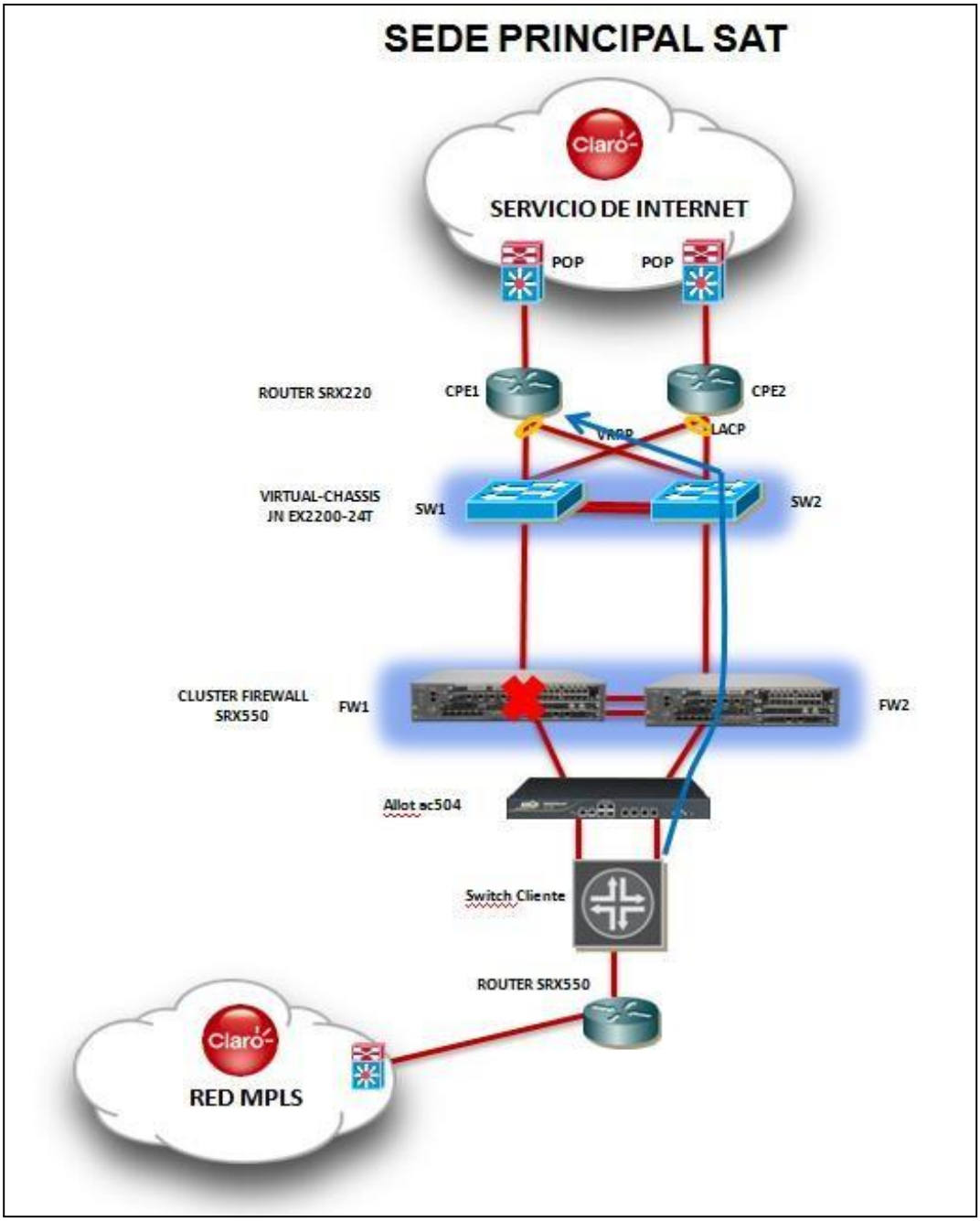


Figura 3.6: Diagrama de caída del Firewall Principal
Fuente: Elaboración propia.

En caso falle el Firewall Secundario, todo el tráfico seguirá saliendo por el Firewall Principal ya que los equipos están en Cluster, haciendo que el flujo hacia internet no se vea interrumpido.

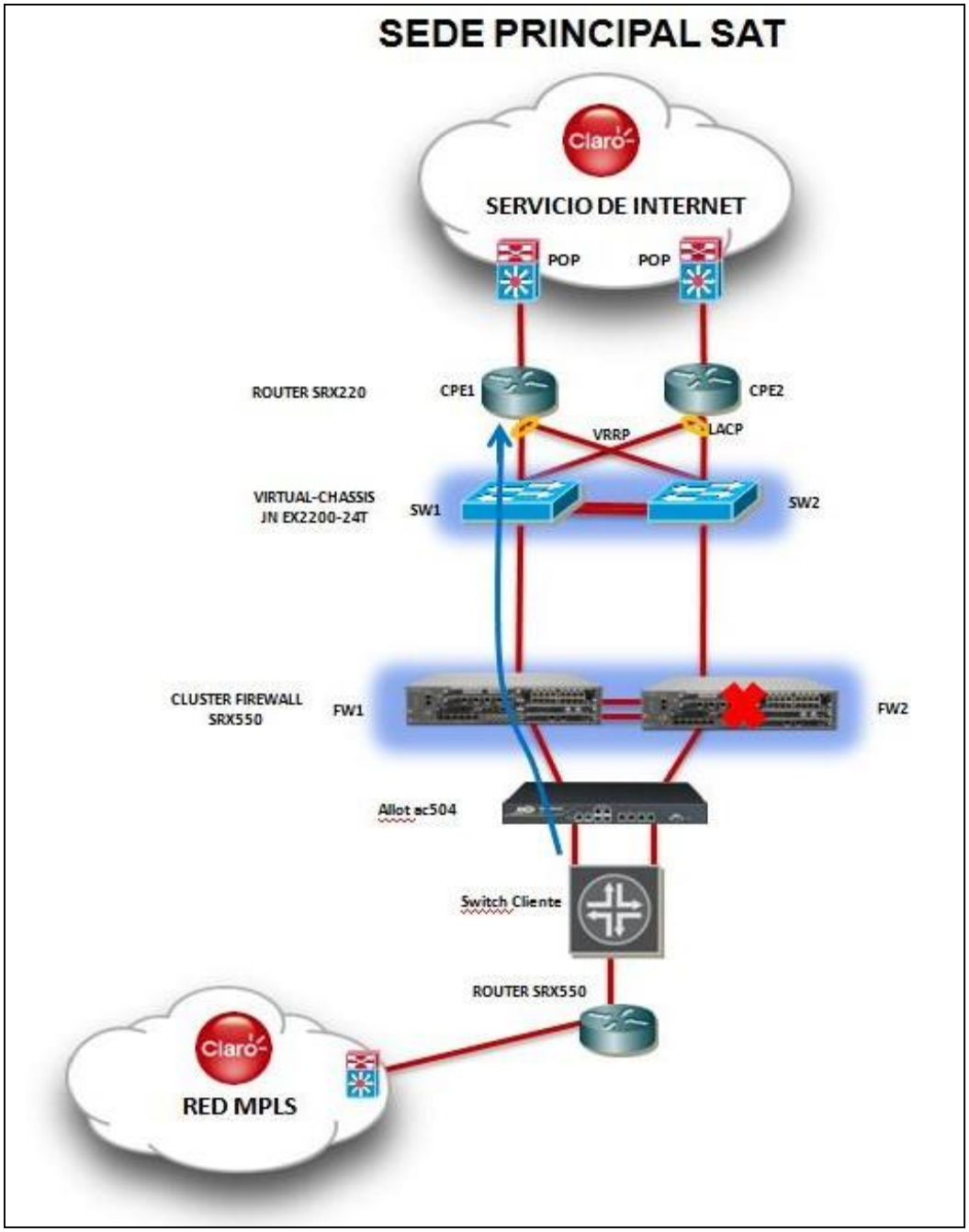


Figura 3.7: Diagrama de caída del Firewall Secundario
Fuente: Elaboración propia.

En caso falle el Allot el flujo de tráfico no se verá interrumpido por la funcionalidad Bypass que tienen dichos equipos.

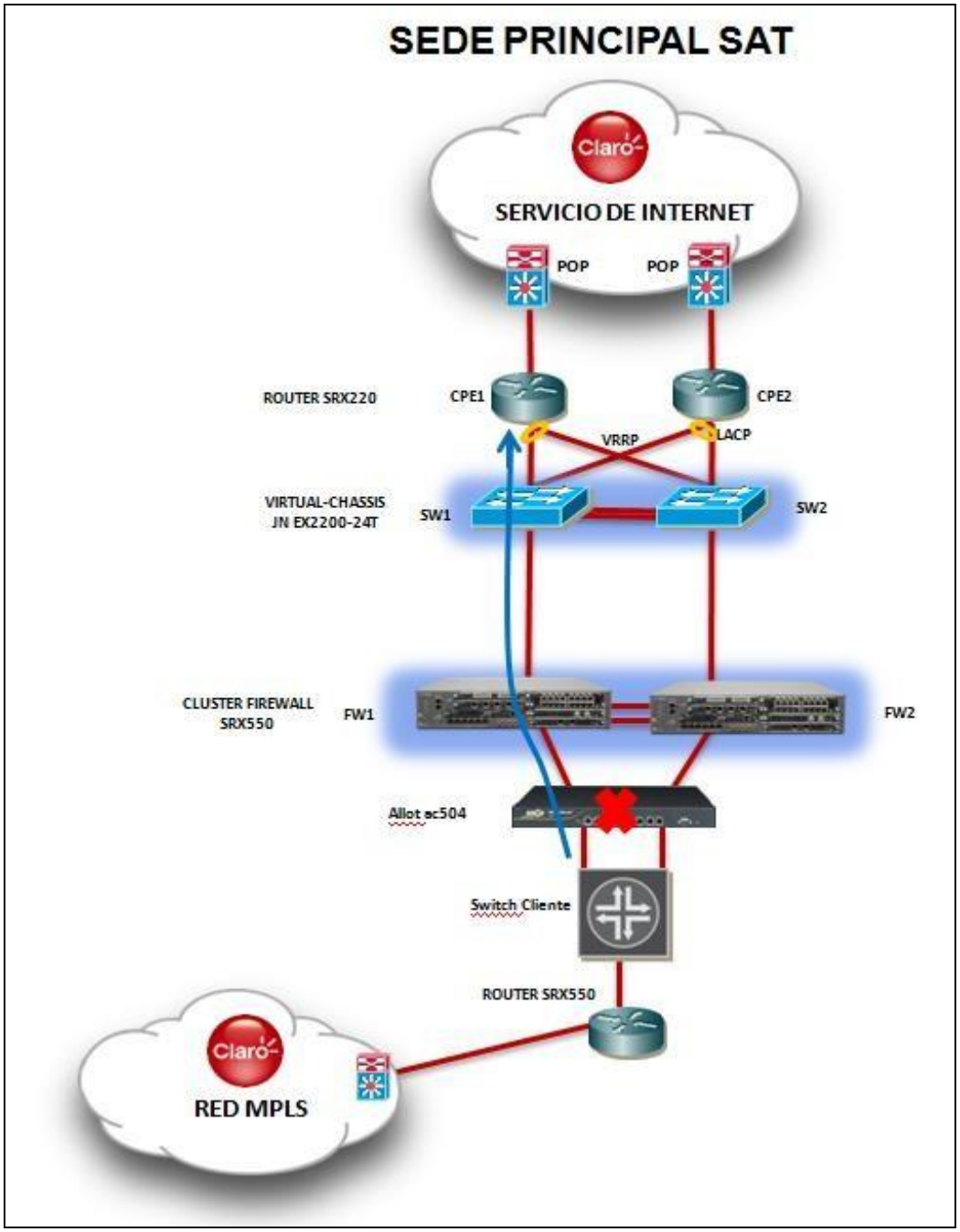


Figura 3.8: Diagrama de caída del Administrador de Ancho de Banda (ALLOT)
Fuente: Elaboración propia.

3.1.4 DIAGRAMA DE RED DE LAS SEDES REMOTAS (AGENCIAS).

El diagrama muestra las 5 agencias interconectadas a través de la rpv con la sede principal, además de su dirección tanto Lan como Wan, lookback y la cantidad de ancho de banda asignada para cada Cos.

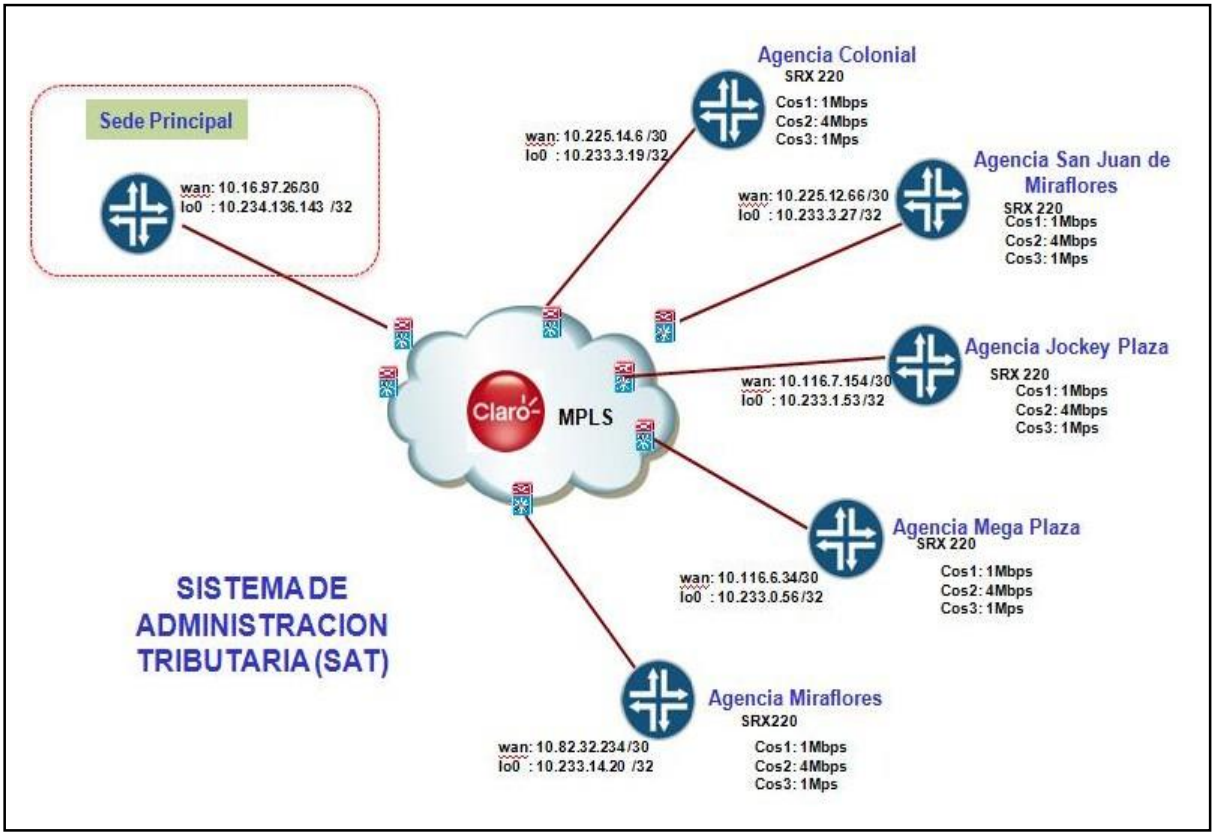


Figura 3.9: Diagrama de sedes remotas
Fuente: Elaboración propia.

3.1.5 CARACTERISTICAS DEL PROYECTO.

La propuesta tecnológica ofrecida al SATestá diseñada para los siguientes servicios y soluciones:

- Disponer de un sistema con seguridad en la red, definida por políticas de seguridad.
- Disponer de conectividad entre la sede principal y sedes remotas para optimizar procesos.
- Contar con un sistema de administración de red y servicios con funcionalidades de administración de fallas, desempeño, configuración y de nivel de servicio para administrar RPV.
- Tener una visualización de los tipos de tráfico, es decir, qué elementos consumen mayor ancho de banda, y monitorear el tráfico de la red de datos en tiempo real y hacer reportes de historial de consumo.
- Hacer que todo el tráfico de las sedes remotas, salgan por el enlace de la sede principal para que así pueda ser visualizado por el Administrador de ancho de banda.
- Tener escalabilidad en la red además, está diseñada para implementar cualquier tipo de seguridad adicional a la estructura brindada.

3.2 CONSTRUCCIÓN DISEÑO

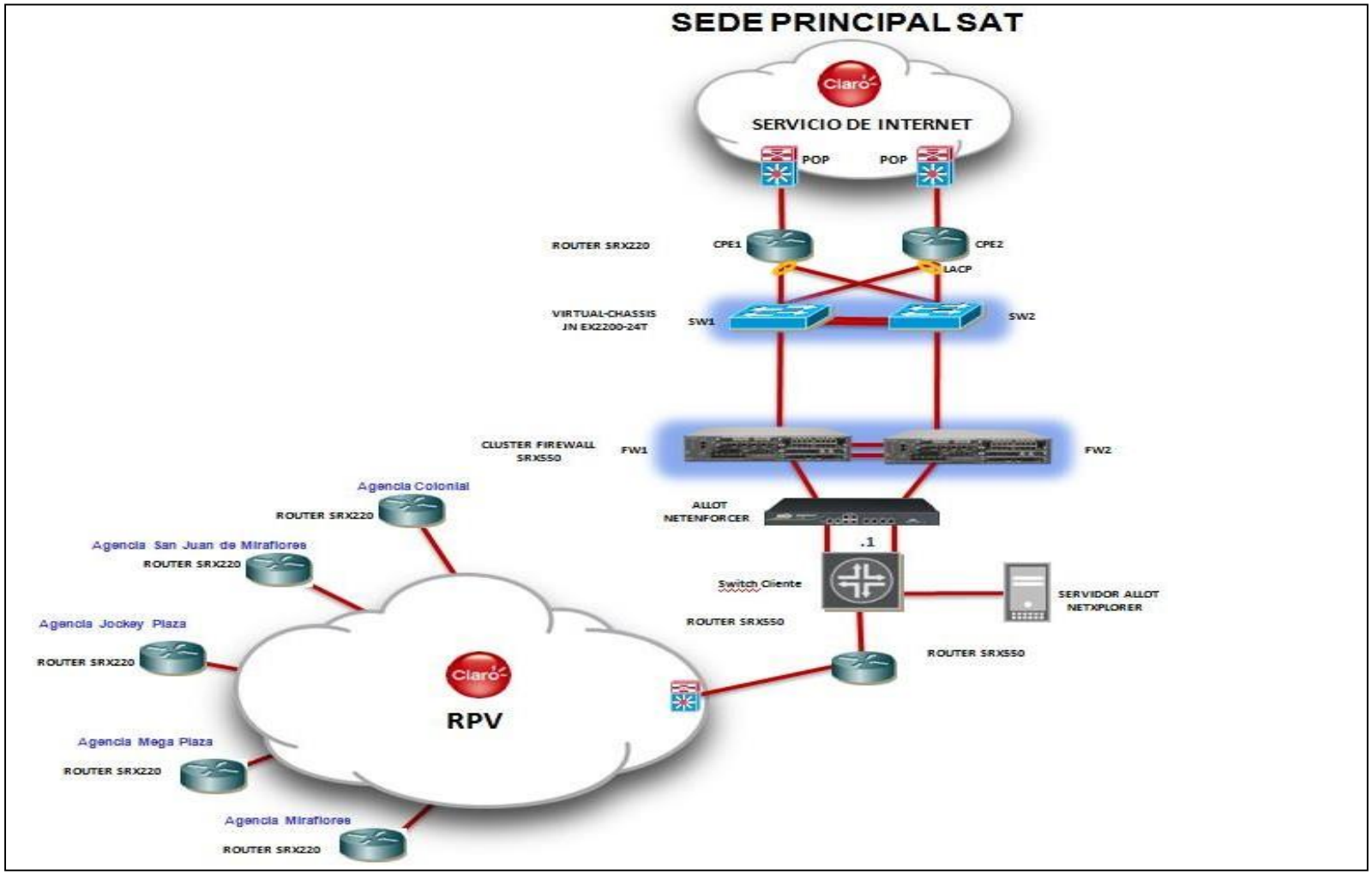


Figura 3.10: Estructura de red
Fuente: Elaboración propia.

REQUERIMIENTOS DE INSTALACIÓN LADO CLARO Y CLIENTE

a. Introducción

Para la instalación de los equipos se necesita que ambas partes tanto la superintendencia de Administración Tributaria (SAT) y el Proveedor de Internet (CLARO), cumplan con lo que está determinado en las bases y provean los equipos y accesorios necesarios para el levantamiento del servicio.

b. Equipamiento lado CLARO

1. ROUTER Juniper SRX220

Tanto el activo como el pasivo fueron creados los link agregation ae1 y ae2, con el fin de aumentar el rendimiento más de lo que una sola conexión podría sostener, además de proporcionar redundancia si es que un enlace llegara a fallar, estos equipos están en bajo el protocolo VRRP, ya que al ser activo/pasivo poseen una interface virtual diseñado para aumentar la disponibilidad de la puerta de enlace.

Figura 3.11: Router Juniper SRX220
Fuente: Elaboracion propia

2. Firewall Juniper SRX550

Se realiza la conexión formando un clúster entre ambos equipos, esta configuración hace que los equipos estén sincronizados es decir al hacer un cambio y ejecutar el comando commit se reflejara en ambos nodos. Las conexiones del clúster dependen del modelo de cada equipo en este caso para el SRX550 se utilizaran las interfaces ge-0/0/1 y ge-0/0/6 para managment y control respectivamente.

Figura 3.12: Firewall Juniper SRX550
Fuente: Elaboracion propia

3. Switches Juniper EX2200

Los switches fueron configurados de tal manera que formen un virtual chassis, la cual hace que ambos equipos se comporten como si fuera uno solo, la configuración es la misma para ambos swiches, dando la ventaja de que si el enlace activo falla automáticamente pasa a tomar el papel de máster el otro switch, no viéndose interrumpido la conexión hacia internet.

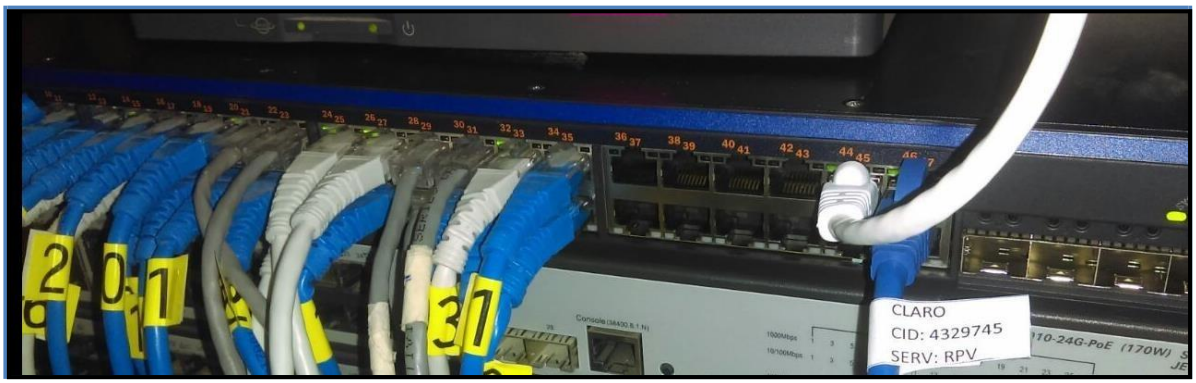


Figura 3.13: Switch Juniper EX2200
Fuente: Elaboracion propia

4. RPV Juniper SRX220

La comunicación por la RPV se dará a través de los equipos Juniper SRX220, se instalaran en cada una de las sedes del SAT (Agencia) conectados al media coverter para la comunicación hacia el POP, además de un SW Juniper para la interconexión con su LAN, este Sw estará con configurado en capa 2 con auto negociación en sus interfaces.

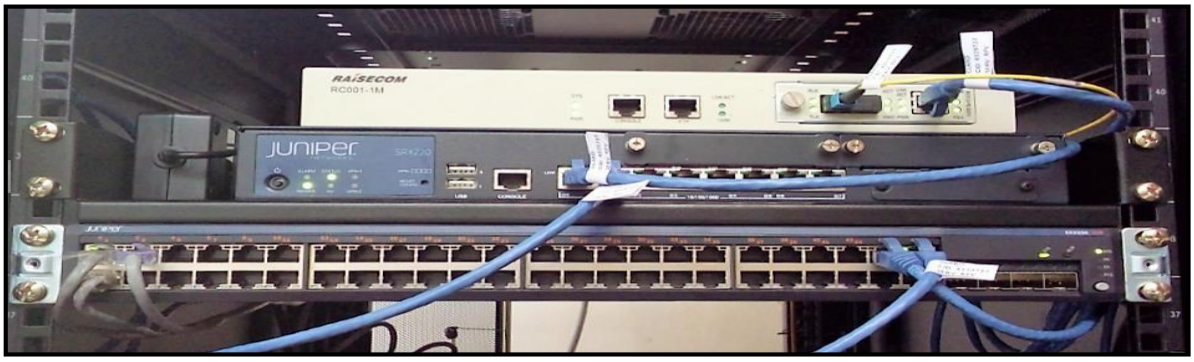


Figura 3.14: RPV con SRX220 en sedes remotas
Fuente: Elaboracion propia

5. Administrador de Ancho de Banda (ALLOT).

Este Administrador de Ancho de Banda cuenta con un módulo Bypass, se conectan a la red en las interfaces Internal0, External0 e Internal1, External1; las interfaces están configuradas en el modo bypass por lo que si se produce algún error en el equipo la conexión a internet no se pierde; además la administración de este equipo se hace a través del NetXplorer, que está instalado en un servidor, donde creamos las políticas para limitar los diferentes servicios.

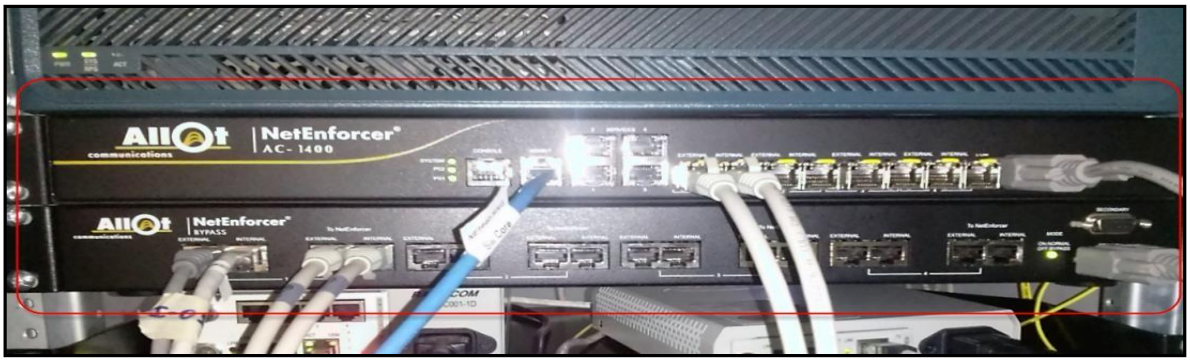


Figura 3.15: Administrador de Ancho de Banda AC- 1400 (NetEnforcer)
Fuente: Elaboracion propia

Figura 3.16: Servidor Proliant hp (NetXplorer)
Fuente: Elaboracion propia

6. PatchCord UTP

Para la interconexión de los diferentes equipos usaremos la Categoría 5e, y también otras categorías dependiendo del requerimiento del servicio.

Figura 3.17: Conectores rj45 para cables utp
Fuente: Elaboracion propia

C. Requerimiento lado CLIENTE.

1. Media Converter.

Equipo cuya instalación es hecha por planta externa.

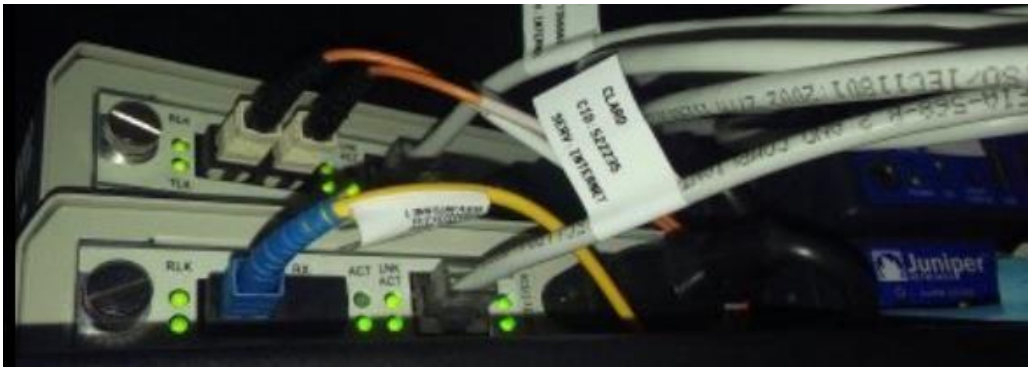


Figura 3.18: Conversor raisecom
Fuente: Elaboracion propia

2. Switch Core CISCO

El SAT actualmente cuenta con un sw-corecatalyst de Cisco, la cual toda configuración, gestión y soporte lo realiza otra empresa a cargo, si se necesitara que se modifique algo por temas de configuración se tendrá que gestionar ya que la única que tiene los accesos de dicho equipo es el SAT.

Figura 3.19: SwitchCore Cisco – cliente
Fuente: Elaboracion propia

3. Jumper de Fibra Óptica

Por parte del cliente para la conexión de su media converter al panduit necesitara un Jumper de Fibra Óptica Monomodo: Largo alcance de color Amarillo, Fibra de 2 y 1 Hilo. Con los conectores ST-SC, SC-SC, ST-LC, SC-LC, SC-FC

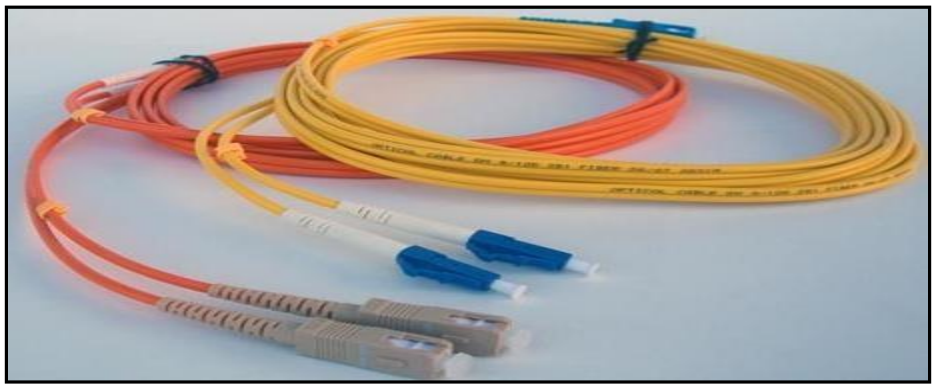


Figura 3.20: Conectores del jumper
Fuente: Elaboracion propia

4. Caja Panduit.

Es la terminación Óptica, final que deja la entidad con otra contrata, para realizar la conexión con el enlace directo al POP o NODO.

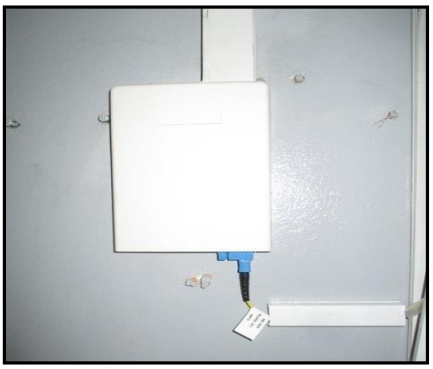


Figura 3.21: Caja panduit
Fuente: Elaboracion propia

5. Cableado Reflejo

Aquí se realiza la interconexión entre equipos sin necesidad de tomar puertos directos.

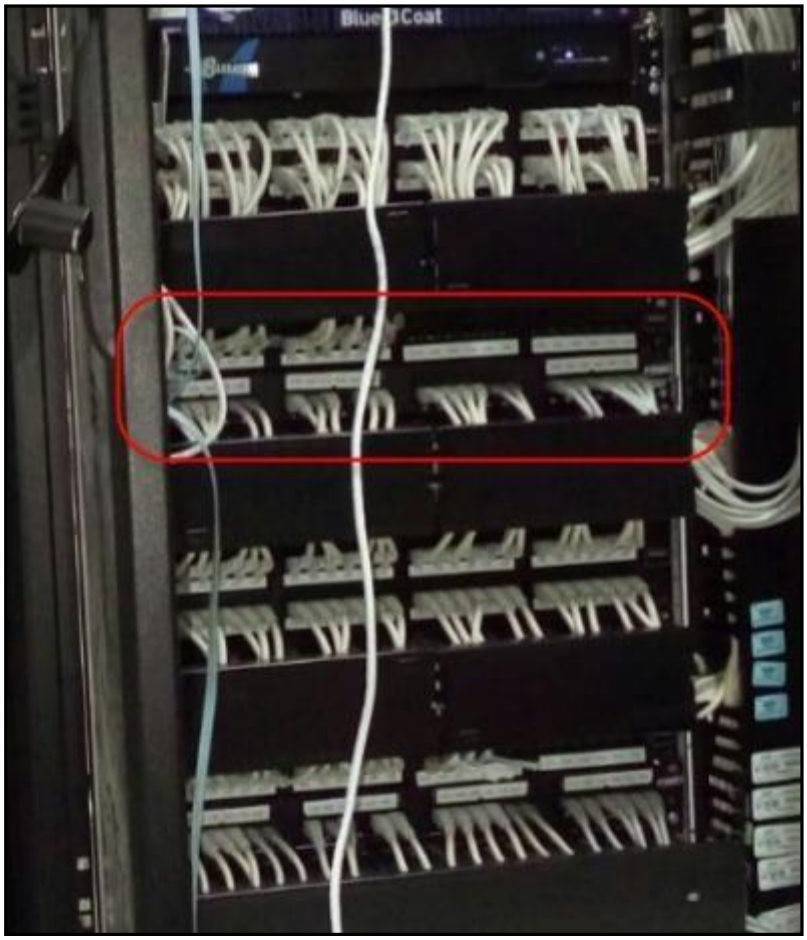


Figura 3.22: Vista de equipos instalados
Fuente: Elaboracion propia

6. Tomas eléctricas.

Aquí dependiendo de la factibilidad se hará la instalación con los power de los equipos en base a la toma eléctrica que posea el SAT.

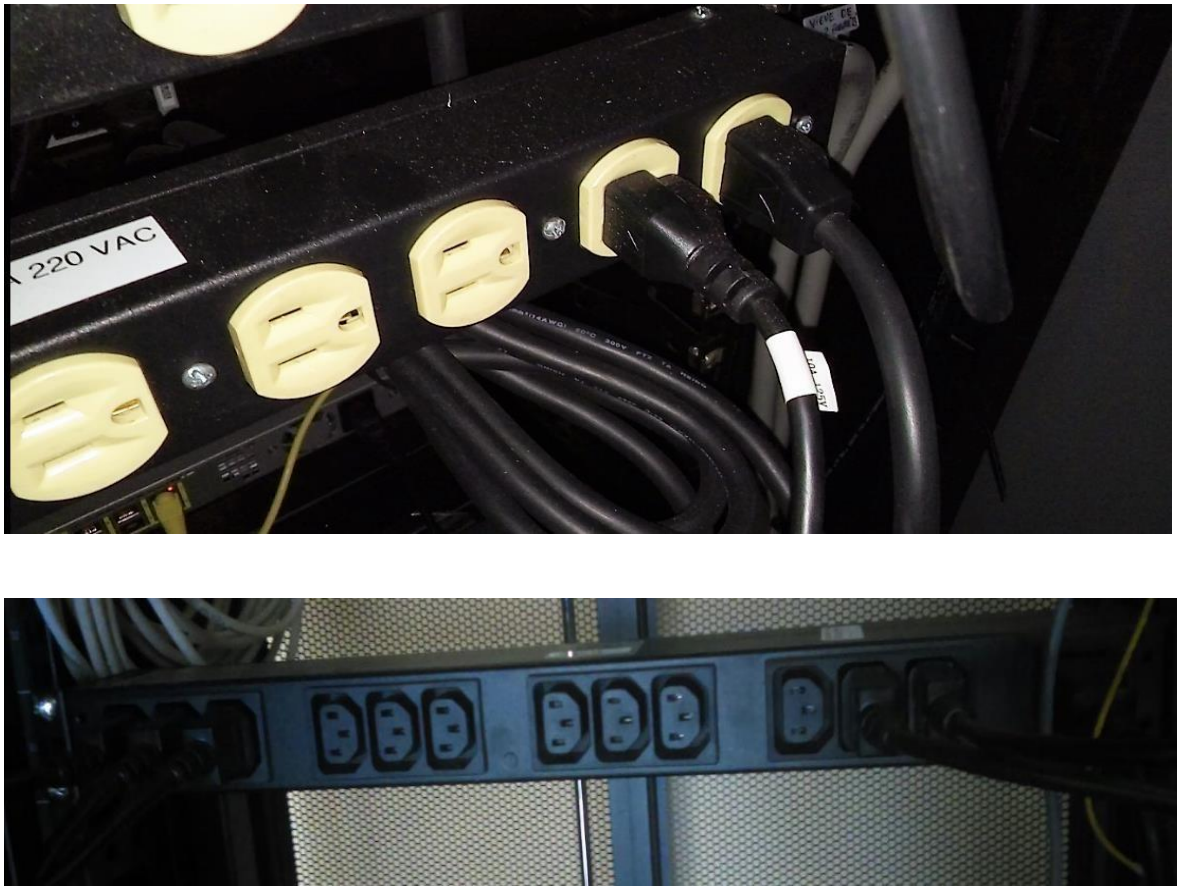


Figura 3.23: Vista de los diferentes tipos de tomas eléctricas
Fuente: Elaboracion propia

3.3 REVISIÓN Y CONSOLIDACIÓN DE RESULTADOS

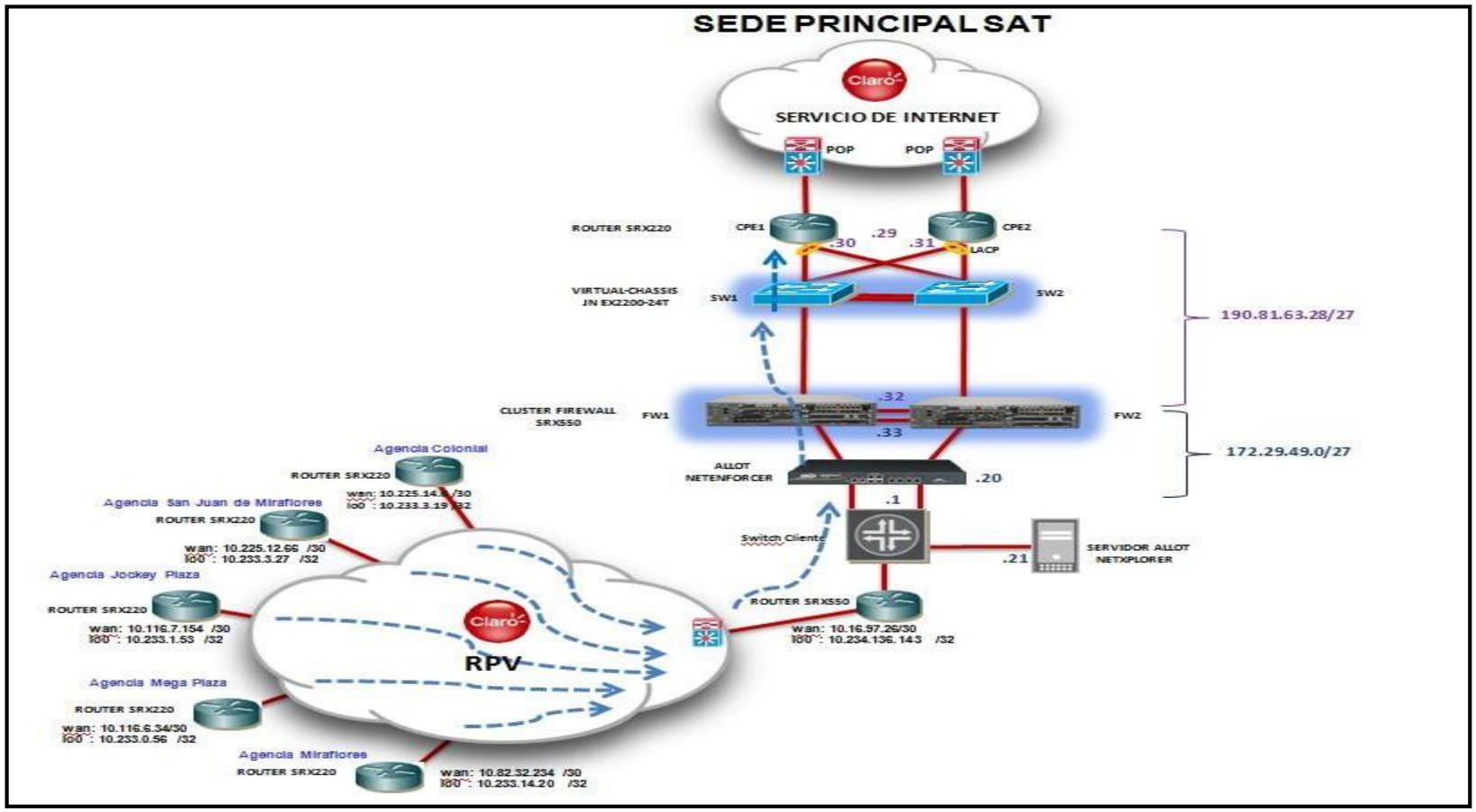


Figura 3.24: Red diseñada para el SAT
Fuente: Elaboración propia

Checklist del Router Principal: Comandos importantes.

SHOW VERSION:

Muestra la versión del software Junos en el router.

```
[edit]
root@SAT_Internet_Principal# run show version
Hostname: SAT_Internet_Principal
Model: srx220h2
JUNOS Software Release [12.1X46-D40.2]
```

SHOW SYSTEM STORAGE:

Muestra la memoria del equipo.

```
[edit]
root@SAT_Internet_Principal# run show system storage
Filesystem             Size       Used      Avail  Capacity   Mounted on
/dev/ad0s2a            594M       147M       400M        27%  /
devfs                  1.0K       1.0K         0B       100%  /dev
/dev/md0                20M      1002K        17M         5%  /junos
/cf/packages           594M       147M       400M        27%  /junos/cf/packages
devfs                  1.0K       1.0K         0B       100%  /junos/cf/dev
/cf/usr                594M       147M       400M        27%  /junos/cf/usr
/cf/boot               594M       147M       400M        27%  /junos/cf/boot
/dev/md1               407M       407M         0B       100%  /junos
/cf                     20M      1002K        17M         5%  /junos/cf
devfs                  1.0K       1.0K         0B       100%  /junos/dev/
/cf/packages           594M       147M       400M        27%  /junos/cf/packages1
/cf/boot               594M       147M       400M        27%  /junos/cf/boot
/cf/usr                594M       147M       400M        27%  /junos/cf/usr1
procfs                 4.0K       4.0K         0B       100%  /proc
/dev/bo0s3e             46M        28K        42M         0%  /config
/dev/bo0s3f            593M       6.8M       539M         1%  /cf/var
/dev/md2               336M        20M       289M         6%  /mfs
/cf/var/jail           593M       6.8M       539M         1%  /jail/var
/cf/var/log            593M       6.8M       539M         1%  /jail/var/log
devfs                  1.0K       1.0K         0B       100%  /jail/dev
/dev/md3                63M       4.0K        58M         0%  /mfs/var/run/utm
/dev/md4               1.8M       4.0K       1.7M         0%  /jail/mfs
```

SHOW CHASSIS HARDWARE:

Muestra el modelo y número de serie del Router.

```
[edit]
root@SAT_Internet_Principal# run show chassis hardware detail | no-more
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                               CF4715AK0637      SRX220H2
Routing Engine   REV 05   750-048778   ACNK4086          RE-SRX220H2
  ad0    1919 MB  ATP COMPACT FLASH    99008150917130201841 Compact Flash
  usb0 (addr 1)  DWC OTG root hub 0    vendor 0x0000     uhub0
  usb0 (addr 2)  product 0x005a 90     vendor 0x0409     uhub1
FPC 0                                                   FPC
  PIC 0                                                 8x GE Base PIC
Power Supply 0
```

SHOW ROUTE:

Muestra todas las rutas.

```
[edit]
root@SAT_Internet_Principal# run show route

inet.0: 7 destinations, 9 routes (7 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[BGP/170] 01:15:11, localpref 100
                      AS path: 12252 6453 I
                    > to 200.24.183.49 via ge-0/0/0.0
                    [BGP/170] 00:09:41, localpref 100
                      AS path: 12252 6453 I
                    > to 190.81.63.131 via vlan.2
190.81.63.128/27   *[Direct/0] 00:11:33
                    > via vlan.2
                    [BGP/170] 00:09:41, localpref 100
                      AS path: I
                    > to 190.81.63.131 via vlan.2
190.81.63.129/32   *[Local/0] 00:11:28
                      Local via vlan.2
190.81.63.130/32   *[Local/0] 01:25:25
                      Local via vlan.2
200.24.181.248/29  *[BGP/170] 00:09:41, localpref 100
                      AS path: I
                    > to 190.81.63.131 via vlan.2
200.24.183.48/29   *[Direct/0] 01:15:21
                    > via ge-0/0/0.0
200.24.183.53/32   *[Local/0] 01:25:25
                      Local via ge-0/0/0.0
```

PING WAN:

Muestra la conectividad entre el router y el equipo de acceso (Red de CLARO).

```
[edit]
root@SAT_Internet_Principal# run ping 200.24.183.49 rapid count 1000
PING 200.24.183.49 (200.24.183.49): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!
--- 200.24.183.49 ping statistics ---
1000 packets transmitted, 1000 packets received, 0% packet loss
round-trip min/avg/max/stddev = 2.129/2.695/32.948/1.238 ms
```

PING PÁGINA WEB:

Se muestra acceso a internet desde el CPE.

```
[edit]
root@SAT_Internet_Principal# run ping www.lan.com rapid count 1000
PING a1129.q.akamai.net (179.6.253.24): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- a1129.q.akamai.net ping statistics ---
1000 packets transmitted, 1000 packets received, 0% packet loss
round-trip min/avg/max/stddev = 3.850/4.488/35.684/2.064 ms
```

PING PÁGINA WEB:

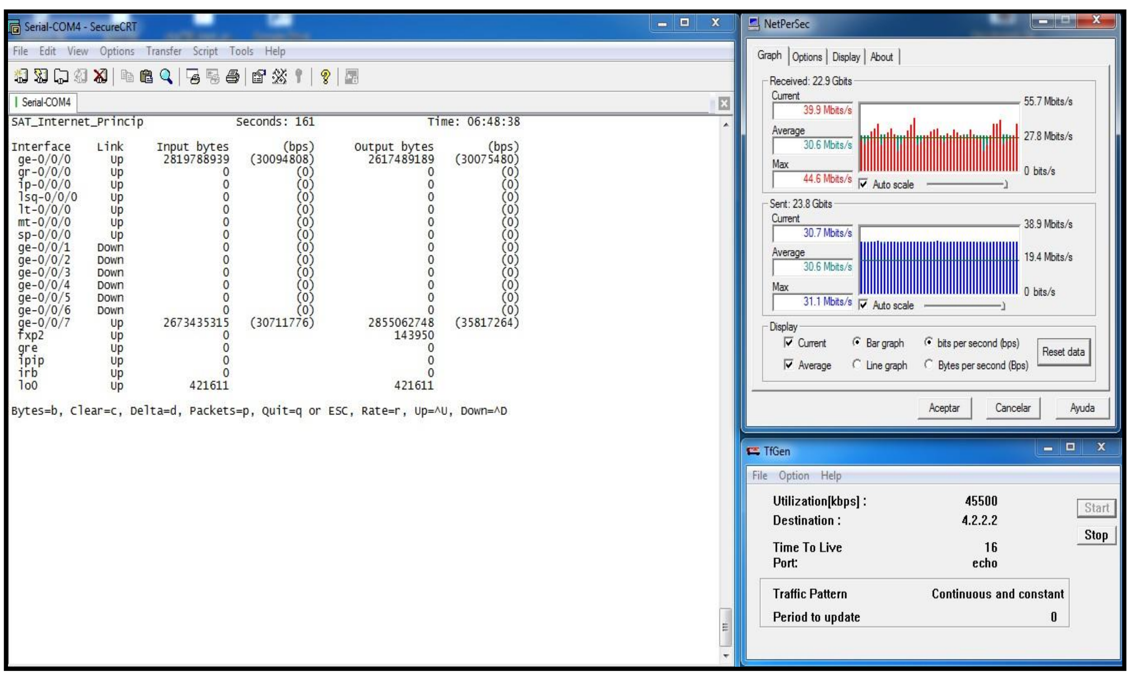
Se muestra acceso a internet desde la LAN.

```
[edit]
root@SAT_Internet_Principal# run ping www.lan.com source 190.81.63.130 rapid count 1000
PING a1129.q.akamai.net (179.6.253.24): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- a1129.q.akamai.net ping statistics ---
1000 packets transmitted, 1000 packets received, 0% packet loss
round-trip min/avg/max/stddev = 2.362/2.922/32.968/1.231 ms
```

PRUEBAS DE SATURACIÓN:

SHOW MONITOR INTERFACE TRAFFIC:

Muestra el consumo de ancho de banda en tiempo real.



SHOW INTERFACES QUEUE FE-0/0/0:

Muestra el consumo de ancho de banda por calidad de servicio en tiempo real en la parte WAN.

```
[edit]
root@SAT_Internet_Principal# run show interfaces queue ge-0/0/0 | no-more
Physical interface: ge-0/0/0, Enabled, Physical link is Up
  Interface index: 134, SNMP ifIndex: 508
Forwarding classes: 8 supported, 5 in use
Egress queues: 8 supported, 5 in use
Queue: 0, Forwarding classes: best-effort
  Queued:
    Packets              :            156411066                3608 pps
    Bytes                :          96232647433            30686624 bps
  Transmitted:
    Packets              :            156411066                3591 pps
    Bytes                :          96232647433            30481352 bps
    Tail-dropped packets :                   0                   0 pps
    RED-dropped packets  :                   0                   0 pps
     Low                 :                   0                   0 pps
     Medium-low          :                   0                   0 pps
     Medium-high         :                   0                   0 pps
     High                :                   0                   0 pps
    RED-dropped bytes    :                   0                   0 bps
     Low                 :                   0                   0 bps
     Medium-low          :                   0                   0 bps
     Medium-high         :                   0                   0 bps
     High                :                   0                   0 bps
Queue: 1, Forwarding classes: qos1
  Queued:
    Packets              :                   0                   0 pps
    Bytes                :                   0                   0 bps
  Transmitted:
    Packets              :                   0                   0 pps
    Bytes                :                   0                   0 bps
    Tail-dropped packets :                   0                   0 pps
    RED-dropped packets  :                   0                   0 pps
     Low                 :                   0                   0 pps
     Medium-low          :                   0                   0 pps
     Medium-high         :                   0                   0 pps
     High                :                   0                   0 pps
    RED-dropped bytes    :                   0                   0 bps
     Low                 :                   0                   0 bps
     Medium-low          :                   0                   0 bps
     Medium-high         :                   0                   0 bps
     High                :                   0                   0 bps
Queue: 2, Forwarding classes: qos2
  Queued:
    Packets              :                   0                   0 pps
    Bytes                :                   0                   0 bps
  Transmitted:
    Packets              :                   0                   0 pps
    Bytes                :                   0                   0 bps
    Tail-dropped packets :                   0                   0 pps
    RED-dropped packets  :                   0                   0 pps
```

```
      Low                    :                       0                       0 pps
      Medium-low             :                       0                       0 pps
      Medium-high            :                       0                       0 pps
      High                   :                       0                       0 pps
    RED-dropped bytes        :                       0                       0 bps
      Low                    :                       0                       0 bps
      Medium-low             :                       0                       0 bps
      Medium-high            :                       0                       0 bps
      High                   :                       0                       0 bps
Queue: 3, Forwarding classes: qos5
  Queued:
    Packets                  :                    1553                       0 pps
    Bytes                    :                  407336                       0 bps
  Transmitted:
    Packets                  :                    1553                       0 pps
    Bytes                    :                  407336                       0 bps
    Tail-dropped packets     :                       0                       0 pps
    RED-dropped packets      :                       0                       0 pps
      Low                    :                       0                       0 pps
      Medium-low             :                       0                       0 pps
      Medium-high            :                       0                       0 pps
      High                   :                       0                       0 pps
    RED-dropped bytes        :                       0                       0 bps
      Low                    :                       0                       0 bps
      Medium-low             :                       0                       0 bps
      Medium-high            :                       0                       0 bps
      High                   :                       0                       0 bps
Queue: 7, Forwarding classes: network-control
  Queued:
    Packets                  :                       0                       0 pps
    Bytes                    :                       0                       0 bps
  Transmitted:
    Packets                  :                       0                       0 pps
    Bytes                    :                       0                       0 bps
    Tail-dropped packets     :                       0                       0 pps
    RED-dropped packets      :                       0                       0 pps
      Low                    :                       0                       0 pps
      Medium-low             :                       0                       0 pps
      Medium-high            :                       0                       0 pps
      High                   :                       0                       0 pps
    RED-dropped bytes        :                       0                       0 bps
      Low                    :                       0                       0 bps
      Medium-low             :                       0                       0 bps
      Medium-high            :                       0                       0 bps
      High                   :                       0                       0 bps
```

Checklist del Router de Contingencia: Comandos importantes.

SHOW VERSION:

Muestra la versión del software Junos en el router.

```
[edit]
NOC@SAT_CAMANA_Contingencia# run show version
Hostname: SAT_CAMANA_Contingencia
Model: srx220h2
JUNOS Software Release [12.1X46-D40.2]
```

SHOW SYSTEM STORAGE:

Muestra la memoria del equipo.

```
[edit]
NOC@SAT_CAMANA_Contingencia# run show system storage
Filesystem             Size       Used      Avail  Capacity   Mounted on
/dev/ad0s2a            594M       147M       400M       27%  /
devfs                  1.0K       1.0K         0B      100%  /dev
/dev/md0                20M      1002K        17M        5%  /junos
/cf/packages           594M       147M       400M       27%  /junos/cf/packages
devfs                  1.0K       1.0K         0B      100%  /junos/cf/dev
/cf/usr                594M       147M       400M       27%  /junos/cf/usr
/cf/boot               594M       147M       400M       27%  /junos/cf/boot
/dev/md1               407M       407M         0B      100%  /junos
/cf                     20M      1002K        17M        5%  /junos/cf
devfs                  1.0K       1.0K         0B      100%  /junos/dev/
/cf/packages           594M       147M       400M       27%  /junos/cf/packages1
/cf/boot               594M       147M       400M       27%  /junos/cf/boot
/cf/usr                594M       147M       400M       27%  /junos/cf/usr1
procfs                 4.0K       4.0K         0B      100%  /proc
/dev/bo0s3e             46M        28K        42M        0%  /config
/dev/bo0s3f            593M       6.8M       539M        1%  /cf/var
/dev/md2               336M        18M       290M        6%  /mfs
/cf/var/jail           593M       6.8M       539M        1%  /jail/var
/cf/var/log            593M       6.8M       539M        1%  /jail/var/log
devfs                  1.0K       1.0K         0B      100%  /jail/dev
/dev/md3                63M       4.0K        58M        0%  /mfs/var/run/utm
/dev/md4               1.8M       4.0K       1.7M        0%  /jail/mfs
```

SHOW CHASSIS HARDWARE:

Muestra el modelo y número de serie del Router.

```
[edit]
NOC@SAT_CAMANA_Contingencia# run show chassis hardware detail
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                               CF4715AK0516      SRX220H2
Routing Engine   REV 05   750-048778   ACNK3903          RE-SRX220H2
  ad0    1919 MB  ATP COMPACT FLASH    99008150917130201930 Compact Flash
  usb0 (addr 1)  DWC OTG root hub 0    vendor 0x0000     uhub0
  usb0 (addr 2)  product 0x005a 90     vendor 0x0409     uhub1
FPC 0                                                   FPC
  PIC 0                                                 8x GE Base PIC
Power Supply 0
```

SHOW ROUTE:

Muestra todas las rutas.

```
[edit]
root@SAT_Internet_Contingencia# run show route

inet.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[BGP/170] 02:47:26, localpref 100
                      AS path: 12252 6453 I
                    > to 200.24.181.249 via ge-0/0/0.0
190.81.63.128/27   *[Direct/0] 00:01:33
                    > via vlan.2
190.81.63.129/32   *[Local/0] 00:01:26
                      Local via vlan.2
190.81.63.131/32   *[Local/0] 02:47:59
                      Local via vlan.2
200.24.181.248/29  *[Direct/0] 02:47:38
                    > via ge-0/0/0.0
200.24.181.253/32  *[Local/0] 02:47:59
                      Local via ge-0/0/0.0
```

PING WAN:

Muestra la conectividad entre el router y el equipo de acceso (Red de CLARO).

```
[edit]
root@SAT_Internet_Contingencia# run ping 200.24.181.249 rapid count 1000
PING 200.24.181.249 (200.24.181.249): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 200.24.181.249 ping statistics ---
1000 packets transmitted, 1000 packets received, 0% packet loss
round-trip min/avg/max/stddev = 2.609/4.404/187.570/6.256 ms
```

PING PÁGINA WEB:

Se muestra acceso a internet desde el CPE.

```
[edit]
root@SAT_Internet_Contingencia# run ping www.lan.com rapid count 1000
PING a1129.q.akamai.net (179.6.253.24): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- a1129.q.akamai.net ping statistics ---
1000 packets transmitted, 1000 packets received, 0% packet loss
round-trip min/avg/max/stddev = 3.850/4.488/35.684/2.064 ms
```

PING PÁGINA WEB:

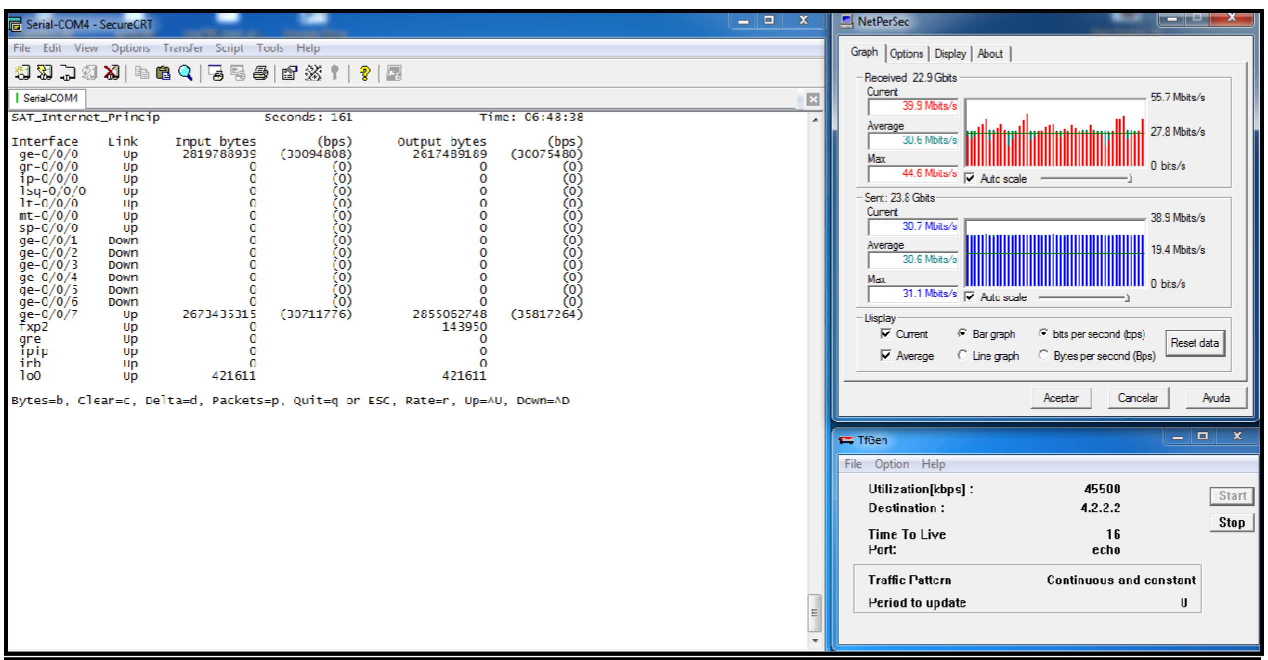
Se muestra acceso a internet desde la LAN.

```
[edit]
root@SAT_Internet_Contingencia# run ping www.lan.com source 190.81.63.131 rapid count 1000
PING a1129.q.akamai.net (179.6.253.32): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- a1129.q.akamai.net ping statistics ---
1000 packets transmitted, 1000 packets received, 0% packet loss
round-trip min/avg/max/stddev = 3.913/4.824/93.911/4.104 ms
```

PRUEBAS DE SATURACIÓN:

SHOW MONITOR INTERFACE TRAFFIC:

Muestra el consumo de ancho de banda en tiempo real.



SHOW INTERFACES QUEUE FE-0/0/0:

Muestra el consumo de ancho de banda por calidad de servicio en tiempo real en la parte WAN.

```
[edit]
NOC@SAT_CAMANA_Contingencia# run show interfaces queue ge-0/0/0 | no-more
Physical interface: ge-0/0/0, Enabled, Physical link is Up
  Interface index: 135, SNMP ifIndex: 508
Forwarding classes: 8 supported, 5 in use
Egress queues: 8 supported, 5 in use
Queue: 0, Forwarding classes: best-effort
  Queued:
    Packets              :              2394919                 4227 pps
    Bytes                :           2182903433              31295408 bps
  Transmitted:
    Packets              :              2394919                 4227 pps
    Bytes                :           2182903433              31295408 bps
    Tail-dropped packets :                    0                    0 pps
    RED-dropped packets  :                    0                    0 pps
     Low                 :                    0                    0 pps
     Medium-low          :                    0                    0 pps
     Medium-high         :                    0                    0 pps
     High                :                    0                    0 pps
    RED-dropped bytes    :                    0                    0 bps
     Low                 :                    0                    0 bps
     Medium-low          :                    0                    0 bps
     Medium-high         :                    0                    0 bps
     High                :                    0                    0 bps
Queue: 1, Forwarding classes: qos1
  Queued:
    Packets              :                    0                    0 pps
    Bytes                :                    0                    0 bps
  Transmitted:
    Packets              :                    0                    0 pps
    Bytes                :                    0                    0 bps
    Tail-dropped packets :                    0                    0 pps
    RED-dropped packets  :                    0                    0 pps
     Low                 :                    0                    0 pps
     Medium-low          :                    0                    0 pps
     Medium-high         :                    0                    0 pps
     High                :                    0                    0 pps
    RED-dropped bytes    :                    0                    0 bps
     Low                 :                    0                    0 bps
     Medium-low          :                    0                    0 bps
     Medium-high         :                    0                    0 bps
     High                :                    0                    0 bps
Queue: 2, Forwarding classes: qos2
  Queued:
    Packets              :                    0                    0 pps
    Bytes                :                    0                    0 bps
  Transmitted:
    Packets              :                    0                    0 pps
    Bytes                :                    0                    0 bps
    Tail-dropped packets :                    0                    0 pps
    RED-dropped packets  :                    0                    0 pps
```

```
    Tail-dropped packets :                    0                    0 pps
    RED-dropped packets  :                    0                    0 pps
     Low                 :                    0                    0 pps
     Medium-low          :                    0                    0 pps
     Medium-high         :                    0                    0 pps
     High                :                    0                    0 pps
    RED-dropped bytes    :                    0                    0 bps
     Low                 :                    0                    0 bps
     Medium-low          :                    0                    0 bps
     Medium-high         :                    0                    0 bps
     High                :                    0                    0 bps
Queue: 3, Forwarding classes: qos5
  Queued:
    Packets              :                   61                    0 pps
    Bytes                :                 9901                    0 bps
  Transmitted:
    Packets              :                   61                     0 pps
    Bytes                :                 9901                    0 bps
    Tail-dropped packets :                    0                    0 pps
    RED-dropped packets  :                    0                    0 pps
     Low                 :                    0                    0 pps
     Medium-low          :                    0                    0 pps
     Medium-high         :                    0                    0 pps
     High                :                    0                    0 pps
    RED-dropped bytes    :                    0                    0 bps
     Low                 :                    0                    0 bps
     Medium-low          :                    0                    0 bps
     Medium-high         :                    0                    0 bps
     High                :                    0                    0 bps
Queue: 7, Forwarding classes: network-control
  Queued:
    Packets              :                    0                    0 pps
    Bytes                :                    0                    0 bps
  Transmitted:
    Packets              :                    0                     0 pps
    Bytes                :                    0                    0 bps
    Tail-dropped packets :                    0                    0 pps
    RED-dropped packets  :                    0                    0 pps
     Low                 :                    0                    0 pps
     Medium-low          :                    0                    0 pps
     Medium-high         :                    0                    0 pps
     High                :                    0                    0 pps
    RED-dropped bytes    :                    0                    0 bps
     Low                 :                    0                    0 bps
     Medium-low          :                    0                    0 bps
     Medium-high         :                    0                    0 bps
     High                :                    0                    0 bps
```

PRUEBA DE VALIDACIÓN DEL FIREWALL.

SHOW VERSION

Muestra la versión actual de ambos equipos ya que están configurados en cluster.

```
{primary:node0}[edit]
NSOC-CONNECT@SAT-PRINCIPAL# run show version
node0:
--------------------------------------------------------------------------
Hostname: SAT-PRINCIPAL
Model: srx550
JUNOS Software Release [12.1X46-D40.2]

node1:
--------------------------------------------------------------------------
Hostname: SAT-SECUNDARIO
Model: srx550
JUNOS Software Release [12.1X46-D40.2]
```

SHOW CHASSIS CLUSTER STATUS

Muestra el estado de los equipos tanto el máster como el de backup, es decir nos da la información de por donde actualmente está pasando el tráfico.

```
{primary:node0}[edit]
NSOC-CONNECT@SAT-PRINCIPAL# run show chassis cluster status
Monitor Failure codes:
    CS  Cold Sync monitoring        FL  Fabric Connection monitoring
    GR  GRES monitoring             HW  Hardware monitoring
    IF  Interface monitoring        IP  IP monitoring
    LB  Loopback monitoring         MB  Mbuf monitoring
    NH  Nexthop monitoring          NP  NPC monitoring
    SP  SPU monitoring              SM  Schedule monitoring

Cluster ID: 1
Node   Priority Status         Preempt Manual   Monitor-failures

Redundancy group: 0 , Failover count: 1
node0  254      primary        no      no       None
node1  1        secondary      no      no       None

Redundancy group: 1 , Failover count: 17
node0  200      primary        yes     no       None
node1  199      secondary      yes     no       None
```

SHOW CHASSIS ROUTING-ENGINE

Nos muestra la información de consumo de memoria de los equipos.

```
{primary:node0}[edit]
NSOC-CONNECT@SAT-PRINCIPAL# run show chassis routing-engine
node0:
--------------------------------------------------------------------------
Routing Engine status:
    Temperature                 34 degrees C / 93 degrees F
    CPU temperature             34 degrees C / 93 degrees F
    Total memory              2048 MB Max  1311 MB used ( 64 percent)
      Control plane memory    1088 MB Max   653 MB used ( 60 percent)
      Data plane memory        960 MB Max   662 MB used ( 69 percent)
    CPU utilization:
      User                      38 percent
      Background                 0 percent
      Kernel                     4 percent
      Interrupt                  0 percent
      Idle                      58 percent
    Model                       RE-SRXSME-SRX550
    Serial ID                   ACMT4036
    Start time                  2016-04-03 00:03:54 PET
    Uptime                      127 days, 23 hours, 43 minutes, 29 seconds
    Last reboot reason          0x200:normal shutdown
    Load averages:              1 minute   5 minute  15 minute
                                    0.63       0.63       0.64

node1:
--------------------------------------------------------------------------
Routing Engine status:
    Temperature                 29 degrees C / 84 degrees F
    CPU temperature             29 degrees C / 84 degrees F
    Total memory              2048 MB Max  1126 MB used ( 55 percent)
      Control plane memory    1088 MB Max   457 MB used ( 42 percent)
      Data plane memory        960 MB Max   662 MB used ( 69 percent)
    CPU utilization:
      User                       7 percent
      Background                 0 percent
      Kernel                     1 percent
      Interrupt                  0 percent
      Idle                      92 percent
    Model                       RE-SRXSME-SRX550
    Serial ID                   ACMP9952
    Start time                  2016-04-03 00:14:25 PET
    Uptime                      127 days, 23 hours, 32 minutes, 53 seconds
    Last reboot reason          0x200:normal shutdown
    Load averages:              1 minute   5 minute  15 minute
                                    0.13       0.14       0.10
```

SHOW ROUTING-OPTION

Nos muestra todas las rutas configuradas en el firewall.

```
{primary:node0}[edit]
NSOC-CONNECT@SAT-PRINCIPAL# show routing-options
static {
    route 172.29.50.0/25 next-hop 172.29.49.1;
    route 172.29.50.128/25 next-hop 172.29.49.1;
    route 172.29.51.0/25 next-hop 172.29.49.1;
    route 172.29.51.128/25 next-hop 172.29.49.1;
    route 172.29.52.0/25 next-hop 172.29.49.1;
    route 172.29.52.128/25 next-hop 172.29.49.1;
    route 172.29.53.0/25 next-hop 172.29.49.1;
    route 172.29.53.128/25 next-hop 172.29.49.1;
    route 172.29.54.0/25 next-hop 172.29.49.1;
    route 172.29.54.128/25 next-hop 172.29.49.1;
    route 172.29.55.0/25 next-hop 172.29.49.1;
    route 172.29.56.0/24 next-hop 172.29.49.1;
    route 172.29.57.0/25 next-hop 172.29.49.1;
    route 172.29.66.0/24 next-hop 172.29.49.1;
    route 192.168.30.0/24 next-hop 172.29.49.1;
    route 192.168.32.0/24 next-hop 172.29.49.1;
    route 192.168.34.0/24 next-hop 172.29.49.1;
    route 192.168.36.0/24 next-hop 172.29.49.1;
    route 192.168.38.0/24 next-hop 172.29.49.1;
    route 192.168.40.0/24 next-hop 172.29.49.1;
    route 192.168.42.0/24 next-hop 172.29.49.1;
    route 192.168.44.0/24 next-hop 172.29.49.1;
    route 192.168.46.0/24 next-hop 172.29.49.1;
    route 192.168.48.0/24 next-hop 172.29.49.1;
    route 192.168.52.0/24 next-hop 172.29.49.1;
    route 192.168.54.0/24 next-hop 172.29.49.1;
    route 192.168.81.0/24 next-hop 172.29.49.1;
    route 192.168.132.0/25 next-hop 172.29.49.1;
    route 172.29.70.0/29 next-hop 172.29.49.1;
    route 172.25.60.2/32 next-hop 192.168.50.2;
    route 172.25.2.15/32 next-hop 192.168.50.2;
    route 172.25.2.170/32 next-hop 192.168.50.2;
    route 172.25.2.171/32 next-hop 192.168.50.2;
    route 172.25.4.10/32 next-hop 192.168.50.2;
    route 172.25.4.11/32 next-hop 192.168.50.2;
    route 172.25.5.105/32 next-hop 192.168.50.2;
    route 172.25.5.106/32 next-hop 192.168.50.2;
    route 172.25.16.8/32 next-hop 192.168.50.2;
    route 172.25.16.9/32 next-hop 192.168.50.2;
    route 172.25.16.125/32 next-hop 192.168.50.2;
```

SHOW SYSTEM SNAPSHOT MEDIA INTERNAL

Verificar que las particiones Primary y backup tengan la misma versión de SO.

```
{primary:node0}[edit]
NSOC-CONNECT@SAT-PRINCIPAL# run show system snapshot media internal
node0:
--------------------------------------------------------------------------
Information for snapshot on       internal (/dev/ad0s1a) (backup)
Creation date: Mar 17 22:00:30 2016
JUNOS version on snapshot:
  junos  : 12.1X46-D40.2-domestic
Information for snapshot on       internal (/dev/ad0s2a) (primary)
Creation date: Apr 3 00:04:12 2016
JUNOS version on snapshot:
  junos  : 12.1X46-D40.2-domestic

node1:
--------------------------------------------------------------------------
Information for snapshot on       internal (/dev/ad0s1a) (backup)
Creation date: Mar 17 22:03:50 2016
JUNOS version on snapshot:
  junos  : 12.1X46-D40.2-domestic
Information for snapshot on       internal (/dev/ad0s2a) (primary)
Creation date: Apr 3 00:14:43 2016
JUNOS version on snapshot:
  junos  : 12.1X46-D40.2-domestic
```

PING WAN

Muestra la conectividad del equipo hacia el router.

```
NSOC-CONNECT@SAT-PRINCIPAL# run ping 190.81.63.129 rapid count 1000
PING 190.81.63.129 (190.81.63.129): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 190.81.63.129 ping statistics ---
1000 packets transmitted, 1000 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.838/3.292/150.831/6.112 ms
```

PING LAN

Muestra la conectividad hacia el sw-core

```
{primary:node0}[edit]
NSOC-CONNECT@SAT-PRINCIPAL# run ping 192.168.50.2 rapid count 1000
PING 192.168.50.2 (192.168.50.2): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 192.168.50.2 ping statistics ---
1000 packets transmitted, 1000 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.697/0.916/12.988/0.599 ms
```

PRUEBA DE VALIDACION CON EL BANDWIDTH MANAGER (ALLOT).

Creación de políticas de limitación de ancho de banda

UNMSM									
Identification	Conditions							Actions	
Name	Alarms Assign...	In Use	Internal	Direction	External	Service	Time	Access	Quality of Service
Fallback			Any	⇔	Any	All Service	Anytime	Accept	Normal Line QoS
Fallback			Any	⇔	Any	All Service	Anytime	Accept	Normal Pipe QoS
Auditores_Ex			Auditores_Externos	⇔	Any	All IP	Anytime	Accept	BW_RTVSM_4MB
Streaming			Any	⇔	Any	HTTP_Streaming	Anytime	Accept	BW_RTSM_Ocho...
			Any	⇔	Any	iPlayer	Anytime		
			Any	⇔	Any	HTTP_Audio	Anytime		
Prueba			IP_Test	⇔	Any	All IP	Anytime	Accept	Normal Virtual Ch...
Aceleradores			Any	⇔	Any	HTTP DownloadM...	Anytime	Accept	BW_Aceleradore...
Updates			IPs_SoporteSC	⇔	Any	All IP	Anytime	Accept	Normal Virtual Ch...
BITS			Any	⇔	Any	BITS	Anytime	Drop	Normal Virtual Ch...
			Any	⇔	Any	WindowsUpdate	Anytime		
OCA_172.28			OCA_IP_172.28.1...	⇔	Any	All IP	Anytime	Accept	Normal Virtual Ch...
CEPRE_172			172.16.156.123_f...	⇔	Any	All IP	Anytime	Accept	Normal Virtual Ch...
DEP_CEPRE			G_CEPRE_SERV...	⇔	Any	All IP	Anytime	Accept	BW_WIFI_UNMS...
172.16.208.1			172.16.208.10_C...	⇔	Any	All IP	Anytime	Accept	Normal Virtual Ch...
172.16.156.2			172.16.156.224_...	⇔	Any	All IP	Anytime	Accept	Normal Virtual Ch...

UNMSM

Identification	Conditions							Actions	
Name	Alarms Assign...	In Use	Internal	Direction	External	Service	Time	Access	Quality of Service
172.16.156.2		☑	172.16.156.224_...	⇔	Any	All IP	Anytime	Accept	Normal Virtual Ch...
RTVSM_Rep		☑	RTVSM_Repetido...	⇔	Any	All IP	Anytime	Accept	BW_ViceInvestiga...
Bloqueo_all_		☑	Bloqueo_IPs	⇔	Any	All IP	Anytime	Drop	Normal Virtual Ch...
Bloq_Salidas		☑	Ataques_Out	⇔	Web_Atacada	All IP	Anytime	Drop	Normal Virtual Ch...
Campus		☑	Campus_Server	⇔	Any	All IP	Anytime	Accept	BW_Campus_5Mb
Paracas2		☑	Paracas2_172.16...	⇔	Any	All IP	Anytime	Accept	BW_Paracas2_1...
172.16.172.2		☐	172.16.172.250_...	⇔	Any	All IP	Anytime	Accept	BW_OCA_Estadi...
172.16.157.3		☑	172.16.157.33_R...	⇔	Any	All IP	Anytime	Accept	BW_1.0Mb
172.16.156.1		☑	172.16.156.140_...	⇔	Any	All IP	Anytime	Accept	BW_VPN_10Mb
DEP_RTVSM		☑	Grupo_RTVSM	⇔	Any	All IP	Anytime	Accept	BW_RTVSM_4MB
PERMIT_YOU		☑	G_TOTALMENTE...	⇔	Any	YouTube	Anytime	Accept	BW_Youtube_10...
		☐	G_LIBRE	⇔	Any	YouTube	Anytime		
		☑	G_SECGEN	⇔	Any	YouTube	Anytime		
		☑	G_TOTALMENTE...	⇔	Any	YouTube-HD	Anytime		
		☐	G_LIBRE	⇔	Any	YouTube-HD	Anytime		
		☑	G_SECGEN	⇔	Any	YouTube-HD	Anytime		

Creacion de host list

Host

Name	Description	Scope	Date Modified
172.16.156.115		UNMSM	20/04/15 03:53 PM
172.16.156.123_f5_WAM	IP Cepre en el f5 WAM 172.16.156.81	Global	28/10/14 03:56 PM
172.16.156.140_VPN_Huacachina_Nuevo	Server Huacachina Min5Mb Max10Mb	UNMSM	25/03/15 01:06 PM
172.16.156.224_Cisco_Prime	VM server de Monitoreo	Global	18/03/15 03:36 PM
172.16.156.37_Contabilidad_Servidor	Servidor Contabilidad	UNMSM	30/09/14 02:06 PM
172.16.157.1_RTVSM_Auditorio_evento	evento 271114	UNMSM	27/11/14 06:57 PM
172.16.157.33_Red Telematica	BW-1Mb	UNMSM	13/02/14 04:01 PM
172.16.160.100_Evento	Para los dias 20 y 21 de noviembre del 14	UNMSM	19/11/14 12:41 PM
172.16.172.250_OCA_Estadio	Oca Estadio	Global	24/03/15 11:04 AM
172.16.19.204_Contabilidad_Auditorio	IP para RTVSM	UNMSM	21/11/14 02:39 PM
172.16.208.10_Controladora_WIFI	Controladora WIFI UNMSM	UNMSM	18/03/15 03:35 PM
172.16.90.112_113_Evento261114	evento 261114	UNMSM	25/11/14 03:23 PM
75.125.197.150_W_Atacada	Posible ataque	UNMSM	22/04/14 10:30 AM
Alto_Consumo	Fac Contabilidad	UNMSM	27/03/15 09:45 AM
Any		Global	30/12/04 12:00 AM
Any IPv4	All IPv4 hosts	Global	10/04/12 10:01 AM
Any IPv6	All IPv6 hosts	Global	10/04/12 10:07 AM
Ataques_Out	Atacantes a Internet	UNMSM	14/01/15 06:29 PM
Auditores_Externos	172.16.162.[86-89] Auditoria Externa	Global	25/05/15 11:20 AM
Block Service Plan	Service Plan Subscribers Host Group	Global	28/02/07 12:00 AM
Bloqueo_IPs	Bloquear Ips	UNMSM	26/05/15 11:27 AM
Campus_Server	Campus.unmsm.edu.pe	UNMSM	22/04/14 10:02 AM
Cepre_IP_172.16.64.46	Server encuesta	Global	27/05/15 10:45 AM

Name	Description	Scope	Date Modified
Cepre_IP_172.16.64.46	Server encuesta	Global	27/05/15 10:45 AM
Cepre_IP_172.16.64.47	Server Aplicaciones	Global	27/05/15 10:46 AM
Default Service Plan	Service Plan Subscribers Host Group	Global	6/12/07 12:00 AM
DEP_Otros	Otros con menos de 256kb	UNMSM	12/02/14 04:26 PM
G2_LIBRE_ADICIONAL		Global	20/05/15 03:11 PM
G_ADMIN_FACEBOOK	Administrativos solo con Facebook	UNMSM	25/02/15 03:15 PM
G_ADMINISTRATIVOS_VIP	Administrativos con Privilegios	UNMSM	26/05/15 12:42 PM
G_ARTE_CULTURA	Arte y Cultura	UNMSM	16/03/15 12:37 PM
G_CENTRO_CULTURAL	Centro Cultural SM	UNMSM	25/02/14 03:45 PM
G_CEPRE_SERVERS	Server aplicaciones y encuesta cepre	Global	27/05/15 10:47 AM
G_DOCENTES	Docentes	UNMSM	25/02/14 07:46 PM
G_INFORMATICA	Informatica	UNMSM	22/05/15 12:16 PM
G_INVESTIGACION		UNMSM	20/02/15 03:23 PM
G_JEFATURA	Jefatura de Alto Rango	UNMSM	26/05/15 04:57 PM
G_JEFES_INFORMATICA	Jefes de Informatica	UNMSM	20/01/15 12:02 PM
G_LIBRE		UNMSM	22/05/15 09:38 AM
G_LIBRE_ADICIONAL	Libre	UNMSM	6/04/15 04:22 PM
G_LIBRE_Mod	grupo libre	Global	25/05/15 10:30 AM
G_QUIPU	Quipu	UNMSM	4/11/14 10:56 AM
G_REDES_SOCIALES	Redes sociales	UNMSM	2/06/15 09:55 AM
G_RS_C_FACEBOOK	RS c Facebook	UNMSM	9/03/15 05:09 PM
G_SECGEN		UNMSM	23/04/15 09:18 AM
G_Solo_Face	Solo Face sin Youtube	UNMSM	14/04/15 12:48 PM

Asignacion de la calidad de servicio

Quality of Service		
Name	Description	Date Modified
BW_1.0Mb	Maximo BW	3/09/14 03:49 PM
BW_64Kbps	Ancho de banda para Oscar y Daniel Telematica	24/06/14 02:33 PM
BW_Abastecimiento_1.8Mb	Max 1.8Mb	25/02/15 03:30 PM
BW_Aceleradores_3Mb	3Mbps	22/04/15 09:48 AM
BW_Acreditacion_OCCAA	Max 1Mb	27/04/15 04:39 PM
BW_AdminCentral_19.5Mb	Min2Mb Max19502Mb	14/01/14 10:22 AM
BW_Alto_Consumo_750Mb	750Mps max	27/03/15 10:09 AM
BW_Asesoria_Legal_0.77Mb	Max 0.77Mb	12/02/14 11:04 AM
BW_Auditoria_1.5Mb	Max 1.5Mb	19/03/14 10:56 AM
BW_Biblioteca_6.0Mb	Max 6.0 Mb	2/06/14 10:49 AM
BW_Biologia_7.2Mb	Min2Mb Max7.0Mb	30/05/14 03:02 PM
BW_Campus_5Mb	Server Campus 5Mb	22/04/14 10:06 AM
BW_Cinfo_8.9MB	Min2MB Max8.9MB	21/01/14 10:37 AM
BW_Comisiones_Perm_0.82Mb	Max 0.82Mb	12/02/14 10:50 AM
BW_Contabilidad_3.0Mb	Max 3.0 Mb	24/10/14 01:06 PM
BW_Control_Previo_0.56Mb	Max 0.56Mb	12/02/14 04:37 PM
BW_Cooperacion_2Mbps	Max 2 Mbps	25/03/15 05:34 PM
BW_Derecho_17.3Mb	Min2Mb Max17305Mb	10/02/15 01:37 PM
BW_DGA_DIGA_0.768Mb	Max 0.768Mb	12/02/14 10:46 AM
BW_Economia_14.5Mb	Min2Mb Max14.59Mb	16/04/15 08:35 AM
BW_Educacion1_13.8Mb	Min2Mb Max13824Mb	16/04/15 08:36 AM
BW_Electronica1_8Mb	Min2Mb Max8Mb	16/04/15 08:36 AM
BW_Fac_Administracion_9Mb	Min2MB Max9MB	16/04/15 08:36 AM

CONCLUSIONES

1.- Se diseñó esta topología para la seguridad en la sede principal, además de tener una alta disponibilidad y control del ancho de banda que se maneja. Este proyecto se puede implementar en cualquier entidad del estado o empresa.

2.- Hay la necesidad de hacer que las agencias salgan hacia internet por la sede principal, ya que de esa manera no se contrataría un servicio de internet independiente para cada sede y se tendría un control y visualización del tráfico que pasa por cada una de las agencia.

3.-Se instalan los equipos dependiendo de la necesidad del SAT, además la descripción técnica de los equipos está basada en los requerimientos de la entidad a instalar cuyas marcas son Juniper y Allot; las respectivas versiones están actualizadas a las recomendadas por el fabricante de cada una de las marcas.

4.- Este proyecto se presenta para el Sistema de Administración Tributaria (SAT) como una alternativa de solución al manejo de la transmisión de datos, ya que la finalidad es dar un óptimo desempeño y sobretodo una transmisión de datos de calidad.

RECOMENDACIONES

1.- Actualmente el administrador de ancho de banda es un equipo primordial y necesario para el control del tráfico, cuyas políticas y asignación del ancho de banda depende de las diferentes necesidades de la entidad, el no tener dicho equipo generaría una saturación en la red, y por ende una mala percepción en la navegación por parte del usuario.

2.- Tener en cuenta que las etapas para la realización del proyecto que se mencionan en el presente trabajo, sirve para la estructuración y realización de futuros proyectos, ya que en ellos se desglosan las fases básicas que se debe ejecutar para plantear una propuesta adecuada a todos los requerimientos.

3.- Considerar que el SRX de Juniper puede trabajar tanto como router o firewall y eso es dependiendo la configuración y las necesidades de cada cliente, los usuarios son limitados a ciertas redes y accesos por temas de seguridad.

4.- Considerar que los equipos que están instalados dentro de un data center, tienen que estar a una temperatura adecuada y un fluido eléctrico estable, por eso se recomienda contar con un equipo UPS en caso falle la energía eléctrica y un sistema de aire acondicionado, para así evitar posibles fallas o daños en el tiempo de vida útil de los equipos.

BIBLIOGRAFÍA

- Siyan, Karajit. Hare, Chrys. (1995) Internet y seguridad en redes.Edtit.Prentice Hall
- David J. Marchette. (2001) Computer Intrussion Detection and Network Monitoring, Springer Verlag.
- Herrera, Omar. (2003) Sistemas de detección de intrusos. Artículos de Seguridad Informática y Seguridad de Redes.
- Firewalls - Security in Distributed Systems, por IndrekPeri. (2000), University of Helsinki, Department of Computer Science.
- Walter Goralski W (1998). ADSL and DSL Technologies. Ed. Hill Associates
- S. Kent, R. Atkinson (1998) IP Encapsulating Security Payload (ESP), Network Working.
- Chapman, D. B.; Zwicky, E. D. (1995) Building Internet Firewalls. O'Reilly Associates.
- Roody Cayambe, Holger Murillo (2006) "Estudio de un administrador de ancho de banda aplicado a un ISP" (Tesis, Facultad de Ingeniería en Electricidad y Computación, Escuela Superior Politécnica del Litoral.
- Jorge R. Hernández (2004), Modelo OSI y el protocolo de Internet (IP versión 6),

ANEXOS

ANEXO A. PROPUESTA ECONOMICA

	Item	Cantidad	Marca	Tipo	Número de parte	Descripción	Unitari	Total
Routers Internet (Sede La Punta & Sede Argentina)	1	7	Juniper	PDT	SRX220H2	SRX services gateway 220 with 8 x GE ports, 2x mini-PIM slots, 2GB DRAM and 2GB CF. External power supply and cord included.	$1,599.00	$11,193.00
FW 02 (Cluster en la sede Principal) 01 Firewall sede Argentina = 03 Firewalls	2	3	Juniper	PDT	SRX550-645AP	SRX550 Platform, 2RU Height, 6 GPIM Slots, 2 MPIM Slots, 6 10/100/1000Base-T Ports, 4 GE SFP Ports, dual PS Slots, fans. Ships with 1 645Watt AC Power Supply with POE power, power cord, rack mount kit,	$9,999.00	$29,997.00
	3	3	Juniper	PDT	SRX-GP-16GE	Ethernet Switch 16-port 10/100/1000Base-T XPIM. Takes 2 slots. Spare	$2,800.00	$8,400.00
	4	3	Juniper	PDT	SRX-RAC-5-LTU	Dynamic VPN Service: 5 simultaneous users	$200.00	$600.00
	5	3	Juniper	PDT	SRX550-APPSEC-A-3	3 year Subscription for Application Security and IPS updates for SRX550	$10,120.00	$30,360.00
	6	3	Juniper	PDT	SV3-ND-SRX550	Juniper Care 3YR Prepaid Next Day Support for SRX550	$2,606.00	$7,818.00
*02 switch para Virtual Chasis (EX2200-24T)	7	2	Juniper	PDT	EX4300-48T	JPSU-350-AC-AFO; 40GE QSFP+ to be ordered separately fo	$8,795.00	$17,590.00
	8	2	Juniper	PDT	EX4300-48-AFL	e for 48-port skus of EX4300 (Requires separate purchase of En	$5,995.00	$11,990.00
	9	2	Juniper	PDT	EX4300-48-EFL	Enhanced Feature License for 48-port skus of EX4300	$1,395.00	$2,790.00
Allot	10	1	Allot	PDT	KAC-504-AC		$7,400.00	$7,400.00
	11	2	Allot	PDT	W1-KAC-540-8P-COP		$1,110.00	$2,220.00
	12	1	Allot	PDT	SBC-500-50M		$8,000.00	$8,000.00
	13	1	Allot	PDT	W1-SBC-1400-1G		$1,200.00	$1,200.00
	14	1	Allot	PDT	SNR-500		$2,000.00	$2,000.00
	15	1	Allot	PDT	W1-SNR-500		$300.00	$300.00
	16	1	HP	PDT	Servidor	NetXplorer + Solarwinds 100 nodos	$3,000.00	$3,000.00
	17	1	Microsoft		Sistema Operativo SO	NetXplorer + Solarwinds 100 nodos	$1,000.00	$1,000.00
								$145,858.00

ANEXO B. DATASHEET DE ALGUNOS EQUIPOS JUNIPER

The Juniper Networks® SRX Series Services Gateways for the branch combine next generation firewall and unified threat management (UTM) services with routing and switching in a single, high-performance, cost-effective network device.

- SRX Series for the branch runs Juniper Networks Junos® operating system, the proven OS that is used by core Internet routers in all of the top 100 service providers around the world. The rigorously tested carrier-class routing features of IPv4/IPv6, OSPF, BGP, and multicast have been proven in over 15 years of worldwide deployments.
- SRX Series for the branch provides perimeter security, content security, application visibility, tracking and policy enforcement, user role-based control, threat intelligence through integration with Juniper Networks Spotlight Secure*, and network-wide threat visibility and control. Using zones and policies, network administrators can configure and deploy branch SRX Series gateways quickly and securely. Policy-based VPNs support more complex security architectures that require dynamic addressing and split tunneling. The SRX Series also includes wizards for firewall, IPsec VPN, Network Address Translation (NAT), and initial setup to simplify configurations out of the box.

Architecture and Key Components

Key Hardware Features of the Branch SRX Series Products

Product	Description
SRX100 Services Gateway	· Eight 10/100 Ethernet LAN ports and 1 USB port (support for 3G USB) · Full UTM[1]; antivirus[1], antispam[1], enhanced Web filtering[1], and content filtering · Intrusion prevention system[1], AppSecure[1] · 2 GB DRAM, 2 GB flash default
SRX110 Services Gateway	· VDSL/ADSL2+ and Ethernet WAN interfaces · Eight 10/100 Ethernet LAN ports and two USB port (support for 3G USB) · Full UTM[1]; antivirus[1], antispam[1], enhanced Web filtering[1], intrusion prevention system[1], AppSecure[1] · Unified Access Control (UAC) and content filtering · 2 GB DRAM, 2 GB CF default
SRX210 Services Gateway	· Two 10/100/1000 Ethernet and 6 10/100 Ethernet LAN ports, 1 Mini-PIM slot, and 2 USB ports (support for 3G USB) · Factory option of 4 dynamic Power over Ethernet (PoE) ports 802.3af · Support for T1/E1, serial, ADSL/2/2+, VDSL, G.SHDSL, and Ethernet small form-factor pluggable transceiver (SFP) · Content Security Accelerator hardware for faster performance of IPS and ExpressAV (with high memory version) · Full UTM[1]; antivirus1, antispam[1], enhanced Web filtering[1], and content filtering · Intrusion prevention system[1], User role-based firewall, and AppSecure[1] · 2 GB DRAM, 2 GB flash default
SRX220 Services Gateway	· Eight 10/100/1000 Ethernet LAN ports, 2 Mini-PIM slots · Factory option of 8 PoE ports; PoE+ 802.3at, backwards compatible with 802.3af · Support for T1/E1, serial, ADSL2/2+, VDSL, G.SHDSL, and Ethernet SFP · Content Security Accelerator hardware for faster performance of IPS and ExpressAV · Full UTM[1]; antivirus[1], antispam[1], enhanced Web filtering[1], and content filtering · Intrusion prevention system[1], User role-based firewall and AppSecure[1] · 2 GB DRAM, 2 GB CF default
SRX240 Services Gateway	· 16 10/100/1000 Ethernet LAN ports, 4 Mini-PIM slots · Factory option of 16 PoE ports; PoE+ 802.3at, backwards compatible with 802.3af · Support for T1/E1, serial, ADSL2/2+, VDSL, G.SHDSL, and Ethernet SFP · Content Security Accelerator hardware for faster performance of IPS and ExpressAV · Full UTM[1]; antivirus1, antispam[1], enhanced Web filtering[1], and content filtering · Intrusion prevention system[1], AppSecure[1]
SRX550 Services Gateway	· Ten fixed Ethernet ports (6 10/100/1000 copper, 4 SFP), 2 Mini-PIM slots, 6 GPIM slots or multiple GPIM and XPIM combinations · Support for T1/E1, serial, ADSL2/2+, VDSL, G.SHDSL, DS3/E3, Gigabit Ethernet ports; supports up to 52 Ethernet ports including SFP; 40 switch ports with optional PoE including 802.3at, PoE+, backwards compatible with 802.3af (or 50 non-PoE 10/100/1000 copper ports) · Content Security Accelerator hardware for faster performance of IPS and ExpressAV · Full UTM[1]; antivirus[1], antispam[1], enhanced Web filtering[1], and content filtering · Intrusion prevention system[1], User role-based firewall, and AppSecure[1] · Threat intelligence for protection from command and control (C&C) botnets, Web application threats, and advanced malware, and policy enforcement based on GeoIP data · 2 GB DRAM default, 2 GB compact flash default (SRX550) · 4 GB DRAM default, 8 GB compact flash default (SRX550 High Memory) · Optional redundant AC power; standard AC power supply that is PoE-ready; PoE power up to 250 watts single power supply or 500 watts dual power supply
SRX650 Services Gateway	· Four fixed ports 10/100/1000 Ethernet LAN ports, 8 GPIM slots or multiple GPIM and XPIM combinations · Support for T1, E1, DS3/E3, Ethernet ports; supports up to 52 Ethernet ports including SFP; 48 switch ports with optional PoE including 802.3at, PoE+, backwards compatible with 802.3af (or 52 non-PoE 10/100/1000 copper ports) · Content Security Accelerator hardware for faster performance of IPS and ExpressAV · Full UTM[1]; antivirus[1], antispam[1], enhanced Web filtering[1], and content filtering · Intrusion prevention system[1], User role-based firewall, and AppSecure[1] · Threat intelligence for protection from command and control (C&C) botnets, Web application threats, and advanced malware, and policy enforcement based on GeoIP data · Modular Services and Routing Engine; future internal failover and hot-swap · 2 GB DRAM default, 2 GB compact flash default, external compact flash slot for additional storage · Optional redundant AC power; standard AC power supply that is PoE-ready; PoE power up to 250 watts single power supply or 500 watts dual power supply

Product Comparison

	SRX100	SRX110	SRX210	SRX220	SRX240	SRX550	SRX650
Maximum Performance and Capacity							
Junos OS version tested	Junos OS 12.1X44-D15	Junos OS 12.1X44-D15	Junos OS 12.1X44-D15	Junos OS 12.1X44-D15	Junos OS 11.4R5	Junos OS 12.1/15.1[7]	Junos OS 11.4R5
Firewall performance (large packets)	700 Mbps	700 Mbps	850 Mbps	950 Mbps	1.8 Gbps	7 Gbps	7 Gbps
Firewall performance (IMIX)	200 Mbps	200 Mbps	250 Mbps	300 Mbps	600 Mbps	2 Gbps	2.5 Gbps
Firewall + routing PPS (64 Byte)	70 Kpps	70 Kpps	95 Kpps	125 Kpps	200 Kpps	700 Kpps	850 Kpps
Firewall performance[8] (HTTP)	100 Mbps	100 Mbps	290 Mbps	350 Mbps	830 Mbps	2 Gbps	2 Gbps
IPsec VPN throughput (large packets)	65 Mbps	65 Mbps	85 Mbps	100 Mbps	300 Mbps	1.0 Gbps	1.5 Gbps
IPsec VPN tunnels	128	128	256	512	1,000	2,000	3,000
AppSecure firewall throughput[8]	90 Mbps	90 Mbps	250 Mbps	300 Mbps	750 Mbps	2.0 Gbps	1.9 Gbps
IPS (intrusion prevention system)	75 Mbps[9]	75 Mbps	65 Mbps	80 Mbps	230 Mbps	800 Mbps	1 Gbps
Antivirus	25 Mbps (Sophos AV)	25 Mbps (Sophos AV)	30 Mbps (Sophos AV)	35 Mbps (Sophos AV)	85 Mbps (Sophos AV)	300 Mbps (Sophos AV)	350 Mbps (Sophos AV)
Connections per second	1,800	1,800	2,200	2,800	8,500	27,000	35,000
Maximum concurrent sessions	32 K[7]	32 K[7]	64 K[7]	96 K[7]	256 K[7]	375 K	512 K
DRAM options	2 GB DRAM	2 GB DRAM	2 GB DRAM	2 GB DRAM	2 GB DRAM	2 GB/4 GB[7] DRAM	2 GB DRAM
Maximum security policies	384	384	512	2,048	4,096	8,000	8,192
Maximum users supported	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted
Network Connectivity							
Fixed I/O	8 x 10/100	8 x 10/100 VDSL/ ADSL2+ WAN (Annex A or B)	2 x 10/100/1000 BASE-T + 6 x 10/100	8 x 10/100/1000 BASE-T	16 x 10/100/1000 BASE-T	6 x 10/100/1000 BASE-T + 4 SFP	4 x 10/100/1000 BASE-T
I/O slots	N/A	N/A	1 x SRX Series Mini-PIM	2 x SRX Series Mini-PIM	4 x SRX Series Mini-PIM	2 x SRX Series Mini-PIM, 6 x GPIM or multiple GPIM and XPIM combinations	8 x GPIM or multiple GPIM and XPIM combinations
Services and Routing Engine slots	No	No	No	No	No	No	2[10]
WAN/LAN interface options	N/A	N/A	See ordering information	See ordering information	See ordering information	See ordering information	See ordering information
Maximum number of PoE ports (PoE optional on some SRX Series models)	N/A	N/A	Up to 4 ports of 802.3af with maximum 50 W	Up to 8 ports of 802.3af/ at with maximum 120 W	Up to 16 ports of 802.3af/ at with maximum 150 W	Up to 40 ports of 802.3af/ at with maximum 247 W	Up to 48 ports of 802.3af/ at with maximum 247 W
USB	1	2	2	2	2	2	2 per SRE

	SRX100	SRX110	SRX210	SRX220	SRX240	SRX550	SRX650
Routing							
Routing (Packet Mode) PPS	100Kpps	100Kpps	150Kpps	200Kpps	300Kpps	1000Kpps	1000Kpps
BGP instances	5	5	10	16	20	56	64
BGP peers	8	8	16	16	32	192	256
BGP routes	8 K	8 K	16 K	32 K	600 K	712 K	800 K
OSPF instances	4	4	10	16	20	56	64
OSPF routes	8 K	8 K	16 K	32 K	200 K	200 K	200 K
RIP v1 / v2 instances	4	4	10	16	20	56	64
RIP v2 routes	8 K	8 K	16 K	32 K	32 K	32 K	32 K
Static routes	8 K	8 K	16 K	32 K	100 K	100 K	100 K
Source-based routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Policy-based routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Equal-cost multipath (ECMP)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Reverse path forwarding (RPF)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPsec VPN							
Concurrent VPN tunnels	128	128	256	512	1,000	2,000	3,000
Tunnel interfaces	10	10	64	64	128	456	512
DES (56-bit), 3DES (168-bit) and AES (256-bit)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MD-5, SHA-1 and SHA-2 authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Manual key, Internet Key Exchange (IKE v1+v2), public key infrastructure (PKI) (X.509)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Perfect forward secrecy (DH Groups)	1, 2, 5	1, 2, 5	1, 2, 5	1, 2, 5	1, 2, 5	1, 2, 5	1, 2, 5
Prevent replay attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dynamic remote access VPN	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPsec NAT traversal	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Redundant VPN gateways	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Number of remote access users	25 users	25 users	50 users	150 users	250 users	500 users	500 users
User Authentication and Access Control							
Third-party user authentication	RADIUS, RSA SecureID, LDAP	RADIUS, RSA SecureID, LDAP	RADIUS, RSA SecureID, LDAP	RADIUS, RSA SecureID, LDAP	RADIUS, RSA SecureID, LDAP	RADIUS, RSA SecureID, LDAP	RADIUS, RSA SecureID, LDAP
RADIUS accounting	Yes	Yes	Yes	Yes	Yes	Yes	Yes
XAUTH VPN, Web-based, 802.X authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PKI certificate requests (PKCS 7 and PKCS 10)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Certificate Authorities supported	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Virtualization							
Maximum number of security zones	10	10	12	24	64	96	128
Maximum number of virtual routers	3	3	10	15	64	128	128
Maximum number of VLANs	16	16	64	128	2,000	3,967	3,967

ANEXO C. CONFIGURACION DE LOS EQUIPOS.

CONFIGURACION DE ROUTER PRINCIPAL

```
version 12.1X46-D40.2;
system {
    time-zone America/Lima;
    authentication-order [ tacplus password ];
    root-authentication {
        encrypted-password "$1$r5H7MpiA$6oVbQzQ2HmJv0egf5hOCi0"; ## SECRET-DATA
    }
    name-server {
        200.24.191.11;
        200.62.191.11;
        200.62.191.12;
        200.24.191.12;
    }
    tacplus-server {
        200.14.241.43 {
            secret "$9$SgGlK8Nds4oGLxwYoaHk5QF/9pKvW"; ## SECRET-DATA
            source-address 190.116.112.166;
        }
    }
    accounting {
        events [ login change-log interactive-commands ];
        destination {
            tacplus {
                server {
                    200.14.241.43 {
                        secret "$9$TFnC0BEyrvApRhrlXxbs2aJDn69"; ## SECRET-DATA
                        single-connection;
                        source-address 190.116.112.166;
                    }
                }
            }
        }
    }
    login {
        user NOC {
uid 2000;
            class super-user;
            authentication {
                encrypted-password "$1$qx965ZPe$KSX2N0QHI9XrWczXisp8g0"; ## SECRET-DATA
            }
        }
        user remote {
uid 2004;
            class super-user;
        }
    }
```

```
    services {
ssh;
        telnet;
        web-management {
            http;
        }
    }
    syslog {
        archive size 100k files 3;
        user * {
            any emergency;
        }
        file messages {
            any critical;
            authorization info;
        }
        file interactive-commands {
            interactive-commands error;
        }
    }
    license {
autoupdate {
url https://ae1.juniper.net/junos/key_retrieval;
        }
    }
ntp {
        server 190.81.124.76;
    }
}
chassis {
    aggregated-devices {
ethernet {
            device-count 1;
        }
    }
}
interfaces {
    interface-range LAN_INTERNET {
        member ge-0/0/3;
        member ge-0/0/4;
        member ge-0/0/5;
        description "INTERFACE LAN INTERNET";
        unit 0 {
            family ethernet-switching {
vlan {
                    members LAN_INTERNET;
                }
            }
        }
    }
    interface-range LAN_VRF {
```

```
        member ge-0/0/6;
        member ge-0/0/7;
        description "INTERFACE LAN VRF";
        unit 0 {
            family ethernet-switching {
vlan {
                    members LAN_VRF;
                }
            }
        }
    }
    ge-0/0/0 {
        per-unit-scheduler;
vlan-tagging;
        speed 100m;
        link-mode full-duplex;
        unit 500 {
            description "Interface WAN CID RPV LITE";
vlan-id 3649;
            family inet {
                filter {
                    output policing-wan-rpvV;
                }
                address 10.10.47.78/30 {
                    primary;
                }
            }
        }
        unit 3002 {
            description "Interface WAN CID356524 INTERNET CARRIER CLASS 30Mbps";
vlan-id 3002;
            family inet {
                filter {
                    input SECURE;
                }
                sampling {
                    input;
                    output;
                }
                address 190.116.112.166/30 {
                    primary;
                }
            }
        }
    }
    ae0 {
        aggregated-ether-options {
lacp {
                active;
            }
        }
```

```
        unit 0 {
            family ethernet-switching {
                port-mode access;
vlan {
                    members LAN_INTERNET;
                }
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                filter {
                    input RESTRIC.ACCESS;
                }
            }
        }
    }
vlan {
        unit 2 {
            description "INTERFACE LAN INTERNET";
            family inet {
                sampling {
                    input;
                    output;
                }
                address 190.81.63.130/27 {
                    primary;
vrrp-group 2 {
                        virtual-address 190.81.63.129;
                        priority 200;
                        fast-interval 800;
                        preempt;
                        accept-data;
                        track {
                            interface ge-0/0/0.3002 {
                                priority-cost 100;
                            }
                        }
                    }
                }
            }
        }
        unit 3 {
            family inet {
                filter {
                    input setqosClass_VRF;
                }
                address 172.28.156.33/30 {
                    primary;
                }
```

```
        }
      }
   }
}
forwarding-options {
   sampling {
      input {
         rate 10;
         run-length 9;
         max-packets-per-second 7000;
      }
      family inet {
         output {
            flow-server 190.81.124.41 {
               port 9996;
               autonomous-system-type origin;
               no-local-dump;
               version 5;
            }
         }
      }
   }
}
routing-options {
   router-id 190.116.112.166;
   autonomous-system 64517;
}
protocols {
bgp {
      group CONN_PE {
          type external;
         description Conexion-al-PE;
         local-address 190.116.112.166;
         hold-time 30;
         log-updown;
         import RECIBIR_RUTAS;
         authentication-key "$9$okZjkCA0EhSLxwY24DjTz3n/tleWdbsWL"; ## SECRET-DATA
         export SETCOMM;
         peer-as 65210;
         neighbor 190.116.112.165;
      }
      group CONN_CPE {
         type internal;
descriptionConexion-al-CPE-Contingencia;
local-address 190.81.63.130;
         hold-time 30;
         log-updown;
         export IBGP;
         neighbor 190.81.63.131;
      }
   }
```

```
    inactive: lldp {
        interface all;
    }
rstp;
}
policy-options {
    prefix-list RED_INTERNET {
        190.81.63.128/27;
    }
    prefix-list RED_VRF {
        172.28.156.32/30;
    }
    prefix-list RED_DEFAULT {
        0.0.0.0/0;
    }
    policy-statement ENVIAR_REDES_VRF {
        term ENVIAR_RED_VRF {
            from {
                prefix-list RED_VRF;
            }
            then accept;
        }
    }
    policy-statement IBGP {
        term EXPORT {
            then accept;
        }
    }
    policy-statement RECIBIR_RUTAS {
        term PERMITIR_DEFAULT {
            from {
                prefix-list RED_DEFAULT;
            }
            then accept;
        }
        term RECHAZAR_RESTO {
            from protocol bgp;
            then reject;
        }
    }
    policy-statement SETCOMM {
        from {
            prefix-list RED_INTERNET;
        }
        then {
            community set CE-PE1;
            accept;
        }
    }
    community CE-PE1 members 12252:1200;
    }
```

```
class-of-service {
   forwarding-classes {
      queue 0 best-effort;
      queue 1 qos1;
queue 2 qos2;
queue 3 qos5;
queue 7 network-control;
}
   interfaces {
      ge-0/0/0 {
         unit 3649 {
            scheduler-map qos-map-schedV;
            shaping-rate 704k;
            rewrite-rules {
dscpSetDscpWan;
            }
         }
      }
   }
   rewrite-rules {
dscpSetDscpWan {
         forwarding-class qos1 {
            loss-priority low code-point cs1;
         }
         forwarding-class qos2 {
            loss-priority low code-point cs2;
         }
         forwarding-class qos5 {
            loss-priority low code-point cs5;
         }
         forwarding-class best-effort {
            loss-priority low code-point 000000;
         }
         forwarding-class network-control {
            loss-priority low code-point cs6;
         }
      }
   }
   scheduler-maps {
qos-map-schedV {
         forwarding-class qos2 scheduler sched-qos2V;
         forwarding-class best-effort scheduler sched-defaultV;
         forwarding-class network-control scheduler sched-network-controlV;
      }
   }
   schedulers {
      sched-qos2V {
         transmit-rate 512k;
         buffer-size percent 50;
         priority strict-high;
      }
```

```
sched-network-controlV {
        transmit-rate 64k;
        buffer-size percent 5;
        priority high;
    }
sched-defaultV {
        transmit-rate 128k;
        buffer-size {
            remainder;
        }
        priority low;
    }
  }
}
security {
  forwarding-options {
    family {
mpls {
        mode packet-based;
      }
    }
  }
}
firewall {
  family inet {
    filter setqosClass_VRF {
      term cos2 {
        from {
          source-address {
            172.28.156.32/30;
          }
        }
        then {
          loss-priority low;
          forwarding-class qos2;
          accept;
        }
      }
      term default {
        then {
          forwarding-class best-effort;
          accept;
        }
      }
    }
    filter policing-wan-rpvV {
      term qos2 {
        from {
          source-address {
            172.28.156.32/30;
          }
```

```
        }
        then {
            policer qos2-policer-rpvV;
            loss-priority low;
            accept;
        }
    }
    term default {
        then {
            loss-priority low;
            accept;
        }
    }
}
filter SECURE {
    term 1 {
        from {
            source-address {
                190.81.124.76/32;
            }
            destination-address {
                190.116.112.166/32;
            }
            protocol udp;
            port ntp;
        }
        then accept;
    }
    term 2 {
        from {
            destination-address {
                190.116.112.166/32;
                190.81.63.130/32;
            }
            protocol udp;
            port ntp;
        }
        then {
            discard;
        }
    }
    term 3 {
        then accept;
    }
}
filter RESTRIC.ACCESS {
    term WHITE.LIST {
        from {
            source-address {
                190.223.26.34/32;
                190.116.112.165/32;
```

```
                190.81.63.130/32;
            }
        }
        then accept;
    }
    term BLOCK {
        from {
            destination-port [ telnet ssh ];
        }
        then {
            log;
            reject;
        }
    }
    term PERMIT.ANY {
        then accept;
    }
  }
 }
 policer qos2-policer-rpvV {
  if-exceeding {
   bandwidth-limit 512k;
   burst-size-limit 192k;
  }
  then discard;
 }
}
routing-instances {
 VRF {
  instance-type virtual-router;
  interface ge-0/0/0.3649;
  interface vlan.3;
  routing-options {
   static {
    route 0.0.0.0/0 next-hop 10.10.47.77;
   }
   router-id 10.10.47.78;
   autonomous-system 64517;
  }
 }
}
vlans {
 LAN_INTERNET {
vlan-id 2;
  l3-interface vlan.2;
 }
 LAN_VRF {
vlan-id 3;
  l3-interface vlan.3;
}
```

CONFIGURACION DE ROUTER SECUNDARIO

```
version 12.1X46-D40.2;
system {
    host-name SAT_CAMANA_Contingencia;
    time-zone America/Lima;
    authentication-order [ tacplus password ];
    root-authentication {
        encrypted-password "$1$r5H7MpiA$6oVbQzQ2HmJv0egf5hOCi0"; ## SECRET-DATA
    }
    name-server {
        200.24.191.11;
        200.62.191.11;
        200.62.191.12;
        200.24.191.12;
    }
    tacplus-server {
        200.14.241.43 {
            secret "$9$SgGlK8Nds4oGLxwYoaHk5QF/9pKvW"; ## SECRET-DATA
            source-address 190.116.112.162;
        }
    }
    accounting {
        events [ login change-log interactive-commands ];
        destination {
            tacplus {
                server {
                    200.14.241.43 {
                        secret "$9$TFnC0BEyrvApRhrlXxbs2aJDn69"; ## SECRET-DATA
                        single-connection;
                        source-address 190.116.112.162;
                    }
                }
            }
        }
    }
    login {
        user NOC {
uid 2000;
            class super-user;
            authentication {
                encrypted-password "$1$qx965ZPe$KSX2N0QHI9XrWczXisp8g0"; ## SECRET-DATA
            }
        }
        user remote {
uid 2004;
            class super-user;
        }
    }
    services {
```

```
ssh;
        telnet;
        web-management {
            http;
        }
    }
    syslog {
        archive size 100k files 3;
        user * {
            any emergency;
        }
        file messages {
            any critical;
            authorization info;
        }
        file interactive-commands {
            interactive-commands error;
        }
    }
    license {
autoupdate {
url https://ae1.juniper.net/junos/key_retrieval;
        }
    }
ntp {
        server 190.81.124.76;
    }
}
chassis {
    aggregated-devices {
ethernet {
            device-count 1;
        }
    }
}
interfaces {
    interface-range LAN_INTERNET {
        member ge-0/0/3;
        member ge-0/0/4;
        member ge-0/0/5;
        description "INTERFACE LAN INTERNET";
        unit 0 {
            family ethernet-switching {
vlan {
                    members LAN_INTERNET;
                }
            }
        }
    }
    interface-range LAN_VRF {
        member ge-0/0/6;
```

```
        member ge-0/0/7;
        description "INTERFACE LAN VRF";
        unit 0 {
            family ethernet-switching {
vlan {
                    members LAN_VRF;
                }
            }
        }
    }
    ge-0/0/0 {
        per-unit-scheduler;
vlan-tagging;
        speed 100m;
        link-mode full-duplex;
        unit 1666 {
            description "Interface WAN CID RPV LITE";
vlan-id 1666;
            family inet {
                filter {
                    output policing-wan-rpvV;
                }
                address 10.14.0.210/30 {
                    primary;
                }
            }
        }
        unit 3003 {
            description "Interface WAN CID3571187 INTERNET CARRIER CLASS 45Mbps";
vlan-id 3003;
            family inet {
                filter {
                    input SECURE;
                }
                sampling {
                    input;
                    output;
                }
                address 190.116.112.162/30;
            }
        }
    }
    ae0 {
        aggregated-ether-options {
lacp {
                active;
            }
        }
        unit 0 {
            family ethernet-switching {
                port-mode access;
```

```
vlan {
                members LAN_INTERNET;
            }
        }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        filter {
          input RESTRICT.ACCESS;
        }
      }
    }
  }
vlan {
    unit 2 {
      description "INTERFACE LAN INTERNET";
      family inet {
        sampling {
          input;
          output;
        }
        address 190.81.63.131/27 {
          primary;
vrrp-group 2 {
                virtual-address 190.81.63.129;
                priority 150;
                fast-interval 800;
                preempt;
                accept-data;
            }
        }
      }
    }
    unit 3 {
      family inet {
        filter {
          input setqosClass_VRF;
        }
        address 172.28.154.21/30 {
          primary;
        }
      }
    }
  }
}
forwarding-options {
  sampling {
    input {
      rate 10;
```

```
            run-length 9;
            max-packets-per-second 7000;
        }
        family inet {
            output {
                flow-server 190.81.124.41 {
                    port 9996;
                    autonomous-system-type origin;
                    no-local-dump;
                    version 5;
                }
            }
        }
    }
}
routing-options {
    router-id 190.116.112.162;
    autonomous-system 64517;
}
protocols {
bgp {
        group CONN_PE {
             type external;
            description Conexion-al-PE;
            local-address 190.116.112.162;
            hold-time 30;
            log-updown;
            import RECIBIR_RUTAS;
            authentication-key "$9$okZjkCA0EhSLxwY24DjTz3n/tleWdbsWL"; ## SECRET-DATA
            export SETCOMM;
            peer-as 65210;
            neighbor 190.116.112.161;
        }
        group CONN_CPE {
            type internal;
descriptionConexion-al-CPE-Contingencia;
local-address 190.81.63.131;
            hold-time 30;
            log-updown;
            export IBGP;
            neighbor 190.81.63.130;
        }
    }
    inactive: lldp {
        interface all;
    }
rstp;
}
policy-options {
    prefix-list RED_INTERNET {
        190.81.63.128/27;
```

```
    }
    prefix-list RED_VRF {
        172.28.154.20/30;
    }
    prefix-list RED_DEFAULT {
        0.0.0.0/0;
    }
    policy-statement ENVIAR_REDES_VRF {
        term ENVIAR_RED_VRF {
            from {
                prefix-list RED_VRF;
            }
            then accept;
        }
    }
    policy-statement IBGP {
        term EXPORT {
            then accept;
        }
    }
    policy-statement RECIBIR_RUTAS {
        term PERMITIR_DEFAULT {
            from {
                prefix-list RED_DEFAULT;
            }
            then accept;
        }
        term RECHAZAR_RESTO {
            from protocol bgp;
            then reject;
        }
    }
    policy-statement SETCOMM {
        from {
            prefix-list RED_INTERNET;
        }
        then {
            community set CE-PE1;
            accept;
        }
    }
    community CE-PE1 members 12252:1201;
}
class-of-service {
    forwarding-classes {
        queue 0 best-effort;
        queue 1 qos1;
queue 2 qos2;
queue 3 qos5;
queue 7 network-control;
}
```

```
   interfaces {
      ge-0/0/0 {
         unit 1666 {
            scheduler-map qos-map-schedV;
            shaping-rate 704k;
            rewrite-rules {
dscpSetDscpWan;
            }
         }
      }
   }
   rewrite-rules {
dscpSetDscpWan {
         forwarding-class qos1 {
            loss-priority low code-point cs1;
         }
         forwarding-class qos2 {
            loss-priority low code-point cs2;
         }
         forwarding-class qos5 {
            loss-priority low code-point cs5;
         }
         forwarding-class best-effort {
            loss-priority low code-point 000000;
         }
         forwarding-class network-control {
            loss-priority low code-point cs6;
         }
      }
   }
   scheduler-maps {
qos-map-schedV {
         forwarding-class qos2 scheduler sched-qos2V;
         forwarding-class best-effort scheduler sched-defaultV;
         forwarding-class network-control scheduler sched-network-controlV;
      }
   }
   schedulers {
      sched-qos2V {
         transmit-rate 512k;
         buffer-size percent 50;
         priority strict-high;
      }
sched-network-controlV {
         transmit-rate 64k;
         buffer-size percent 5;
         priority high;
      }
sched-defaultV {
         transmit-rate 128k;
         buffer-size {
```

```
            remainder;
        }
        priority low;
    }
  }
}
security {
  forwarding-options {
    family {
mpls {
        mode packet-based;
      }
    }
  }
}
firewall {
  family inet {
    filter setqosClass_VRF {
      term cos2 {
        from {
          source-address {
            172.28.154.20/30;
          }
        }
        then {
          loss-priority low;
          forwarding-class qos2;
          accept;
        }
      }
      term default {
        then {
          forwarding-class best-effort;
          accept;
        }
      }
    }
    filter policing-wan-rpvV {
      term qos2 {
        from {
          source-address {
            172.28.154.20/30;
          }
        }
        then {
          policer qos2-policer-rpvV;
          loss-priority low;
          accept;
        }
      }
      term default {
```

```
        then {
            loss-priority low;
            accept;
        }
    }
}
filter SECURE {
    term 1 {
        from {
            source-address {
                190.81.124.76/32;
            }
            destination-address {
                190.116.112.162/32;
            }
            protocol udp;
            port ntp;
        }
        then accept;
    }
    term 2 {
        from {
            destination-address {
                190.116.112.162/32;
                190.81.63.131/32;
            }
            protocol udp;
            port ntp;
        }
        then {
            discard;
        }
    }
    term 3 {
        then accept;
    }
}
filter RESTRICT.ACCESS {
    term WHITE.LIST {
        from {
            source-address {
                190.116.112.161/32;
                190.223.26.34/32;
            }
        }
        then accept;
    }
    term BLOCK {
        from {
            destination-port [ telnet ssh ];
        }
```

```
            then {
                log;
                reject;
            }
        }
        term PERMIT.ANY {
            then accept;
        }
    }
  }
  policer qos2-policer-rpvV {
    if-exceeding {
      bandwidth-limit 512k;
      burst-size-limit 192k;
    }
    then discard;
  }
}
routing-instances {
  VRF {
    instance-type virtual-router;
    interface ge-0/0/0.1666;
    interface vlan.3;
    routing-options {
      static {
        route 0.0.0.0/0 next-hop 10.14.0.209;
      }
      router-id 10.14.0.210;
      autonomous-system 64517;
    }
  }
}
vlans {
  LAN_INTERNET {
vlan-id 2;
    l3-interface vlan.2;
  }
  LAN_VRF {
vlan-id 3;
    l3-interface vlan.3;
}
}
```

CONFIGURACION DEL FIREWALL EN CLUSTER

```
version 12.1X46-D40.2;
```

```
    groups {
        node0 {
            system {
                host-name SAT-PRINCIPAL;
                services {
                    ssh {
                        max-sessions-per-connection 32;
                    }
                }
                syslog {
                    file default-log-messages {
                        any info;
                        match "(requested 'commit' operation)|(copying configuration to juniper.save)|(commit
complete)|ifAdminStatus|(FRU power)|(FRU removal)|(FRU insertion)|(link
UP)|transitioned|Transferred|transfer-file|(license add)|(license delete)|(package -X update)|(package -X
delete)|(FRU Online)|(FRU Offline)|(plugged in)|(unplugged)|GRES";
                        structured-data;
                    }
                }
            }
            interfaces {
                fxp0 {
                    unit 0 {
                        family inet;
                    }
                }
            }
        }
        node1 {
            system {
                host-name SAT-SECUNDARIO;
            }
            interfaces {
                fxp0 {
                    unit 0 {
                        family inet;
                    }
                }
            }
        }
    }
    apply-groups "${node}";
    system {
        time-zone America/Lima;
        root-authentication {
            encrypted-password "$1$nCT7a3LJ$j978qlzsSf1TqOjy.Tre10"; ## SECRET-DATA
        }
        name-server {
            200.24.191.11;
            200.24.191.12;
            200.62.191.11;
```

```
    200.62.191.12;
}
scripts {
    commit {
        file templates.xsl;
    }
}
login {
    user adminsat {
        uid 2000;
        class super-user;
        authentication {
            encrypted-password "$1$SDjw.mFC$T4jrVVDr/oIz6cL4nf5mk."; ## SECRET-DATA
        }
    }
    user pr0y3ct0s {
        uid 2001;
        class super-user;
        authentication {
            encrypted-password "$1$lNpo0Ofa$ySr4CuiA4UN6wb1v0qyHx/"; ## SECRET-DATA
        }
    }
}
services {
    ssh;
    telnet;
    netconf {
        ssh;
    }
    web-management {
        https {
            system-generated-certificate;
        }
    }
}
syslog {
    host 172.29.55.62 {
        any any;
    }
    file SCREEN {
        any any;
        match RT_SCREEN;
        archive size 1m files 3 world-readable;
    }
    file traffic-log {
        any any;
        match RT_FLOW_SESSION;
        archive size 2m files 50 world-readable;
    }
}
```

```
}
chassis {
    cluster {
        control-link-recovery;
        reth-count 9;
        heartbeat-interval 2000;
        heartbeat-threshold 4;
        redundancy-group 0 {
            node 0 priority 254;
            node 1 priority 1;
        }
        redundancy-group 1 {
            node 0 priority 200;
            node 1 priority 199;
            preempt;
            interface-monitor {
                ge-6/0/0 weight 255;
                ge-15/0/0 weight 255;
                ge-6/0/1 weight 255;
                ge-15/0/1 weight 255;
                ge-6/0/2 weight 255;
                ge-15/0/2 weight 255;
                ge-6/0/3 weight 255;
                ge-15/0/3 weight 255;
                ge-6/0/4 weight 255;
                ge-15/0/4 weight 255;
                ge-6/0/5 weight 255;
                ge-15/0/5 weight 255;
                ge-6/0/7 weight 255;
                ge-15/0/7 weight 255;
            }
            ip-monitoring {
                global-weight 255;
                global-threshold 80;
                retry-interval 3;
                retry-count 10;
                family {
                    inet {
                        172.29.49.1 {
                            weight 80;
                            interface reth1.0 secondary-ip-address 172.29.49.15;
                        }
                        190.81.63.129 {
                            weight 80;
                            interface reth0.0 secondary-ip-address 190.81.63.150;
                        }
                    }
                }
            }
        }
    }
```

```
}
interfaces {
    ge-6/0/0 {
        gigether-options {
            redundant-parent reth0;
        }
    }
    ge-6/0/1 {
        gigether-options {
            redundant-parent reth1;
        }
    }
    fab0 {
        fabric-options {
            member-interfaces {
                ge-0/0/2;
            }
        }
    }
    fab1 {
        fabric-options {
            member-interfaces {
                ge-9/0/2;
            }
        }
    }
    reth0 {
        redundant-ether-options {
            redundancy-group 1;
        }
        unit 0 {
            description WAN-SAT;
            family inet {
                sampling {
                    input;
                    output;
                }
                address 190.81.63.132/27;
            }
        }
    }
    reth1 {
        redundant-ether-options {
            redundancy-group 1;
        }
        unit 0 {
            description LAN-SAT;
            family inet {
                address 172.29.49.30/27;
        }
    }
```

```
    }
    st0 {
        unit 5 {
            family inet {
                address 10.10.1.254/32;
            }
        }
    }
}
snmp {
    community space {
        authorization read-write;
        clients {
            190.223.26.37/32;
        }
    }
    community spaceSAT {
        authorization read-write;
    }
    trap-group space {
        version v2;
        destination-port 161;
        targets {
            190.223.26.37;
            172.29.55.114;
        }
    }
}
routing-options {
    static {
        route 172.29.50.0/25 next-hop 172.29.49.1;
        route 172.29.50.128/25 next-hop 172.29.49.1;
        route 172.29.51.0/25 next-hop 172.29.49.1;
        route 172.29.51.128/25 next-hop 172.29.49.1;
        route 172.29.52.0/25 next-hop 172.29.49.1;

        route 192.168.36.0/24 next-hop 172.29.49.1;
        route 192.168.38.0/24 next-hop 172.29.49.1;
        route 192.168.40.0/24 next-hop 172.29.49.1;
        route 192.168.42.0/24 next-hop 172.29.49.1;
        route 192.168.44.0/24 next-hop 172.29.49.1;
        route 192.168.46.0/24 next-hop 172.29.49.1;
        route 192.168.48.0/24 next-hop 172.29.49.1;
        route 192.168.52.0/24 next-hop 172.29.49.1;
        route 192.168.54.0/24 next-hop 172.29.49.1;
        route 192.168.81.0/24 next-hop 172.29.49.1;
        route 192.168.132.0/25 next-hop 172.29.49.1;
        route 172.29.70.0/29 next-hop 172.29.49.1;
        route 172.25.60.2/32 next-hop 192.168.50.2;
        route 172.25.2.15/32 next-hop 192.168.50.2;
        route 172.25.2.170/32 next-hop 192.168.50.2;
```

```
            route 172.25.2.171/32 next-hop 192.168.50.2;
            route 172.25.4.10/32 next-hop 192.168.50.2;
        }
    }
    protocols {
        lldp {
            interface all;
        }
    }
    security {
        alarms {
            potential-violation {
                authentication 3;
                replay-attacks {
                    threshold 100;
                }
                security-log-percent-full 80;
            }
        }
        ssh-known-hosts {
            host 190.223.26.37 {
                rsa-key
AAAAB3NzaC1yc2EAAAADAQABAAABAQC8yEXCLI9Zm47TIZluW7FXnEjYtgPKUO+alkbCXdb
1VhtXZZDPIFQt4ofsDB1E8UzxCEIAXaUpWizZrb6WMOI06nwuxFMV97XM1AJaVE9IRev/q4Z5Fgr
Qfvpl8QJvA8AdsGRH9Xs/+aYLmi/brQ+ZNZlmzXN6uJv/VHbVKfXKkfrnV7As5qnZHkqPzTB1cu5gp
UYH5WcWsSrPTwqAp9wK7mr4YFiFHFroGKz6RcsDdCJ7p07wKwaVZXMkpc8MGMdFQ0V93z/xod
hZOuMF7pFV6e89PeQExBxpRW+H5Cmw6pEhlVSQ3Hr8GY9o42MNFabx1G6eytXnhRfdnchFgTC9;
            }
        }
        ike {
            traceoptions {
                file IKE size 100k;
                flag all;
            }
            proposal PROPOSAL-NCR {
                authentication-method pre-shared-keys;
                dh-group group2;
                authentication-algorithm sha1;
                encryption-algorithm 3des-cbc;
                lifetime-seconds 28800;
            }
            policy POLICY-NCR {
                mode main;
                proposals PROPOSAL-NCR;
                pre-shared-key ascii-text "$9$IaQRylX7-w2o1RVsYgJZ36/tBIylMN-wBI"; ## SECRET-
DATA
            }
            gateway GATEWAY-NCR {
                ike-policy POLICY-NCR;
                address 192.127.94.73;
                external-interface reth0.0;
```

```
    }
}
ipsec {
    traceoptions {
        flag all;
    }
    proposal PROPOSAL-NCR-PHASEII {
        protocol esp;
        authentication-algorithm hmac-sha1-96;
        encryption-algorithm 3des-cbc;
        lifetime-seconds 3600;
    }
    policy POLICY-NCR-PHASEII {
        perfect-forward-secrecy {
            keys group2;
        }
        proposals PROPOSAL-NCR-PHASEII;
    }
    vpn VPN-NCR-PHASEII {
        bind-interface st0.5;
        vpn-monitor;
        ike {
            gateway GATEWAY-NCR;
            proxy-identity {
                local 13.6.11.0/24;
                remote 192.127.229.32/32;
            }
            ipsec-policy POLICY-NCR-PHASEII;
        }
        establish-tunnels immediately;
    }
}
alg {
    dns disable;
    ftp inactive: disable;
    h323 disable;
    mgcp disable;
    msrpc disable;
    sunrpc disable;
    rsh disable;
    rtsp disable;
    sccp disable;
    sql disable;
    talk disable;
    tftp disable;
    pptp inactive: disable;
    ike-esp-nat {
        enable;
    }
}
nat {
```

```
        source {
            rule-set LAN-TO-WAN {
                from zone LAN;
                to zone WAN;
                rule no_nat_ncr {
                    match {
                        source-address 172.29.56.33/32;
                        destination-address 192.127.224.22/32;
                    }
                    then {
                        source-nat {
                            off;
                        }
                    }
                }
                rule r1 {
                    match {
                        source-address [ 192.168.42.75/32 172.29.66.113/32 172.29.58.8/29
192.168.132.116/32 192.168.132.117/32 172.29.55.65/32 172.29.53.58/32 172.29.53.4/32 ];
                        destination-address 0.0.0.0/0;
                    }
                    then {
                        source-nat {
                            interface;
                        }
                    }
                }
        destination {
            pool 172_29_55_24 {
                address 172.29.55.24/32;
            }
            pool 172_29_55_25 {
                address 172.29.55.25/32;
            }
            pool POOL_172_29_55_189 {
                address 172.29.55.189/32 port 443;
            }
            pool POOL_172_29_55_199 {
                address 172.29.55.199/32;
            }
            rule-set MML-TO-LAN {
                from zone MML;
                rule MML-IPS {
                    match {
                        destination-address 192.168.59.245/32;
                    }
                    then {
                        destination-nat {
                            pool {
                                172_29_55_24;
                            }
```

```
            }
        }
    }
    rule MML-IPS2 {
        match {
            destination-address 192.168.11.22/32;
        }
        then {
            destination-nat {
                pool {
                    172_29_55_25;
                }
            }
        }
    }
}

proxy-arp {
    interface st0.5 {
        address {
            13.6.11.10/32;
            13.6.11.26/32;
        }
    }
    interface reth4.0 {
        address {
            10.119.16.135/32;
            10.119.16.161/32;
            10.119.16.162/32;
            10.119.16.163/32;
            10.119.16.164/32;
            10.119.16.165/32;
            10.119.16.166/32;
            10.119.16.167/32;
        }
    }
    interface reth0.0 {
        address {
            190.81.63.134/32;
            190.81.63.135/32;
            190.81.63.136/32;
            190.81.63.137/32;
            190.81.63.138/32;
            190.81.63.139/32;
            190.81.63.140/32;
            190.81.63.141/32;
            190.81.63.142/32;
            190.81.63.143/32;
            190.81.63.144/32;
            190.81.63.146/32;
            190.81.63.148/32;
```

```
                190.81.63.149/32;
            }
        }

    policies {
        from-zone LAN to-zone WAN {
            policy EXTERNAL_FTP {
                match {
                    source-address [ 172.29.55.56 172.29.55.58 ];
                    destination-address 190.81.44.108;
                    application [ junos-ftp FTP_20 ];
                }
                then {
                    permit;
                }
            }
            policy SOURCEFIRE_AMP {
                match {
                    source-address [ IPS_DEFENSE_CENTER IPS_SENSOR ];
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                }
            }
            policy FREE_TRAFFIC_REDES {
                match {
                    source-address [ Internet_Libre RED_WIFI_PRUEBA1 FEBAN_DATCO ];
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
        from-zone RED_MOVIL to-zone DMZ1 {
            policy PAPELETAS_ELECTRONICAS {
                match {
                    source-address [ TERMINALES_MOVILES TERMINALES_MOVILESII
TERMINALES_MOVILESIII ];
                    destination-address [ WEBIIS_PRE01 WEBIIS_DES01 ];
                    application [ junos-ping junos-http ];
                }
                then {
                    permit;
                }
            }
        }
        from-zone WAN to-zone LAN {
```

```
    policy ANTISPAM {
        match {
            source-address any;
            destination-address 172.29.55.50;
            application junos-smtp;
        }
        then {
            permit;
        }
    }
    policy OWA {
        match {
            source-address any;
            destination-address SATMAILEXC02;
            application junos-https;
        }
        then {
            permit;
        }
    }
}
from-zone WAN to-zone DMZ1 {
    policy SATFTP {
        match {
            source-address MTC-FTP;
            destination-address 172.29.55.190;
            application junos-ftp;
        }
        then {
            permit;
            log {
                session-init;
                session-close;
            }
        }
    }
from-zone DMZ1 to-zone WAN {
    policy WEBIISPROD-TO-FTPMTC {
        match {
            source-address WEBIISPROD01;
            destination-address FTPMTC;
            application any;
        }
        then {
            permit;
        }
    }

from-zone MAG to-zone DMZ1 {
    policy ALLOT {
        match {
```

```
            source-address [ 10.10.10.10 10.10.10.11 ];
            destination-address [ 172.29.55.12 172.29.55.33 ];
            application any;
        }
        then {
            permit;
        }
    }
    policy DENY {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            deny;
        }
    }
  }
}
zones {
  security-zone LAN {
    address-book {
        address 172.29.52.26 172.29.52.26/32;
        address 172.29.53.4 172.29.53.4/32;
        address 172.29.55.27 172.29.55.27/32;
        address 172.29.55.39 172.29.55.39/32;
        address 172.29.55.50 172.29.55.50/32;
        address 172.29.55.51 172.29.55.51/32;
        address 172.29.55.10 172.29.55.10/32;
        address satms03 172.29.55.72/32;
        address SATIBC 172.29.55.52/32;
        address 172.29.55.12 172.29.55.12/32;
        address p6a-oci01 172.29.66.113/32;
        address 192.168.1.4 192.168.1.4/32;
        address 192.168.1.5 192.168.1.5/32;
        address 192.168.1.6 192.168.1.6/32;
        address 192.168.1.7 192.168.1.7/32;
        address 192.168.1.8 192.168.1.8/32;
        address 192.168.1.9 192.168.1.9/32;
        address 192.168.1.10 192.168.1.10/32;
        address 192.168.1.11 192.168.1.11/32;
        address 192.168.1.12 192.168.1.12/32;

    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
```

```
    }
    interfaces {
        reth1.0;
    }
}
security-zone MML {
    address-book {
        address 192.168.71.2 192.168.71.2/32;
        address 192.168.71.9 192.168.71.9/32;
        address 192.168.71.199 192.168.71.199/32;
        address 192.168.59.241 192.168.59.241/32;
        address 192.168.59.242 192.168.59.242/32;
        address 192.168.59.243 192.168.59.243/32;
        address 192.168.59.244 192.168.59.244/32;
        address 192.168.59.245 192.168.59.245/32;
        address 192.168.11.20 192.168.11.20/32;
        address 192.168.11.21 192.168.11.21/32;
        address 192.168.11.22 192.168.11.22/32;
        address 192.168.11.23 192.168.11.23/32;
        address 192.168.11.24 192.168.11.24/32;
        address 192.168.11.25 192.168.11.25/32;
        address 192.168.11.26 192.168.11.26/32;
        address 192.168.11.27 192.168.11.27/32;

    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        reth3.0;
    }
}
security-zone VISA {
    address-book {
        address 10.118.253.101 10.118.253.101/32;
    }
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        reth4.0;
        }
```

```
}
security-zone DMZ1 {
    address-book {
        address RedDMZVPNSSL 172.29.55.128/25;
        address 172.29.55.206 172.29.55.206/32;
        address 172.29.55.194 172.29.55.194/32;
        address 172.29.55.205 172.29.55.205/32;
        address 172.29.55.203 172.29.55.203/32;
        address 172.29.55.202 172.29.55.202/32;
        address 172.29.55.200 172.29.55.200/32;
        address 172.29.55.201 172.29.55.201/32;
        address 172.29.55.207 172.29.55.207/32;
        address 172.29.55.190 172.29.55.190/32;
        address 172.29.55.191 172.29.55.191/32;
        address WEBIIS_PRE01 172.29.55.187/32;
        address WEBIIS_DES01 172.29.55.188/32;
        address WEBIIS_PROD01_WS 172.29.55.199/32;
        address app3_sat_gob_pe 172.29.55.199/32;
        address 172.29.55.33 172.29.55.33/32;
        address 172.29.55.12 172.29.55.12/32;
        address-set WEBIISPROD01 {
            address 172.29.55.206;
            address 172.29.55.194;
            address 172.29.55.205;
            address 172.29.55.203;
            address 172.29.55.202;
            address 172.29.55.200;
            address 172.29.55.201;
            address 172.29.55.207;
            address app3_sat_gob_pe;
        }
    }
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        reth5.0;
    }
}
security-zone DMZ3 {
    address-book {
        address 192.168.72.4 192.168.72.4/32;
    }
    host-inbound-traffic {
        system-services {
            all;
```

```
        }
        protocols {
            all;
        }
    }
    interfaces {
        reth6.0;
    }
}
security-zone BANCARRED {
    address-book {
        address ASBANC-DES 172.25.32.190/32;
        address ASBANC-PRO 172.25.120.190/32;
        address ASBANC-CON 172.25.121.190/32;
        address CAJA_METRO-DES 172.25.60.100/32;
        address BBVA-DES 172.25.16.22/32;
        address SCOTIABANK-DES 172.25.5.107/32;
        address BN-DES1 172.25.47.20/32;
        address BN-DES2 172.25.47.21/32;
        address BBVA-PRE 172.25.16.92/32;
        address BN-PRE1 172.25.47.24/32;
        address BN-PRE2 172.25.47.26/32;

    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        reth2.0;
    }
}
security-zone MAG {
    address-book {
        address RED_MAG 10.10.10.0/24;
        address 10.10.10.10 10.10.10.10/32;
        address 10.10.10.11 10.10.10.11/32;
    }
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        reth7.0;
```

```
    }
}
security-zone VPN-NCR {
    interfaces {
        st0.5 {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
        }
    }
}
security-zone DMZ;
security-zone RED_MOVIL {
    address-book {
        address TERMINALES_MOVILES 10.56.240.128/25;
        address TERMINALES_MOVILESII 10.157.59.128/25;
        address TERMINALES_MOVILESIII 10.200.71.33/32;
    }
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        reth8.0;
    }
}
security-zone WAN {
    address-book {
        address 190.81.44.108 190.81.44.108/32;
        address RUSIA-01 2.60.0.0/14;
        address RUSIA-02 2.92.0.0/14;
        address RUSIA-03 5.0.0.0/8;
        address RUSIA-04 31.0.0.0/8;
        address RUSIA-05 37.0.0.0/8;
        address RUSIA-06 46.0.0.0/8;
        address RUSIA-07 62.0.0.0/8;
        address RUSIA-08 77.0.0.0/8;
        address RUSIA-09 78.0.0.0/8;
        address RUSIA-10 79.0.0.0/8;
        address RUSIA-11 80.0.0.0/8;
        address RUSIA-12 81.0.0.0/8;
        address RUSIA-13 82.0.0.0/8;
```

```
            address RUSIA-14 83.0.0.0/8;
            address RUSIA-15 84.0.0.0/8;
            address RUSIA-16 85.0.0.0/8;
            address RUSIA-17 86.0.0.0/8;
            address RUSIA-18 87.0.0.0/8;

        inactive: screen untrust-screen;
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            reth0.0;
        }
    }
  }
}
applications {
  application FTP_20 {
    protocol tcp;
    destination-port 20;
  }
  application TCP_8080 {
    protocol tcp;
    destination-port 8080;
  }
  application TCP_3272 {
    protocol tcp;
    destination-port 3272;
  }
  application RDP_TCP_3389 {
    protocol tcp;
    destination-port 3389;
  }
  application RDP_UDP_3389 {
    protocol udp;
    destination-port 3389;
  }
  application UDP_161 {
    protocol udp;
    destination-port 161;
  }
  application UDP_162 {
    protocol udp;
    destination-port 162;
  }
  application SFTP_1122 {
```

```
        protocol tcp;
        destination-port 1122;
    }
    application VISIONAREA_8000 {
        protocol tcp;
        destination-port 8000;
    }
    application-set RDP {
        application RDP_TCP_3389;
        application RDP_UDP_3389;
    }
}
```