1. Anexo I

Tabla de Contenido

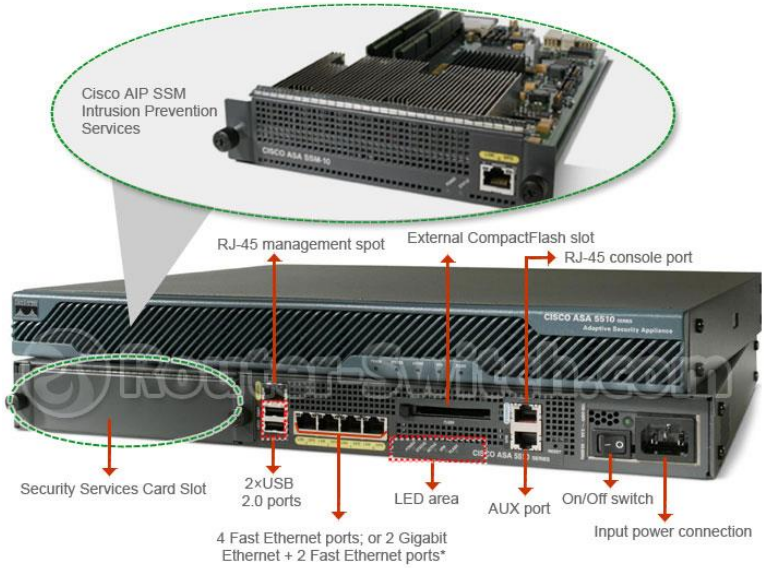
1.1. Introducción al Anexo I

En este anexo podremos encontrar la información respecto a la seguridad de red en cuestión de Firewall, además los cálculos para la utilización de UPS y por último la selección del servicio de internet.

1.2. Desarrollo del Anexo I

1.2.1. Seguridad – Firewall

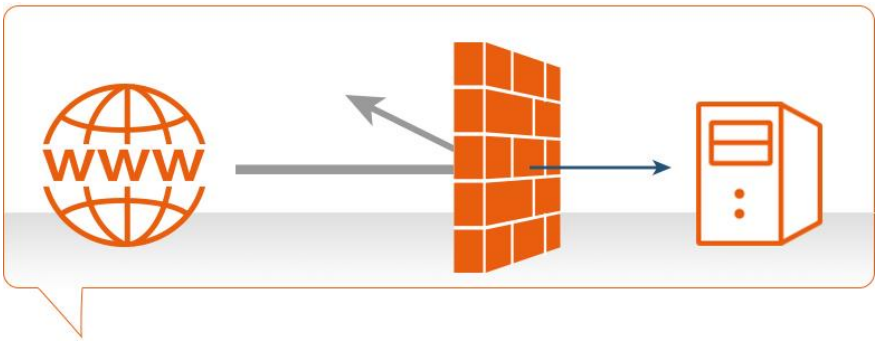
El Firewall que vamos a implementar para la mutualista es **Cisco ASA5510-SEC-BUN-K9 ASA 5510 Security Plus Firewall** el cual será implementado una unidad por piso para lograr la protección de la red en su totalidad.



Cisco ASA 5510 Adaptive Security Appliance ASA5510-BUN-K9 está diseñado para proteger las redes de las medianas, grandes empresas y las empresas a distancia, oficinas sucursales de una manera fácil de implementar y rentable. El Cisco ASA 5510 tiene firewall de alto rendimiento, servicios de VPN y cinco puertos 10/100 Fast Ethernet integrados. También es compatible con la prevención de intrusiones de alto rendimiento y servicios de mitigación de gusano a través de la AIP SSM, o los servicios integrales de protección de software malicioso a través del CSC SSM, de la que los módulos hacen ASA5510-BUN-K9 una excelente opción para los diferentes negocios que requieren.

LED	Color	State	Description
Power	Green	On	The system has power
Status	Green	Flashing	The power-up diagnostics are running or the system is booting
		Solid	The system has passed power-up diagnostics
	Amber	Solid	The power-up diagnostics have failed
Active	Green	Solid	This unit is the Active unit in the failover pair
	Amber	Solid	This unit is the Standby unit
VPN	Green	Solid	A VPN tunnel has been established
Flash	Green	Solid	The CompactFlash is being accessed

Firewall ASA5510-BUN-K9	
Firewall Users	Unlimited
Maximum firewall throughput (Mbps)	300
Maximum connections	50,000
Maximum connections/second	6,000
Packets per second (64 byte)	190,000
Application-layer security	Yes
Layer 2 transparent firewalling	Yes
Security contexts (included/maximum)[3]	0/0
GTP/GPRS inspection[3]	Not available
VPN	
Maximum 3DES/AES VPN throughput (Mbps)	170
Maximum site-to-site and remote access IPsec VPN user sessions	250
SSL user session license included	2
Maximum SSL VPN user sessions[1]	250
VPN clustering and load balancing	Not available
UTM Features Included	
Intrusion Prevention Included (Performance)	No
Content Security [anti-virus, anti-spyware, file blocking, anti-spam, anti-phishing, and URL filtering] (Max users)	No
Other Features	
Integrated ports[2]	5-10/100
Maximum virtual interfaces (VLANs)	50 (trunking enabled)
High availability support[4]	Not supported

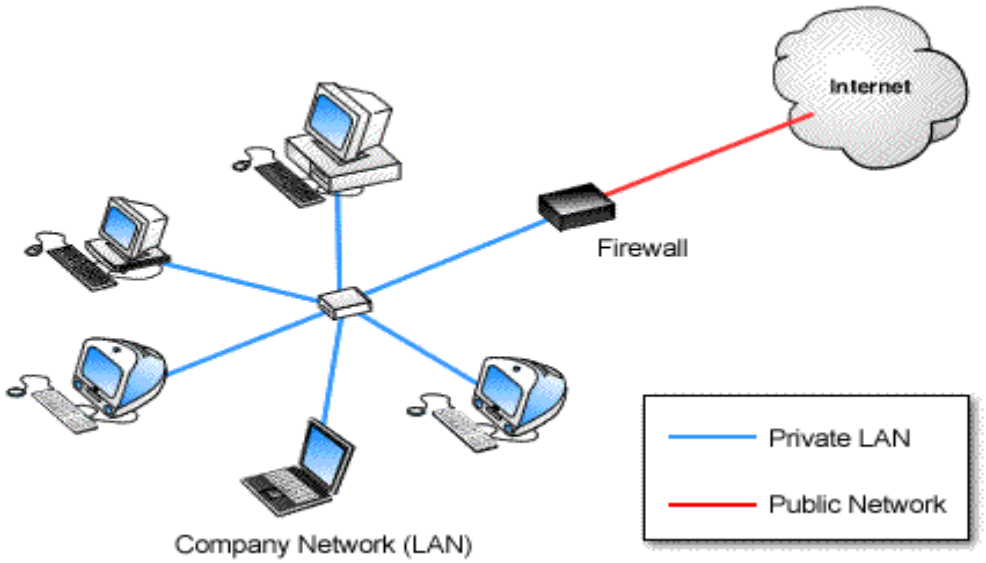


Utilizamos firewall en nuestra red debido a que es una herramienta de software o hardware que tiene como propósito filtrar las conexiones que ingresan a la red interna de la organización, así como también las conexiones de red que se dirigen hacia el exterior de la misma. Se implementa como un mecanismo de control de acceso lógico.

De esta manera, evita que usuarios de Internet que no han sido autorizados para ingresar a la red de la empresa puedan tener acceso a la misma o que miembros de la organización accedan a servicios externos para los cuales no han sido autorizados.

Entonces, ¿dónde radica la importancia de esto? El firewall opera como un filtro que examina todos los paquetes que se dirigen hacia la red corporativa y compara la información del encabezado con reglas previamente establecidas. Si la dirección IP y el puerto son válidos de acuerdo con las reglas, el paquete es entregado, en caso contrario se desecha. La misma operación es realizada con los paquetes que son enviados desde interior hacia Internet.

Por lo tanto, al desechar paquetes que no están permitidos y en consecuencia evitar conexiones que no son válidas de acuerdo a las reglas, el firewall puede evitar la propagación de códigos maliciosos a través de la red, accesos no autorizados o posibles intrusiones de terceros a la red corporativa.



http://www.router-switch.com/asa5510-bun-k9-p-610.html?gclid=CjwKEAjw1_KwBRDEz_WvncL4jGwSJAAEym0dDsKwJYafZR94QY0pFCqCMg2-gr6MjXV4rx9P_3TVGBoCRpvw_wcB

IPTABLES

Herramienta de cortafuegos que permite no solamente filtrar paquetes, sino también realizar traducción de direcciones de red para IPV4 o mantener los registros log.

Iptables es una herramienta de espacio de usuarios mediante la cual el administrador puede definir políticas de filtrado del tráfico que circula por la red.

El cortafuego utilizado para gestionar las conexiones en Linux es iptables. Las posibilidades de iptables son prácticamente infinitas y un administrador que quiera sacarle el máximo provecho, puede realizar configuraciones extremadamente complejas. Iptables permite crear reglas que analizarán los paquetes de datos que entran, salen o pasan por nuestra máquina, y en función de las condiciones que establezcamos, tomaremos una decisión que normalmente será permitir o denegar que dicho paquete siga su curso.

Una forma sencilla de trabajar con iptables es permitir las comunicaciones que nos interesen y luego denegar el resto de las comunicaciones. Lo que se suele hacer es definir la política por defecto aceptar (ACCEPT), después crear reglas concretas para permitir las comunicaciones que nos interesen y finalmente, denegar el resto de comunicaciones. Lo mejor será crear un script en el que dispondremos la secuencia de reglas que queremos aplicar en nuestro sistema.

En resumen, podemos afirmar que utilizaremos la filosofía restrictiva de firewall.

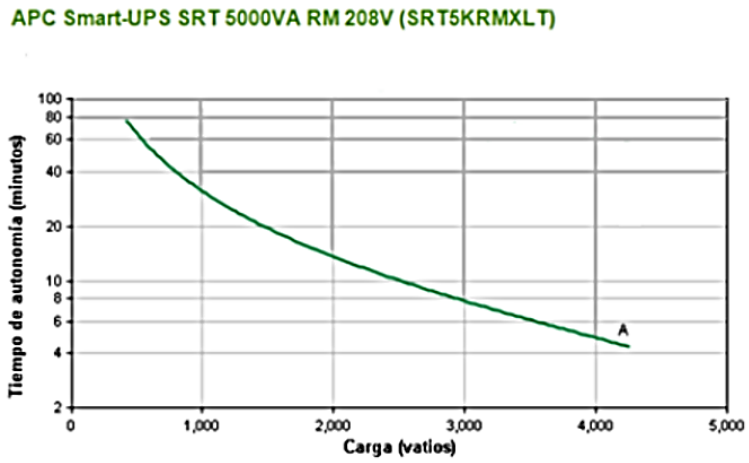
1.2.2. Ups – Cálculos

AUTONOMIA UPS

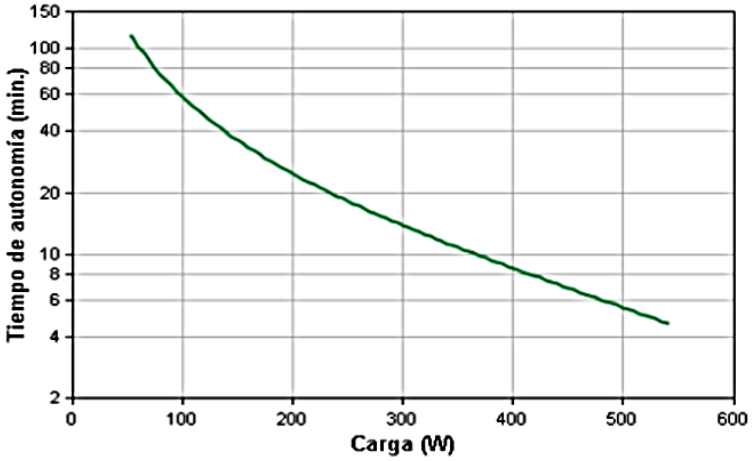
A continuación vamos a mostrar un gráfico con la autonomía en minutos de las UPS a instalar según los Vatios que consume.

Estos gráficos están basados en datos de tiempo de autonomía de mediciones reales. Todas las mediciones se han llevado a cabo con baterías nuevas totalmente cargadas. Los tiempos de autonomía reales pueden variar con respecto a los valores de este gráfico. Los tiempos de autonomía reales dependen de diversas variables como la edad de la batería, el nivel de carga de la batería, las condiciones atmosféricas y las características de la carga conectada.

UPS Autonomía 5000



UPS autonomía 900



1.2.3. Contratación Internet

La conexión a internet será mediante ANTEL usando el plan Internet CORPORATIVO:

Internet Corporativo

Es un servicio orientado a medianas y grandes empresas, que buscan un acceso a Internet de alta calidad, confiabilidad, disponibilidad y flexibilidad para su uso corporativo.

Se implementa en la red MPLS (MultiprotocolLabelSwitching) de última generación de Antel.

Ofrece acceso permanente a Internet para conectividad IP, con la mejor combinación precio-beneficio de forma de proveer la velocidad y herramientas necesarias para aumentar la productividad de las empresas.

En Internet Corporativo todo el tráfico es clasificado con una única clase de servicio en toda la red, la cual cuenta con una alta prioridad garantizando la salida internacional.

Características

- Permite la conexión permanente de su empresa a Internet mediante una conexión ruteada.
- Se implementa en la Red Ethernet/MPLS multiservicio de última generación de Antel.
- Servicio flexible y escalable.
- Utiliza cobre o fibra óptica como medios de acceso.
- Antel instala y administra un router en su empresa.
- Se entrega el servicio en una interfaz de red Ethernet RJ45.
- Se adjudican hasta 29 IPs públicas fijas (prefijo /27).

Gestión

Antel realiza la operación, mantenimiento y supervisión del servicio utilizando su plataforma de gestión centralizada, en régimen de 24x7.

Beneficios para su empresa

- Flexibilidad para adaptarse a las necesidades futuras.
- Brinda alta disponibilidad y confiabilidad.

- Amplia gama de velocidades desde 2 Mbps hasta 100 Mbps.
- Tráfico simétrico.
- Se brinda la posibilidad de contratar el servicio con redundancia
- Su empresa tiene la posibilidad de monitorear el tráfico a través de Portal de Gestión de Servicios para Empresas de Antel
- Todos los equipos son instalados y administrados por el Centro de Operación y Mantenimiento de Antel, el cual opera las 24 horas del día los 365 días del año.
- Se brinda utilizando la mejor conexión internacional, basada en la contratación de capacidad a diferentes proveedores y una óptima utilización de los anillos de fibra existentes en la región.
- Los anillos de fibra óptica nacionales e internacionales, tanto terrestres como submarinos, son redundantes y utilizan tecnologías de última generación.

Tarifa de Conexión

Tarifa de Conexión por Cobre y FTTH

Velocidad	Tarifa de conexión en $ sin impuestos
40 Mbps	15.800

1.2.4. Elementos Pasivos y activos

A continuación se detallaran un listado con los componentes pasivos y activos:

Pasivos:

- Cables: Su función será la de interconectar los componentes activos, y también serán el canal por el cual viajen los datos.
- Outlet doble: Su función será la de vincular el cable de conexión de un ordenador con el cable de conexión de un Rack.
- Patch panel: Es el elemento encargado de recibir los cables de un sistema de cableado estructurado, también será de utilidad para la organización de las conexiones de la red, permitiendo con esto que los elementos relacionados con red puedan ser fácilmente incorporados al sistema.

- Fichas RJ45: Es el conector que se coloca en los extremos de los cables UTP de par trenzado, con el cual se generan los denominados cables “patchcord”.
- Ductos: Estructuras con forma de canales, los cuales se emplean para la protección y enrutamiento del cableado de una red y cableado eléctrico.

Activos:

- Switch: Un conmutador o switch es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes (bridges), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.
- Router: El enrutador (calco del inglés router), direccionador, ruteador o encaminador es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). Un enrutador es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la mejor ruta que debe tomar el paquete de datos.
- Tarjeta de Red: Es un conjunto de circuitos integrados que se inserta en una de las ranuras de expansión de la placa base y cuya función es controlar la conexión de una o más computadores con la finalidad de compartir información.
- Modem Adsl: Encargado de enviar una señal y recibir la señal modulada, este permite el acceso a internet.

- Servidor: Un servidor es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.