ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DISEÑO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS MEDIANTE FIREWALL, AAA, IPS Y SIEM"

INFORME DE PROYECTO INTEGRADOR

Previo a la obtención del Título de:

LICENCIADO EN REDES Y SISTEMAS OPERATIVOS

AUTORES

JORGE LUIS CHALÉN PINCAY
ERICK PAUL CHÁVEZ LÓPEZ

GUAYAQUIL – ECUADOR

AÑO: 2015

AGRADECIMIENTO

Agradezco a Dios por permitirme llegar hasta estas instancias de mi formación profesional, a mis padres que fueron el apoyo constante y la motivación de cada día. Un agradecimiento especial a los profesores que con su sabiduría y conocimiento aportaron para poder cumplir este objetivo.

Jorge Luis Chalén Pincay

Agradezco a Dios y a mi familia por todo el apoyo brindado hasta esta etapa de mi vida, a los profesores y compañeros de la ESPOL que sin lugar a dudas contribuyeron con cada paso de mi formación profesional.

Erick Paúl Chávez López

DEDICATORIA

Dedico este proyecto a todos los que supieron depositar su confianza en mis capacidades, quedando demostrado que con esfuerzo y perseverancia se logra todo objetivo.

Jorge Luis Chalén Pincay.

A Dios, mis padres Stalin y Marcela, mi hermano Oscar y a toda la familia de la ESPOL con la que se compartió muchas vivencias y conocimientos.

Erick Paúl Chávez López.

TRIBUNAL DE EVALUACIÓN

Msg. Robert Andrade Troya

PROFESOR EVALUADOR

Msc. Jorge Magallanes

PROFESOR EVALUADOR

DECLARACIÓN EXPRESA

"La responsabilidad y la autoría del contenido de este Trabajo de Titulación, nos corresponde exclusivamente; y damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

Jorge Luis Chalén Pincay

Erick Paúl Chávez López

RESUMEN

En el presente proyecto se describe las principales causas de inseguridad que se han presentado en la compañía VENSUR S.A tales como acceso de intrusos a la red, el robo de información, la suplantación de identidad y muchos otros que han provocado inestabilidad y desconfianza en la información que se procesa a diario. Es por esto que proponemos cuatro mecanismos de seguridad de red que ayudarán en el control y en la gestión de la administración de la información. Así tenemos la aplicación del Firewall (Corta fuego), IPS (Sistema de Prevención de Intrusos), Protocolo AAA (Autenticación, Autorización y Contabilización) y el SIEM (Sistema de Información y Administración de Eventos).

En el primer capítulo se abarca todo sobre el análisis actual de la infraestructura de red, detallando los problemas encontrados con sus posibles causas y los efectos que estos producen. Así también se incluye la descripción de cada una de las redes que componen a la compañía para poder determinar con mayor exactitud la magnitud de los posibles daños causados por la falta de seguridad en la información.

En el segundo capítulo tratamos acerca de la solución propuesta, en donde describimos cada una de las opciones a utilizar para mitigar las inseguridades de red presentadas. Así tenemos la solución de aplicación de Firewall, para poder controlar el tráfico de información que entra y sale de la red, por medio de restricciones y bloqueos que ayudarán a mantener la red más segura. Otra solución es la aplicación de IPS, este mecanismo ayudará a controlar el acceso a la red por medio de reglas o políticas establecidas, de esta manera evitamos los posibles ataques de acceso a la red y a ayudará a monitorear las vulnerabilidades encontradas. Nuestra siguiente solución es por medio de la aplicación del protocolo AAA, en donde aseguramos el correcto acceso a los equipos de comunicación estableciendo niveles de privilegios para su administración. Por último proponemos la aplicación de un Sistema de Información y Administración de Eventos (SIEM), el cual nos permitirá monitorear en tiempo real todos los eventos o registros que se originan en la red, a la vez funciona como un IDS (Sistema de detección de intrusos) por sus características a aparte de monitorear puede determinar si algún evento suscitado es provocado por algún intruso.

En el tercer capítulo describimos todo el plan de trabajo y el estudio económico que se requiere para realizar la implementación de la solución propuesta. Así mismo se incluye sus beneficios, ventajas y la garantía del proyecto.

Por último se incluye en el cuarto capítulo la descripción de los resultados por obtener con la aplicación de nuestra propuesta, detallando por cada opción sus beneficios y método de trabajo dando las mejores recomendaciones para poder obtener los mejores resultados.

ÍNDICE GENERAL

Contenido

CAPÍTULO 1

1. SEGURIDADES EN UNA RED WAN

En este capítulo se tratará sobre las diferentes amenazas que ha sufrido la compañía VENSUR S.A tales como:

- Códigos Maliciosos: virus, gusanos y caballo de Troya.
- Suplantación de identidad.
- Ataque de acceso.
- Denegación de servicios.

Es por esto que dedicamos este capítulo al análisis de las vulnerabilidades para establecer estrategias de protección. Entre los daños más relevantes tenemos: **[8]**

- Interrupción del negocio
- Pérdida de productividad
- Pérdida de privacidad
- Robo de información
- Pérdida de confianza

Por estas causas hemos visto la necesidad de implementar algunos mecanismos que ayuden al control y manejo de la información.

1.1. Objetivos

1.1.1. Objetivo General

Analizar las distintas vulnerabilidades que se pueden presentar en cada una de las redes LAN en donde nos permita aplicar algunos mecanismos de seguridad, tales como el firewall, IPS, AAA y SIEM con la finalidad de asegurar la confidencialidad, integridad y disponibilidad de la información del sistema.

1.1.2. Objetivos Específicos

Los objetivos específicos del presente trabajo son:

- Realizar un análisis de los riesgos de seguridad de la red actual para determinar la importancia de la protección.
- Proponer un sistema de seguridad haciendo uso de un cortafuego, IPS, normas AAA y SIEM para fortalecer la seguridad de la red.
- Detallar la configuración de los mecanismos de seguridad propuestos.
- Describir ventajas y desventajas de cada mecanismo de seguridad que se propone.
- Elaborar un plan de trabajo y realizar un presupuesto para la implementación de esta solución.

1.2. Análisis de los riesgos de seguridad de la red actual

Puesto que la compañía VENSUR S.A ha sufrido en los últimos años distintos tipos de ataques a la red, los cuales han provocado daños en el normal funcionamiento de los procesos, vemos la necesidad de realizar un análisis de estos riesgos de seguridad de red para determinar cuáles son sus posibles causas.

Un registro llevado por el actual administrador de la red nos brinda unos datos estadísticos en donde podemos observar la cantidad de incidentes registrados en la red actual desde el año 2005 hasta el 2014.

El detalle de la información proporcionada es la siguiente:

- En el 2005 se reportaron un aproximado de 100 incidentes en donde intervienen factores como amenazas de red, de ataques como la denegación de servicios.

- En el 2006 se reportaron un aproximado de 150 incidentes en donde se reflejan amenazas físicas como daños en equipos de comunicación y equipos de usuarios.
- En el 2007 se obtuvo un aproximado de 210 registros de anomalías en los que destacan la pérdida de información, bloqueos de cuentas y más.
- En el 2008 se registró un aproximado de 315 anomalías, en este año se incrementaron las sucursales, pues antes existían solo 2. Aquí se registraron amenazas físicas y lógicas.
- En el 2009 se obtuvo un registro de 350 incidentes en los que resaltan los ataques de suplantación de identidad y los ataques por códigos maliciosos.
- En el 2010 se registraron 380 anomalías en la red, en donde podemos nombrar las amenazas estructuradas u organizadas y amenazas externas.
- En el 2011 se obtuvieron 410 incidentes provocados por los ataques de denegación de servicio, código malicioso y de suplantación de identidad.
- En el 2012 se registraron 420 incidentes la mayoría provocados por la intrusión de personas no autorizadas, pérdida de información, vulnerabilidades en equipos de comunicación.
- En el 2013 se obtuvo un aproximado de 450 anomalías en donde destacan las amenazas físicas de la red, amenazas internas organizadas.
- En el 2014 se registraron 510 casos de anomalías en la red provocados en su mayoría por intrusos a la red por pérdida de información, ataques por códigos maliciosos, suplantación de identidad.

De esta manera es como se ha generado un estudio minucioso para poder determinar las causas de los daños provocados por la falta de seguridad en la compañía, lo cual luego del estudio realizado nos arroja datos alarmantes

y que va ascendiendo conforme pasan los años. Así como vemos en la Figura 1.1

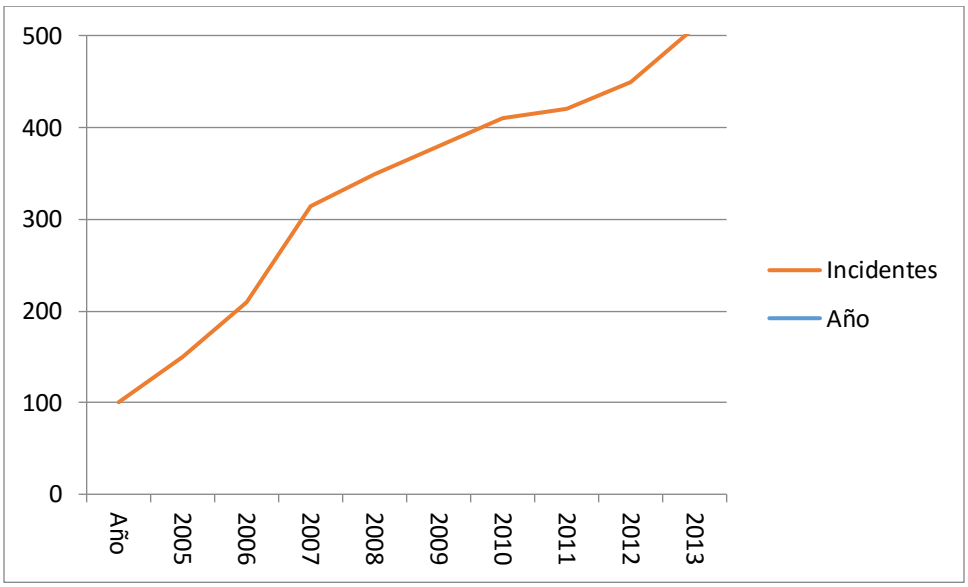


Figura 1.1Datos estadísticos de anomalías

1.2.1. Principales problemas encontrados

Luego del levantamiento de información realizado a la empresa, a continuación listamos los principales problemas que fueron encontrados:

- No se cuenta con equipos apropiados para manejar los accesos, bloqueos y filtros de los paquetes que intentan ingresar o salir de la red.
- No posee un sistema de monitoreo que ayude a la gestión de control de registros y eventos que se presenta en la red.
- No tiene un mecanismo de seguridad que ayude a controlar el intento de acceso de intrusos que de forma desautorizada buscan la manera de infiltrase en la red.

- No cuentan con los equipos de comunicación debidamente configurados para de esta forma prevenir que usuarios con restricciones puedan tener acceso libre y con todos los permisos.

Con la información proporcionada podemos analizar las diferentes causas que provocan estas anomalías de acuerdo a la clasificación de los riesgos, estos pueden ser debido a las vulnerabilidades, amenazas y ataques.

1.2.2. Análisis de las vulnerabilidades presentadas en la red actual

Sin duda alguna contar con un sistema de información provee muchos beneficios puesto que automatiza los procesos, pero esto conlleva a priorizar la seguridad puesto que su vulnerabilidad expondrá la información a los distintos ataques que pudieran presentarse.

Estas vulnerabilidades se pueden originar por factores técnicos, institucionales, ambientales y en conjunto por malas decisiones administrativas.**[12]**

En nuestro caso expuesto se han visto afectados por las siguientes razones:

- Manejo de Protocolos inseguros: No existe un control en la transferencia de datos, puesto que existen protocolos que son vulnerables así como lo son el protocolo de transferencia de hipertexto (HTTP), protocolo de transferencia de archivos (FTP) , protocolo de mensajes de control de internet (ICMP), protocolo de administración de redes simple (SNMP), protocolo simple de transferencia de correos (SMTP)
- Debilidad en los sistemas operativos: Existe en la organización máquinas que manejan diferentes sistemas operativos así como Windows, Mac OS, Unix. Algunos de los cuales se encuentran desactualizadas, sin parches, sin control de acceso y esto se convierte en una vulnerabilidad para el sistema de información.

- Debilidad en los equipos de cómputo: Otro tema de vulnerabilidad es la poca protección en el acceso de ciertos equipos de comunicación como son los conmutadores, enrutadores, firewall. No poseen la seguridad apropiada para su debido funcionamiento.
- Cuentas de usuarios no seguras: Cuando la cuenta de usuarios y la contraseña no se protege de manera apropiada es aprovechada por intrusos para ingresar con esta información a la red.
- Equipos de comunicación mal configurados: El no poder contar con una buena administración de los equipos de cómputo se convierte también en un motivo de vulnerabilidad, puesto que no se establece la seguridad lógica apropiada.
- Falta de renovación periódica: Las contraseñas en un tema de alta importancia, puesto que aquellas que son mal elegidas, fáciles de decodificar o las predeterminadas pueden facilitar el acceso a personas no autorizadas a la red.
- Fácil acceso a los sistemas: La mayor parte de los sistemas son accesibles a muchas personas. La información es más fácil de recopilar pero más difícil de controlar.
- Instalación de hardware y software sin cumplir las políticas: La falta de control de cambios en los equipos se convierte en un tema muy grave de seguridad puesto que por medio de algún software o hardware mal instalado o que contenga código malicioso pueden afectar el normal funcionamiento de la red. **[10]**
- No hay plan de recuperación ante un desastre: Un plan de contingencia es muy necesario para la seguridad, ya que en un caso de emergencia serviría para que no se paralice el normal funcionamiento de la red.

Estos son las amenazas más destacadas en la red actual, existen aún otras que podrían afectar al sistema de información como el tema

eléctrico, climatización, ubicación y más pero nos vamos a referir a lo mencionado anteriormente por ser lo más relevante.

1.2.3. Análisis de las amenazas presentadas en la red actual

Toda compañía sufre amenazas de seguridad en su infraestructura de red, por lo cual se trabaja para poder mitigar estas vulnerabilidades en lo más posible. De acuerdo a los tipos de amenazas que existen podemos distinguirlas de la siguiente manera:

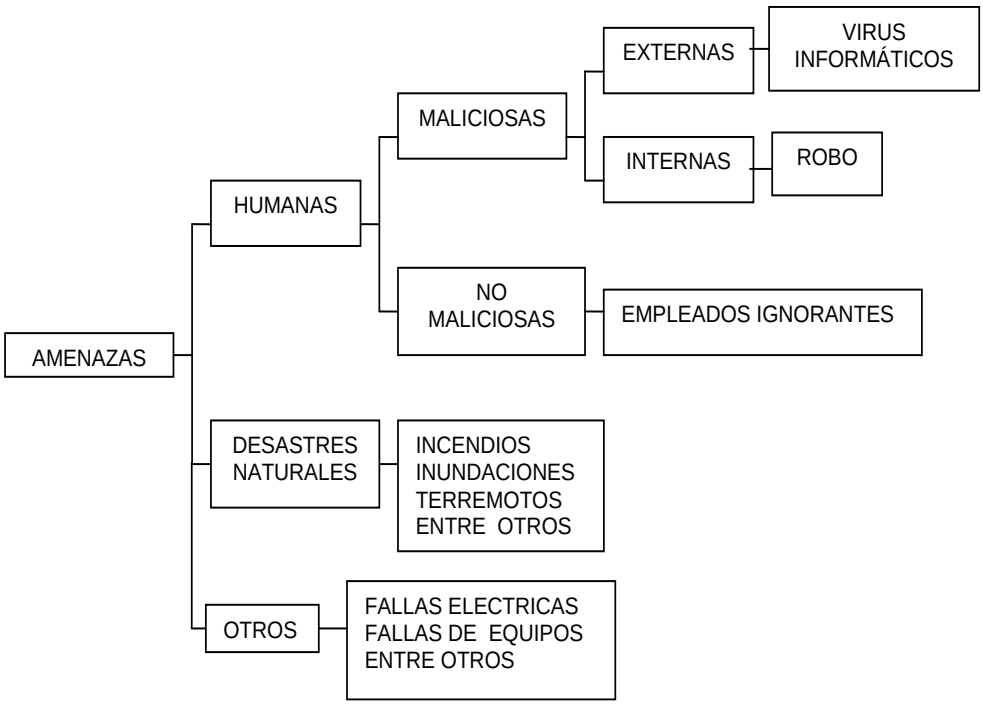


Figura 1.2Tipos de Amenazas

En nuestro caso analizado en los últimos años se han venido dando diferentes tipos de amenazas así como las que describimos a continuación y también se muestran en la Figura 1.2:

Amenazas humanas

Este tipo de amenazas son las más frecuentes, ya que son las acciones provocadas por el hombre y éstas pueden ser de 2 maneras: Maliciosas y no maliciosas.

Maliciosas

Son aquellas amenazas que cuando se llevan a cabo causan un mayor daño a la compañía. De este tipo de amenazas se ha venido registrando en mayor parte los últimos años en nuestro caso de estudio.

Externas

Las amenazas externas son aquellas que son provocadas por personas que no están dentro de la organización y no tiene acceso autorizado, pero sin embargo logran infiltrase para lograr su objetivo. Muchas de las veces estas amenazas provienen del Internet ya que desde aquí se pueden filtrar los hackers, crackers, virus, gusanos y más.

Internas

Este tipo de amenazas se ha venido dando y es más peligrosa puesto que el infractor cuenta con el acceso a ciertos servicios y ocasiona mayor daño al poder contar con ciertos permisos. Muchas de las veces se ha presentado por empleados o ex empleados que guardan algún tipo de resentimiento hacia un superior.

No maliciosas

Las amenazas de tipo no maliciosas, se han presentado también en nuestro caso de estudio, puesto que son aquellas que son provocadas por empleados activos que no cuentan con los conocimientos apropiados y de manera involuntaria han ocasionado algún daño.

Amenazas por desastres naturales

Este tipo de amenazas no son tan frecuentes pero se ha dado ya sea por un sismo, lluvias, tempestades y han provocado ciertos daños que son ocasionados justamente por no contar con un sistema apropiado ante estas anomalías.

Otros

Han existido otro tipo de amenazas menos frecuentes como la variación de energía eléctrica, la variación de temperatura y entre otros que de alguna forma también representa una amenaza para la institución.

1.2.4. Análisis de los ataques presentadas en la red actual

Otros de los factores de riesgo de la seguridad que se ha venido presentado en los últimos años en la compañía VENSUR S.A son lo referente a ataques informáticos, los cuales representan un alto índice de inseguridad, estos implican un riesgo alarmante para la estabilidad de la red de la organización.

Entre los ataques que se han venido presentando podemos mencionar los siguientes:

Ataques de reconocimiento: Este tipo de ataque se ha venido dando de manera muy frecuente, en el cual consiste en que una persona intenta obtener información de la red y por medio de herramientas que analizan el tráfico real puede determinar puertos que se están usando, direcciones IP que están libres, otros tipos de paquetes que estén siendo usados, todo esto con la finalidad de infiltrarse y con ello sacar provecho de alguna información o causar algún otro tipo de daño a la organización.

Ataques de denegación de servicio: Este ataque consiste en enviar de manera simultánea solicitudes de respuesta a un determinado equipo, lo cual genera una saturación provocando inestabilidad en los equipos destino y el colapso de su servicio. Esta anomalía se ha presentado en muchas ocasiones en la compañía que hemos analizado, teniendo así muchos inconvenientes en el funcionamiento normal de sus procesos.

Ataques de acceso: Es un típico tipo de ataque que se ha dado en nuestro caso de estudio, lo cual ha generado mucho daño a la organización puesto que sus estrategias o planes de negocios se han visto expuestas por algunos intrusos que de una u otra forma han

ingresado a la red usurpando todo tipo de información de manera malintencionada.

Ataques de código malicioso: En los últimos años se han visto expuesto algunos equipos ante ciertos ataques de códigos maliciosos como lo son los virus, los gusanos, caballo de Troya. Esta anomalía es muy grave puesto que estos ataques pueden provocar inestabilidad en ciertos equipos.

La mayor vulnerabilidad para este tipo de ataque es el Internet, puesto que de aquí se pueden filtrar los hackers, virus, gusanos, caballo de Troya. Entre los más destacados en nuestro estudio tenemos:

- Hackers: También son conocidos como los piratas informáticos puesto que acceden a la información que existe y se transmite por internet, no solo tienen acceso a e-mails sino a equipos que están enlazadas a la red perjudicando a las empresas haciendo mal uso de la información.
- Cracker: Son personas con muchas habilidades y con un amplio conocimiento informático, que buscan de alguna manera infiltrarse en la red para con ello provocar daño e inestabilidad en la organización.
- Virus: Son software diseñados para modificar o destruir información, pueden ser ingresados al sistema por un dispositivo externo o a través de la red (e-mails) sin intervención directa del atacante.
- Gusanos: Son virus que se activan y transmiten por medio de la red. Tienen como propósito su multiplicación hasta agotar el espacio en disco duro o RAM. Suele ser uno de los ataques más peligrosos porque normalmente produce un colapso en la red
- Caballos de Troya: Son virus que entran al computador. Parecen ser una cosa o programa inofensivo cuando en realidad están

haciendo otra y expandiéndose. Pueden ser muy dañinos cuando es un programador de la propia empresa quien lo instala.

- Spam: También se lo conoce como correo no deseado,provoca hoy en la actualidad pérdidas muy importantes en empresas y organismos.

1.3. Análisis de la red actual

VENSUR S.A es una compañía que se dedica a la fabricación y venta de todo tipo de repuestos de vehículos de toda marca, algunos son importados lo que ha permitido convertirse en uno de los proveedores más grandes en esta línea en todo el país.Por su alta infraestructura, por el tipo de información que maneja y por los continuos intentos de robo de información por parte de la competencia es imprescindible contar con un sistema de seguridad que controle el flujo de información para evitar así posibles daños o pérdida de datos.

1.3.1. Infraestructura de la red WAN

VENSUR S.A cuenta actualmente con una matriz en donde se realiza las principales gestiones de operaciones y ventas. Además, cuenta con cuatro sucursales distribuidas en distintas partes del territorio ecuatoriano.

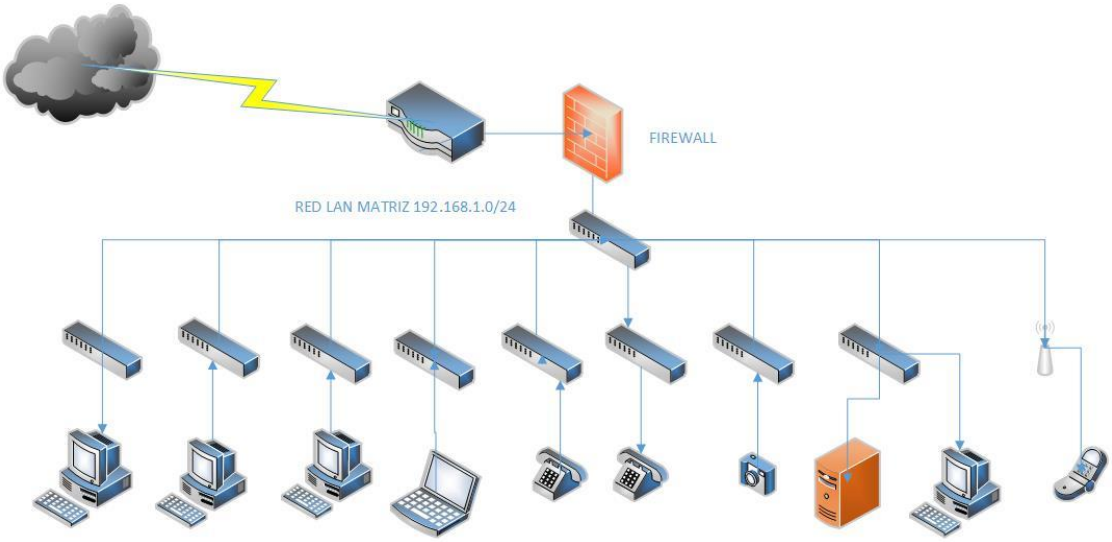
Aproximadamente cuenta con 200 empleados, los cuales se encuentran distribuidos en la matriz y en las cuatro sucursales, ubicadas en Portoviejo, Machala, Quito y Cuenca. El crecimiento paulatino que se ha venido dando en la compañía conlleva a implementar nuevas medidas de seguridad en la información que se maneja a través de la red WAN.

A continuación se muestra en la Figura 1.3 el gráfico de la red WAN de la compañía VENSUR S.A

Figura 1.3 Red empresarial existente

1.4. Infraestructura de red LAN - matriz

La matriz está formada por una red LAN en donde se encuentra la parte operativa y administrativa de la organización, es por ello que aquí se encuentra la mayor parte de equipos de usuarios y equipos de comunicación de toda la compañía como se muestra en la Figura 1.4



Leyenda		
Símbolo	Total	Descripción
	4	PC
	9	Conmutador
	1	Teléfono móvil
	1	Cámara digital
	1	Servidor
	2	Teléfono
	1	Vínculo de comunicación
	1	Nube
	1	Equipo portátil
	1	Enrutador
	1	Firewall
	1	Punto de acceso inalámbrico

Figura 1.4 Red LAN matriz

La red LAN de la matriz se encuentra ubicada en la ciudad de Guayaquil en un edificio en donde funcionan los departamentos administrativos, de operación y distribución. En esta red LAN se cuenta con el siguiente hardware, según la Tabla 1.

CANTIDAD	MARCA	MODELO
9	Switch Cisco	Catalyst 2960 24p
1	Router Cisco	800 iSeries
70	HP Workstation	Pro 3400
10	HP All in One	ProOne 400
20	Laptop HP	Notebook 430
40	Teléfono IP Panasonic	KX-UT123
20	Camara IP Hikvision	DS-2CD2112
5	Impresora HP	Laserjet P2055DN

Tabla 1 Hardware existente en la matriz

1.4.1. Departamentos Administrativos

La estructura organizacional de VENSUR S.A. se encuentra compuesta de la siguiente forma:

- Dirección General
- Financiero
- Comercial
- Mercadeo
- Ventas
- Recursos humanos
- Sistemas
- Distribución y operaciones
- Control interno
- Seguridad ocupacional

Todos los departamentos administrativos se encuentran físicamente ubicados en la matriz. En las sucursales sólo se encuentran personal de distribución de productos y el supervisor.

1.4.2. Servidores

La matriz cuenta con cinco servidores descritos en la tabla 2 que manejan el funcionamiento operativo de la compañía. Estos servidores se encuentran en un centro de procesamiento de datos que es la ubicación física donde se encuentran los recursos necesarios para el procesamiento de la información de una organización, el mismo que cuenta con todas las seguridades debidas, así como: restricción del ingreso, buena climatización, vigilancia permanente mediantes las cámaras IP, dispositivos de detección de humo.

MARCA	MODELO	FUNCIÓN
HP	DL10 HP ProLiant	Servidor de Archivos y Base de Datos
HP	DL10 HP ProLiant	Servidor Web y de Aplicación
HP	DL10 HP ProLiant	DomainControler, DNS y DHCP
HP	DL10 HP ProLiant	Servidor de Virtualización
HP	ProLiant ML10 v2	Aplicación

Tabla 1 Servidores existentes en la matriz

1.4.3. Seguridades

Para controlar la seguridad de la red Lan en la matriz se cuenta con un cortafuegos Fortigate, el cual entre sus funciones está la de filtrar los paquetes que salen e ingresan a la red, antispam, gestiona el acceso VPN, control IPS.

MARCA	MODELO	FUNCIÓN
FORTINET	100	IPS, Filtrado de paquetes

Tabla 2 Firewall existente en la matriz

1.5. DMZ

En la zona desmilitarizada mostrada en la Figura 1.5 se encuentran los servidores en el que se aloja el sitio webwww.vensursa.com.ec, y el servidor de aplicaciones. El sitio web tiene un túnel para hacer consultas del servidor donde se encuentra la base de datos.

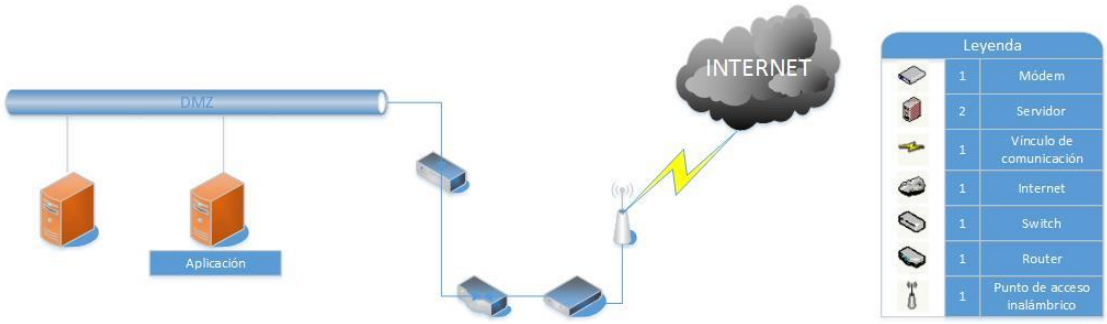


Figura 1.5Gráfico DMZ

1.6. Red LAN Sucursal Portoviejo

La red LAN de Portoviejo descrita en la Tabla 4 cuenta con los siguientes equipos de cómputo:

CANTIDAD	MARCA	MODELO
1	Switch Cisco	Catalyst 2960 24p
1	Router Cisco	800 iSeries
10	HP Workstation	Pro 3400
7	Teléfono IP Panasonic	KX-UT123
5	Camara IP Hikvision	DS-2CD2112

Tabla 3 Hardware sucursal Portoviejo

La gráfica de la red LAN de la sucursal Portoviejo es la que se muestra a continuación en la Figura 1.6

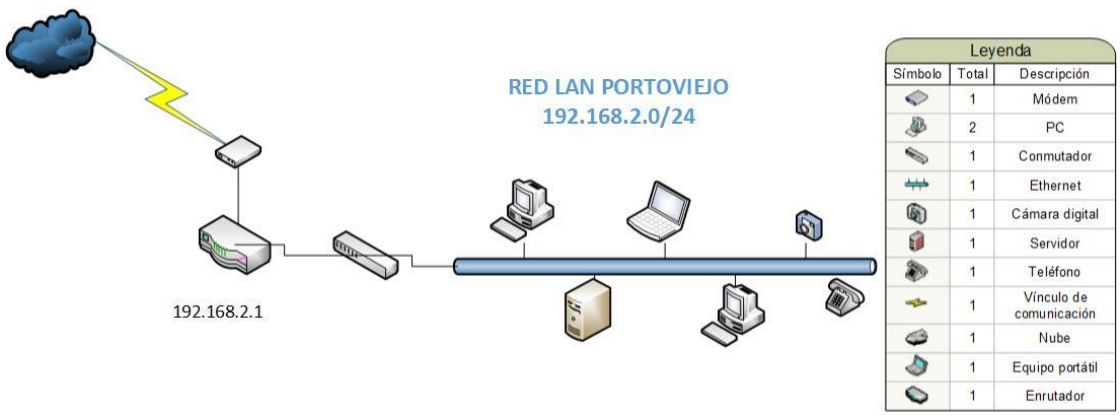


Figura 1.6 Diseño de la Red LAN Portoviejo

1.7. Red LAN sucursal Quito

La red LAN de Quito cuenta con los siguientes equipos de cómputo:

CANTIDAD	MARCA	MODELO
2	Switch Cisco	Catalyst 2960 24p
1	Router Cisco	800 iSeries
15	HP Workstation	Pro 3400
12	Teléfono IP Panasonic	KX-UT123
8	Camara IP Hikvision	DS-2CD2112

Tabla 4 Hardware de la sucursal Quito

La gráfica de la red LAN de la sucursal Quito es la que se muestra a continuación.

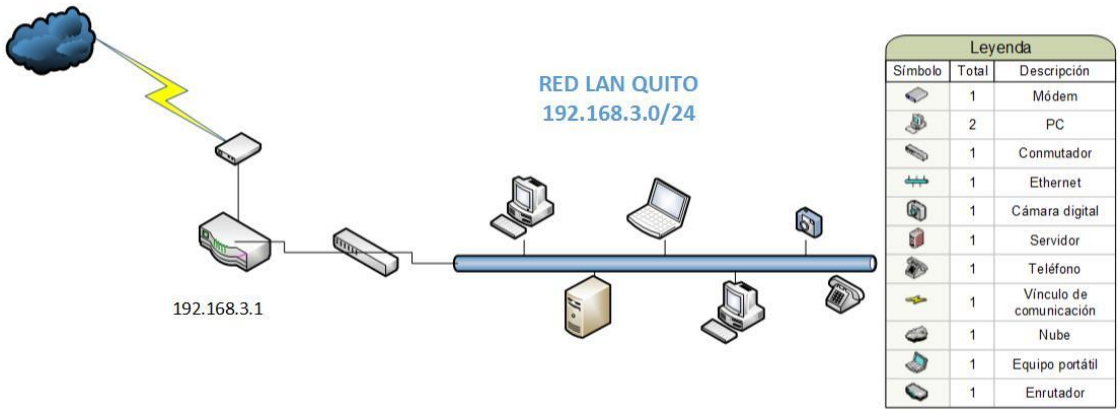


Figura 1.7 Diseño de red LAN sucursal Quito

1.8. Red LAN sucursal Cuenca

La red LAN de Cuenca cuenta con los siguientes equipos de cómputo:

CANTIDAD	MARCA	MODELO
1	Switch Cisco	Catalyst 2960 24p
1	Router Cisco	800 iSeries
8	HP Workstation	Pro 3400
7	Teléfono IP Panasonic	KX-UT123
5	Camara IP Hikvision	DS-2CD2112

Tabla 5 Hardware sucursal Cuenca

La gráfica de la red LAN de la sucursal Cuenca es la que se muestra a continuación.

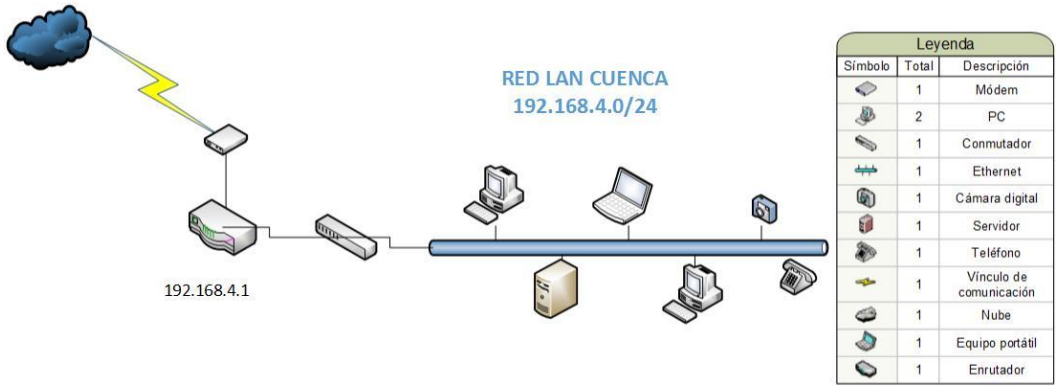


Figura 1.8 Red LAN sucursal Cuenca

1.9. Red LAN sucursal Machala

La red LAN de Machala descrita en la tabla 7 cuenta con los siguientes equipos de cómputo:

CANTIDAD	MARCA	MODELO
1	Switch Cisco	Catalyst 2960 24p
1	Router Cisco	800 iSeries
12	HP Workstation	Pro 3400
10	Teléfono IP Panasonic	KX-UT123
5	Camara IP Hikvision	DS-2CD2112

Tabla 6 Hardware de la sucursal Machala

La gráfica de la red LAN de la sucursal Machala es la que se muestra a continuación en la Figura 1.9

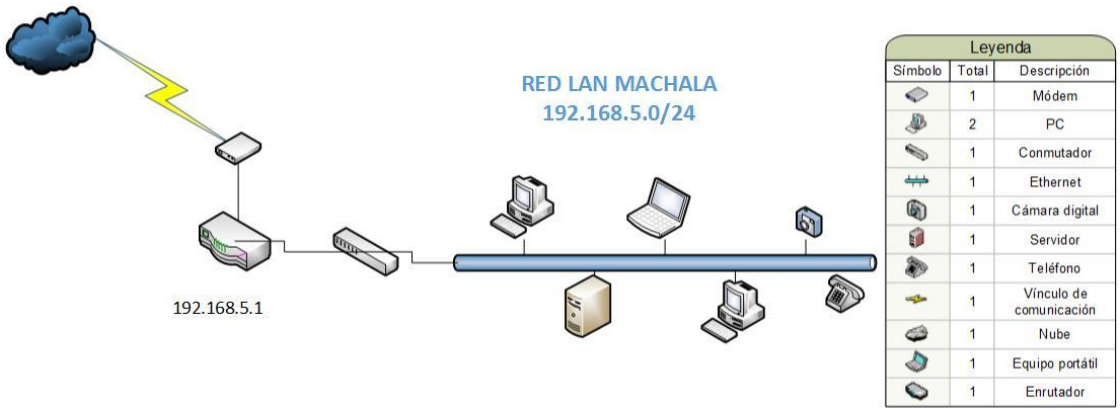


Figura 1.9 Diseño de la red LAN Machala

CAPÍTULO 2

2. SOLUCIÓN PROPUESTA

Después de presentar el análisis a la red WAN y de determinar sus problemas, causas y efectos, presentamos en este capítulo la solución a los problemas identificados, y podemos establecer las siguientes soluciones:

- Ante el problema de que no tienen políticas de seguridad, se establece como solución la configuración de reglas que controlen el flujo de información mediante la aplicación de cortafuegos Fortigate de robustas características. El más sofisticado para la matriz y otros de similares características para las sucursales.
- Ante el tema de los intrusos, se propone la implementación de un IPS, puesto que esto apoyará al manejo de información que intenta ingresar a la red.
- Para los equipos administrables que no presentan un mecanismo de seguridad para su gestión, se propone la aplicación de Método de Seguridad mediante normas AAA para tener un control en la autenticación, autorización, y en la auditoría de los usuarios que ingresan a la administración de los equipos de comunicación.
- Otro mecanismo que nos ayudará a controlar y monitorear los eventos que se presentan en la red es el SIEM, en este caso proponemos el sistema OSSIM que cumple con todos los requisitos apropiados para tener una consola en donde se pueda administrar y controlar todos los eventos que surgen en la red.

2.1. Red WAN Propuesta

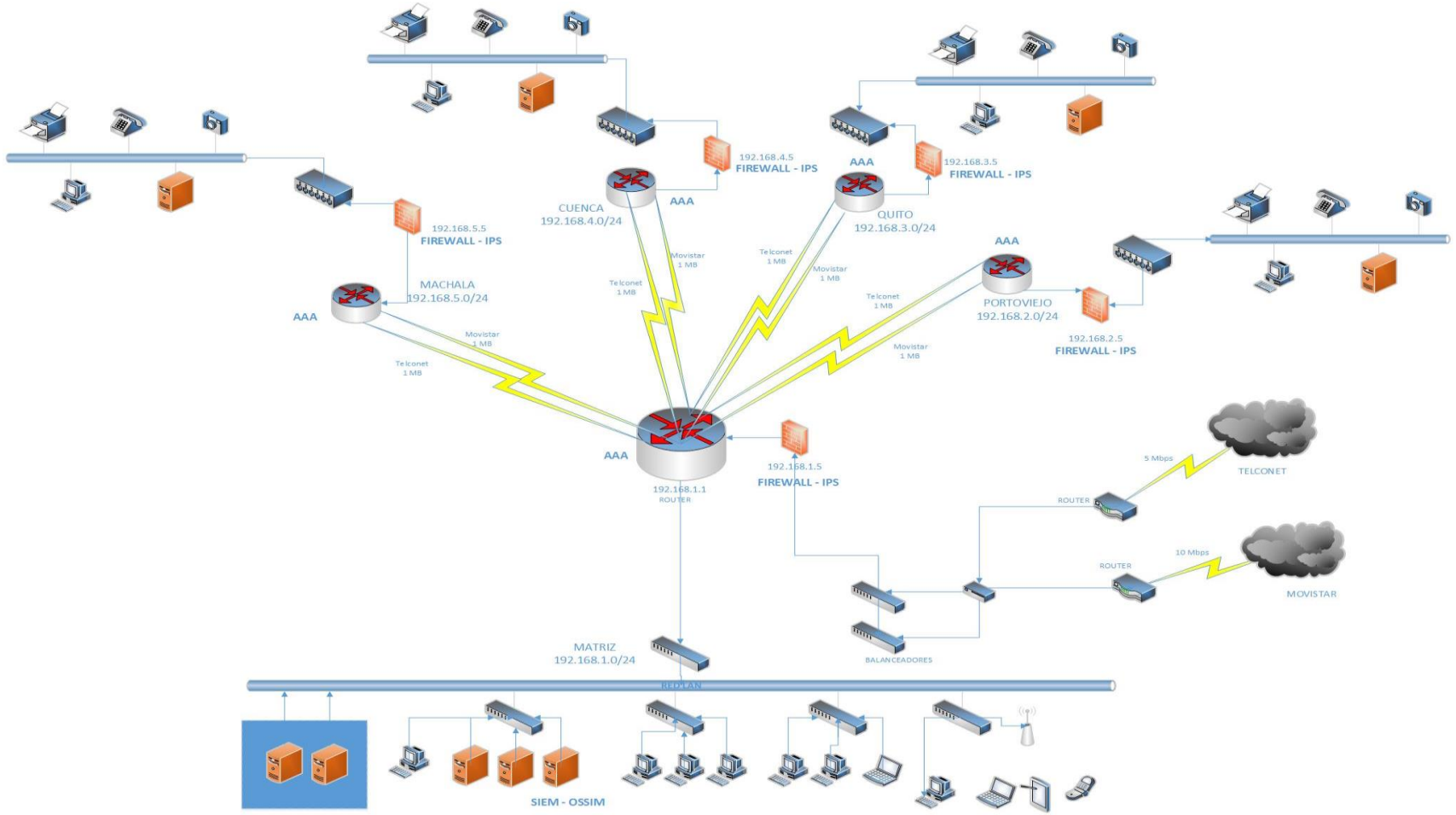


Figura 2.1Red WAN propuesta

En el diseño de la red WAN propuesta mostrado en la Figura 2.1 podemos identificar que se aumentan con relación al diseño existente en la Figura 1.3, los Firewall en cada sucursal por la seguridad interna que además serán también configurados como IPS y en cada enrutador de acceso será configurado con AAA para su correcta administración. Para el monitoreo constante de la red se aplica un servidor SIEM desde la matriz.

2.2. Análisis de la seguridad en la red mediante el uso del cortafuego.

La empresa Vensur S.A. cuenta solo con un cortafuegos que se encuentra ubicado en la matriz y es indispensable contar con uno en cada una de las sucursales, ya que así se reducirá considerablemente las posibilidades de un ataque externo al sistema corporativo y redes internas, inclusive sirve para los mismos miembros de la empresa no comprometan la seguridad de la red al enviar información peligrosa como contraseñas no cifradas o datos privados hacia el exterior de su red.

2.2.1. Alcance y limitaciones del cortafuego.

Un punto débil de un cortafuegos es que está diseñado para proteger de las amenazas conocidas en la actualidad pero de igual manera si se configura el cortafuegos de forma correcta este también será capaz de proteger de amenazas nuevas, por ejemplo se puede negar todos los servicios y habilitar solamente los servicios seguros, sin embargo el cortafuegos no está diseñado para proteger automáticamente de nuevas amenazas que surjan y es muy conocido que cada día se desarrollan nuevas formas de violar la seguridad utilizando por ejemplo servicios que se consideren confiables y pasar paquetes maliciosos a través de ellos.

2.2.2. Software y hardware

Existen 2 tipos de cortafuegos, por software y por hardware.

El cortafuegos por software puede ser versión gratuita o comercial, el gratuito es un programa que se instala en una PC o portátil, la mayoría

vienen instalados por defecto y se los puede usar libremente, pero son cortafuegos básicos que monitorean y bloquean el tráfico de internet.

Los cortafuegos comerciales funcionan de la misma forma que los gratuitos, tampoco necesitan un hardware para funcionar, pero incluye protecciones más avanzadas en cuanto al control de su configuración y funcionamiento, la diferencia radica en que este es pagado y el usuario debe renovarlo periódicamente a su vez de instalar actualizaciones.

2.2.3. Filtrado de paquetes

Filtrar paquetes es un procedimiento que consiste en permitir o denegar el flujo de la información entre la red interna que se desee proteger y la externa, como ya se mencionó este filtrado se realiza por medio de un conjunto de reglas definidas y según las mismas se examinará las cabeceras de los paquetes que irán pasando a través del cortafuegos y el decidirá si el paquete pasa.

Todos los cortafuegos de filtrado de paquetes trabajan en las capas de red y transporte del modelo de sistema de interconexión abierto (OSI), es decir que trabajan solo con la información de las cabeceras de los paquetes IP pero no analiza los datos, para poner un ejemplo un cortafuegos no podrá evitar que un usuario mande algún correo electrónico desde su equipo con otra cuenta diferente a la de su trabajo pero tendría la capacidad acceder al servidor de correo electrónico y que desde este no pueda mandar ningún correo a nadie, es decir no tendría permiso para enviar mails.

2.2.4. Diseño de sistemas mediante el firewall

Un cortafuegos o firewall es un mecanismo o sistema de políticas de seguridad que se encuentra entre la red privada de un usuario y el internet, la misma que tiene como objetivo proteger un sistema de red de computadoras de ataques electrónicos provenientes de internet.

El “firewall” significa “cortafuego” y se le dio ese nombre ya que su función era muy parecida en el área de la tecnología al corta-fuego que

se usa en una construcción que es una pared que evita que el fuego pueda pasar de un lado al otro, de la misma manera un firewall no permite que los peligros de otras redes se filtren en nuestra propia red.

Para que la función del cortafuego sea cumplida, todo tráfico de información a través del internet deberá pasar por el 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. Desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece en torno al mismo.

2.3. Seguridades aplicando firewall

Para controlar la seguridad de la red WAN en la matriz se contará con un Firewall Fortigate 300C mostrado en la Figura 2.2, el cual es muy robusto y nos permite brindar la seguridad requerida, entre sus funciones está la de filtrar los paquetes que salen e ingresan a la red, anti spam, gestiona el acceso de red virtuales públicas (VPN), control IPS.

Figura 2.2 Firewall Fortigate 300C

Características del firewall

- 22 puertos 10/100/1000 Mbs.
- 1 puerto RJ-45 serial.
- 16 Gb de almacenamiento.
- 2.5 Millones, máxima cantidad de sesiones concurrentes.
- 300 Mbs SSL VPN.
- 450 Mbs IPSEC VPN.

2.4. Funcionalidades del Firewall Fortigate 300C

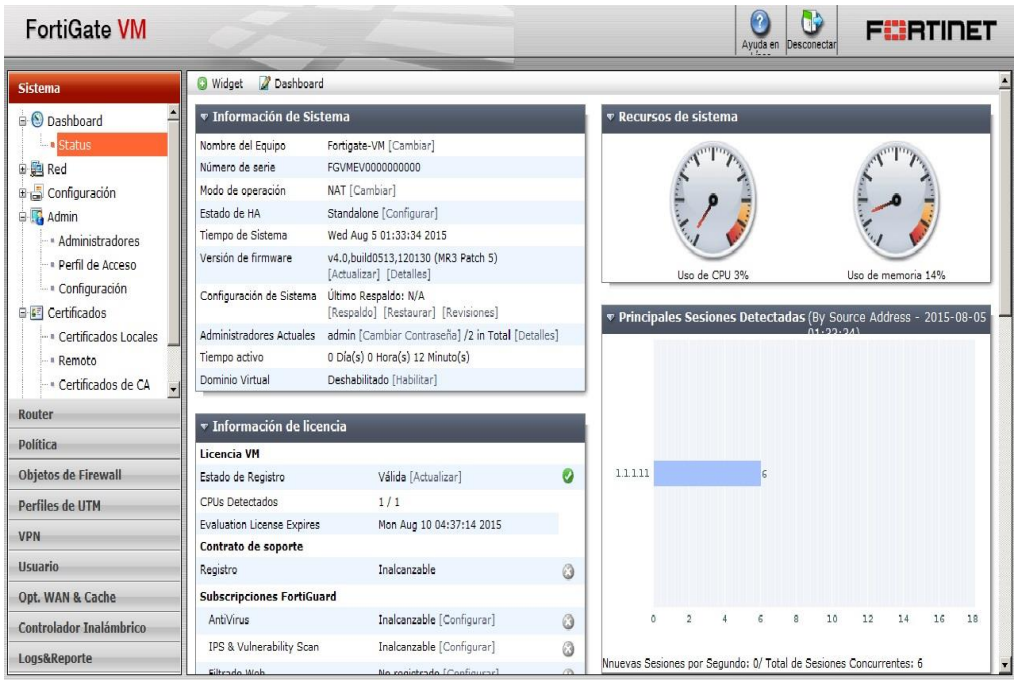


Figura 2.3 Entorno gráfico firewall Fortinet

Las funciones del firewall Fortinet son las siguientes:

- Vigilar todas las conexiones entrantes y salientes de todas las computadoras en la red.
- Preservar nuestra seguridad y privacidad.
- Proteger nuestra red doméstica o empresarial.
- Tener a salvo la información almacenada en la red, servidores, ordenadores.
- Evitar intrusiones de usuarios no deseados en la red.
- El firewall configurado correctamente puede proteger de ataques tales como suplantación de identidad y denegación de servicio (DOS).

2.5. Configuración de firewall Fortinet

Como ya se ha mencionado se utilizara el firewall Fortigate 300C en la matriz, se realizará una demostración con la ayuda de sistema operativo del firewall simulado en una máquina virtual en el programa VMWARE PLAYER y se lo configurara desde un usuario.

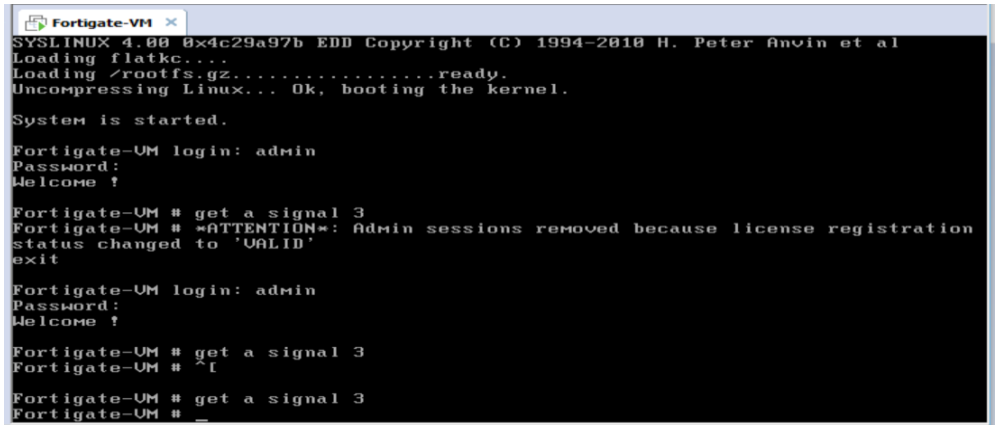


Figura 2.4 Consola simulada del firewall Fortinet

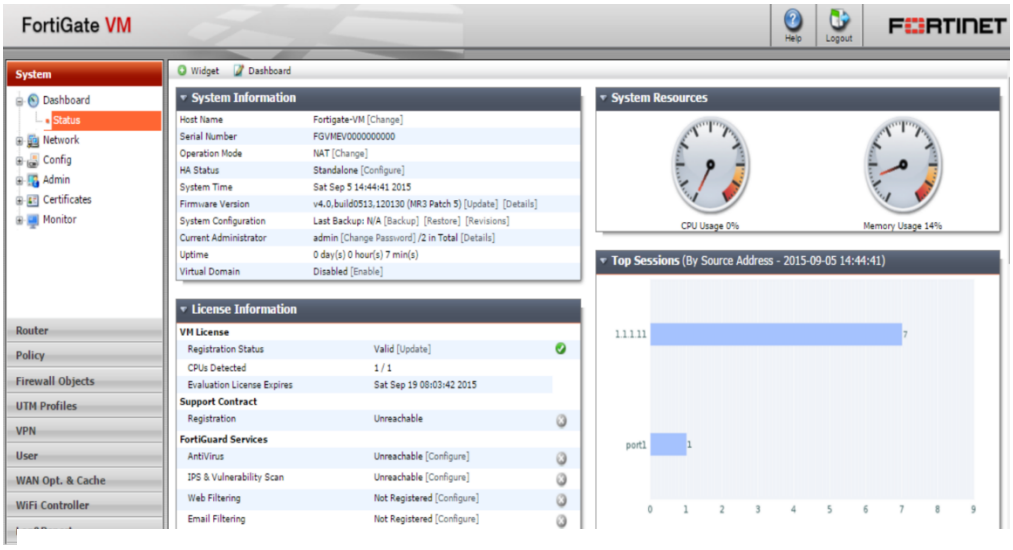


Figura 2.5 Interfaz gráfica del firewall Fortinet

2.6. Configuración de políticas para firewall Fortinet en la Red

La configuración de las políticas del firewall Fortinet se realizará a la matriz y a cada sucursal las cuales son:

- Guayaquil (Matriz)
- Cuenca
- Machala
- Quito
- Portoviejo

Se mostrará como ejemplo la configuración en Guayaquil siendo la matriz con la respectiva dirección IP 192.168.1.5 en el cual permitiremos los siguientes protocolos:

- HTTP: es el protocolo usado en cada transacción del internet.
- HTTPS: es un protocolo para asegurar la comunicación sobre una red de computadoras.
- SMTP: protocolo de transferencia simple de correo.
- POP3: protocolo que permite al usuario recibir y descargar sus correos electrónicos que se encuentran alojados en un servidor remoto.
- FTP: es el protocolo de red para la transferencia dearchivos basado en la arquitectura cliente-servidor
- DNS: es un sistema de nomenclatura jerárquica para computadoras

Teniendo en cuenta estos protocolos a permitir realizamos la respectiva configuración en nuestro firewall Fortinet.

En la consola del firewall nos dirigimos a políticas (police) y creamos una nueva la cual se basara en los servicios que permitiremos mencionados anteriormente.

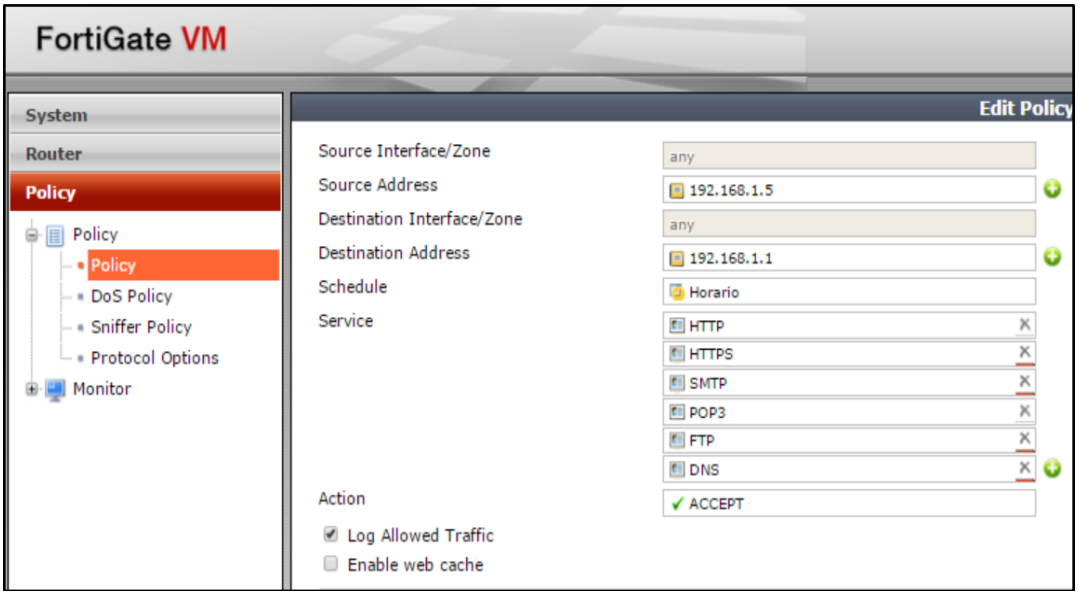


Figura 2.6 Configuración de protocolos permitidos

Como se muestra en esta imagen tenemos las siguientes características dentro de una política:

- Source interface/zone
- Sourceaddress
- Destination interface/zone
- Destinationaddress
- Shedule

Descritas a continuación:

- ServiceSource interface/zone: como interfaz de origen elegimos any
- Sourceaddress: como dirección de origen agregamos la 192.168.1.5 la cual será la dirección que se le asigne al firewall.
- Destination interface/zone: como destino de interfaz elegimos any
- Destinationaddress: como dirección de destino elegimos la 192.168.1.1.
- Shedule: este punto es importante ya que podemos agregar un horario en el que el usuario puede ingresar y ocupar los servicios ya mencionados, será configurado de 7:00 am hasta las 19:00pm.

- Service: como ya se describió los servicios son: HTTP, HTTPS, SMTP, POP3, FTP y DNS, finalmente marcamos la casilla de registrar el tráfico permitido (log allowedtraffic), de esta manera se irá guardando en el firewall todo el tráfico que ha entrado y salido de la red.

2.7. Análisis de la seguridad en la red mediante el uso de IPS

El no contar con un sistema de prevención de intrusos (IPS), priva a la compañía de poder detectar y prevenir futuros ataques que pudiesen presentarse. Este mecanismo de seguridad nos permite mantener una red confiable y segura, puesto que todo paquete de datos que intente ser introducido a la red será analizado y de cumplir con los reglamentos establecidos por medio del IPS se dará el acceso adecuado.

2.7.1. Objetivo de Contar con un IPS

El objetivo de contar con un IPS en una red LAN es la de proteger la red, evitando la intrusión de personas que se dedican al hurto de información. Así como es bien conocido existen varios tipos de hackers que se dedican a la posible vulneración de una red con fines negativos.

Sea de cualquier mecanismo que se use el propósito es el de llegar a la información, que sin tener alguna protección se ve expuesta a ser vulnerada. Entre las herramientas más usadas para prevenir estos tipos de ataques y de cualquier otra índole tenemos:

- Cortafuegos
- IDS (Sistema de Detección de Intrusiones)
- IPS (Sistema de Prevención de Intrusiones)

Entre sus funciones logran aplacar programas maliciosos como troyanos, virus, spam y otros que lo único que intentan es causar daño a una determinada red.

2.8. Sistema de Prevención de Intrusiones, IPS

Este sistema fue diseñado para monitorear el tráfico de una red, en tiempo real y prevenir que se filtre cualquier actividad maliciosa conocida como intrusión, cuando se produce la caída de un paquete o éste pasa dañado o incompleto, en una transmisión de información, inmediatamente la red bloquea la transmisión por prevenir un posible ataque o deformaciones en la transferencia de datos, es considerado una mejora con respeto a los cortafuegos, su diseño es una evolución de los IDS.

A diferencia de los IDS este mecanismo no se limita solo a escuchar el tráfico de la red y a enviar alertas en una consola, después de que suscita una intrusión, el IPS funciona a nivel de la capa 7 y tiene la capacidad de descifrar protocolos como HTTP, FTP y SMTP, algunos IPS permiten establecer políticas como lo hacen los cortafuegos. La tecnología IPS ofrece una visión más profunda de las operaciones de la red brindando información sobre actividades maliciosas, malas conexiones, el contenido inapropiado de la red y muchas otras funciones de la capa de aplicación, utiliza menos recursos que un IDS, siendo una solución ideal que contribuye a la seguridad de la información que se transmite por una red y disminución de costos, para una empresa que opta por adquirir sistemas de este tipo para preservar los datos que posee.

El IPS no utiliza dirección IP como lo hace un cortafuegos, el IPS permite establecer normas y restringir acceso a usuarios, aplicaciones y a hosts (anfitrión, son computadoras conectadas a una red, que proveen y utilizan servicios de ella) siempre y cuando se detectan que estos están teniendo actividades mal intencionadas o código malicioso en el tráfico de la red.**[13]**

2.8.1. Ventajas

- Defensa completa (vulnerabilidades del sistema operativo, puertos, tráfico de IP, códigos maliciosos e intrusos)
- Protección preventiva antes de que ocurra un ataque.

- Maximiza la seguridad y aumenta la eficiencia en la prevención de intrusiones o ataques a la red de una empresa.
- Fácil instalación, configuración y administración.
- Es escalable y permite la actualización de dispositivos a medida que crece la empresa
- No requiere tanta dedicación como un IDS tradicional; esto en consecuencia requeriría menos inversión en recursos para administrar y operar estos sistemas (en comparación con un IDS).

2.8.2. Características de un IPS

- Capacidad de reacción automática ante incidentes
- Aplicación de nuevos filtros conforme detecta ataques en progreso.
- Mínima vigilancia
- Disminución de falsas alarmas de ataques a la red
- Bloqueo automático frente a ataques efectuados en tiempo real
- Protección de sistemas no parchados
- Optimización en el rendimiento del tráfico de la red

Tipos de IPS

2.8.3. IPS basados en host (HIPS)

Esta aplicación de prevención de intrusiones reside en la dirección IP específica de un solo equipo, permite prevenir posibles ataques en los nodos débiles de una red es decir los anfitriones o *hosts*.

2.8.4. IPS basada en red (PIN)

Esta solución IPS es en hardware y cualquier acción tomada para prevenir una intrusión en una red específica de host se hace de una máquina con otra dirección IP en la red.

Son desarrollados específicamente para las plataformas hardware/software que analizan, detectan e informan sobre eventos relacionados con la seguridad. PIN están diseñado para inspeccionar el tráfico y la configuración de las políticas de seguridad, sobre la cual pueden verificar el tráfico malicioso.

2.8.5. Contenido de la base IPS (CBIPS)

Monitoriza el contenido de la base de datos que se va almacenado en un IPS en base a patrones de comportamiento o firmas, para detectar y prevenir varios tipos de ataque conocidos como gusanos, virus y troyanos, aunque no son muy efectivos puesto que existe decenas o incluso cientos de variantes.

2.8.6. Protocolo de análisis

Pueden decodificar la aplicación nativa de la capa de red protocolos, como el protocolo de transferencia de archivos (FTP) y/o el protocolo de transferencia de hipertexto (HTTP), el motor de análisis del IPS puede evaluar diferentes partes del protocolo y analizar si este tiene un comportamiento anómalo. Por ejemplo, la existencia de un gran archivo binario en el campo usuario - agente de una solicitud HTTP sería muy inusual y probablemente una intrusión. Un analizador de protocolos puede detectar este comportamiento anómalo y alertar al motor IPS de la caída de los paquetes.

2.8.7. IPS basado en tarifa (RBIPS)

En sus funciones prioritarias está la de impedir la negación de servicio distribuido. Trabaja con la vigilancia normal de la red y el aprendizaje de conductas de patrones de comportamiento. Por medio del tráfico en tiempo real, el seguimiento y la comparación con las estadísticas almacenadas, RBIPS puede identificar tasas anormales para ciertos tipos de tráfico, por ejemplo el protocolo de control de transmisión (TCP), el protocolos de

datagramas de usuario (UDP) o los paquetes del protocolo de resolución de direcciones (ARP), las conexiones por segundo, conexión por paquetes, los paquetes específicos a los puertos, estos ataques se detectan basándose en estadísticas de tráfico almacenados.

2.9. Seguridades mediante IPS

Un IPS nos garantizará la prevención de Intrusos, para esto existen algunas formas de cómo configurarlo. **[14]**

2.9.1. Funcionalidades del IPS

- Analiza constantemente el flujo de paquetes en una red informática para proteger a los sistemas computacionales de ataques y abusos.
- Detecta una actividad maliciosa y la detiene.
- Puede ser monitoreados a nivel de red (NIPS) y a nivel de host (HIPS)
- Detección basada en firmas, políticas y en anomalías.
- Con la implementación del IPS se garantiza la seguridad de la red con el bloqueo de ciertos ataques.

2.9.2. Pasos de configuración generales

Para obtener los mejores resultados en la configuración de la exploración IPS, se debe seguir los pasos de acuerdo a lo indicado por el fabricante, en caso de omitir o aumentar ciertos parámetrospuede cambiar la funcionalidad del IPS en sí.

Los pasos recomendados son los siguientes:

1. Crear un sensor IPS.
2. Añadir filtros y / o firmas predefinidas y firmas personalizadas al sensor. Los filtros y firmas especifican qué firmas del motor IPS buscará en el tráfico de red.
3. Seleccione una política de seguridad o crear una nueva.
4. En la política de seguridad activar IPS, elegir el sensor IPS de la lista.

Todo el tráfico de la red controlada por esta política de seguridad será procesada de acuerdo a los ajustes en la política. Estos ajustes incluyen el sensor IPS que especifique en la póliza.

2.9.3. Creación de un sensor IPS

Es necesario crear un sensor IPS y guardarlo antes de configurarlo con filtros y entradas.

Para crear un nuevo sensor IPS se realizan los siguientes pasos:

1. Ir a los perfiles de seguridad> Protección de Intrusión> IPS Sensores.
2. Seleccionar el ícono de Crear Nuevo en la parte superior de la ventana de edición del sensor IPS.
3. Introduzca el nombre del nuevo sensor IPS.
4. Opcionalmente, también se puede introducir un comentario. El comentario aparecerá en la lista de sensores IPS y sirve para recordar los detalles del sensor.
5. Seleccione Aceptar.

Se crea el sensor IPS y aparece la ventana de configuración del sensor. Un sensor de nueva creación está vacío y no contiene filtros o firmas. Usted necesita agregar uno o más filtros o firmas antes de que el sensor pueda tener efecto.

2.9.4. Creación de un filtro IPS

Mientras que las firmas individuales se pueden agregar a un sensor, un filtro le permite añadir varias firmas a un sensor especificando las características de las firmas que se añaden.

Para crear un nuevo filtro IPS

1. Ir a los perfiles de seguridad> Protección de Intrusión> IPS Sensores.

2. Seleccione el sensor IPS a la que desea agregar el filtro utilizando la lista desplegable en la fila superior de la ventana de edición del sensor IPS.

3. Seleccione la Nueva Creación icono

4. Para Tipo de Sensor escoger al filtro basado.

5. Configurar el filtro que se requiere. Firmas todas las características especificadas en el filtro se incluirán en el filtro. Seleccionar, Especificar y elegir la opción de filtro que tienen los parámetros adecuados.

2.9.5. Basic

Severity

Se refiere al nivel de amenaza estimada por el ataque.

Las opciones incluyen:

• critical
• high
• medium
• low
• info

Target

Se refiere al tipo de dispositivo de destino por el ataque.

Las opciones incluyen:

• client
• server

OS

Se refiere al sistema operativo afectado por el ataque.

Las opciones incluyen:

BSD	Linux	MacOS
Other	Solaris	Windows

Tabla 8 Sistemas operativos soportados por el IPS

2.9.6. Advanced

Se refiere al proveedor o tipo de aplicación afectada por el ataque.

Las opciones incluyen:

Adobe	Apache	Apple
CGI_app	Cisco	HP
IBM	IE	IIS
Mozilla	MS_Office	Novel
Oracle	PHP_app	Sun

Tabla 9 Aplicaciones afectadas detectadas por IPS

Esta lista se puede ampliar para incluir más opciones seleccionando elenlace. Las opciones adicionales incluyen:

ASP_app	CA	DB2
IM	Ipswitch	MailEnable
MediaPlayer	MS_Exchange	MSSQL
MySQL	Netscape	P2P
PostgreSQL	Real	Samba
SAP	SCADA	Sendmail
Veritas	Winamp	Other

Tabla 10 Otras aplicaciones detectadas por IPS

Protocolo

Se refiere al protocolo que es el vector de ataque.

Las opciones incluyen:

DNS	FTP	HTTP
ICMP	IMAP	LDAP
POP3	SCCP	SIP
SMTP	SNMP	SSH
SSL	TCP	UDP

Tabla 11 Protocolos vector de ataques

Esta lista se puede ampliar para incluir más opciones seleccionando el enlace. Las opciones adicionales incluyen:

BO	DCERPC	DHCP
DNP3	H323	IM
MSSQL	NBSS	NNTP
P2P	RADIUS	RDT
RPC	TRCP	RTP
RTSP	TELNET	TFN

Tabla 12 Otros protocolos vector de ataques

Se escoge una acción para cuando se desencadena una firma.

Signature Default. Todas las firmas predefinidas tienen una acción atributo que se establece en pasar o soltar. Esto significa que si una firma

incluido en el filtro tiene una acción de ajuste Pass, el tráfico de búsqueda de la firma será detectado y luego se deja continuar hasta su destino.
Seleccionar“Aceptarfirma por defecto”utiliza la acción predeterminada para cada firma incluida.

Monitor All.- Seleccionar“Monitor All” para pasar todo el tráfico coincidir las firmas incluidas en el filtro, independientemente de su valor predeterminado “ActionSetting”.
Block All.- Seleccionar “Block All” para descartar tráfico Cualquiera de las firmas incluidas en el filtro.
Reset.-Seleccionar Restablecer para restablecer la sesión cada vez que se activa la firma. En la CLI esta acción se conoce como Reject.
Quarantine.- Tiene 2 campos de la necesidad de ser configurados:
1. Método:
• Dirección IP del atacante - El tráfico de la dirección IP del atacante se negó hasta que se alcance el tiempo de expiración del trigger.
• Dirección del atacante y víctima - Todo el tráfico desde la dirección del atacante a la dirección de la víctima se bloqueará.
• Interfaz de entrada de ataque - la interfaz que experimentó el ataque se niegan aún más el tráfico.
2. Expira (marco de tiempo que la cuarentena estará en efecto):
• 5 minuto (s)
• 30 Minutos (s)
• 1 Hora (s)
• 1 Día (s)
• Una semana (s)
• Mes (s)
• Año (s)

Packetlogging.- Seleccione para habilitar el registro de paquetes para el filtro.
Cuando se habilita el registro de paquetes en un filtro, la unidad guarda

una copia de los paquetes que coincidan con las firmas incluidas en el filtro.
Los paquetes pueden ser analizados más adelante.
Seleccione aceptar.
Se crea el filtro y se añade a la lista de filtros.

2.9.7. Actualización de firmas IPS predefinidas

El servicio FortiGuard actualiza constantemente las firmas predefinidas y agrega nuevas firmas para contrarrestar las amenazas emergentes a razón que aparecen.

Debido a que las firmas incluidas en los filtros se definen por medio de la especificación de los atributos de la firma, las nuevas firmas que emparejan especificaciones filtros existentes se incluirán automáticamente en esos filtros. Por ejemplo, si usted tiene un filtro que incluye todas las firmas para el sistema operativo Windows, el filtro incorporará automáticamente nuevas firmas de Windows como se abonen.

2.9.8. Visualización y búsqueda de firmas IPS predefinidas

Ir a los perfiles de seguridad> Protección de Intrusión> Firmas IPS para ver la lista de firmas IPS existentes. Se puede encontrar firmas por la paginación de forma manual a través de la lista, aplicar filtros, o usando el campo de búsqueda.

2.9.9. Configuración de un sensor IPS

La mayoría de los ajustes de IPS se configuran en un sensor IPS. Sensores IPS se seleccionan en las políticas de firewall. De esta manera, puede crear múltiples sensores IPS, y adaptarlos al tráfico controlado por la política de seguridad en el que se seleccionan. En este ejemplo, creará un sensor IPS.

2.9.10. Para crear gestor basado en web un IPS Sensor-

1. Ir a Security Profiles > Intrusion Protection > IPS Sensors.

2.Seleccionar el ícono Create New En la parte superior de la ventana de edición del sensor IPS.

3.En el campo de nombre escribir basic_ips.

4.En el campo comentario ingrese “protectionfor Windows clients.”

5.Seleccionar OK.

6.Seleccionar “the Create New drop-down” para añadir un nuevo componente al sensor y para el tipo de sensor elegir Filter Based.

7.En las opciones de filtro se escoge las siguientes:

a.Para Severity: Seleccionar todas las opciones

b.Para Target: Seleccionar sólo Cliente

c. Para OS: Seleccionar sólo Windows.

8. En Action dejar por default.

9.Seleccionar OK para guardar filtro.

10. Seleccionar OK para guardar el sensor IPS.

2.9.11. Para crear un sensor IPS — CLI

```
Configips sensor
Editbasic_ips
set comment "IPS protection for Windows clients"
config entries

edit 1

set location client
set os windows
end
end
```

2.9.12. Selección del sensor IPS en una política de seguridad

Un sensor IPS dirige la unidad Fortigate para analizar el tráfico de la red sólo cuando se selecciona en una política de seguridad. Cuando se selecciona un sensor IPS en una política de seguridad, sus valores se aplican a todo el tráfico se encarga de la política de seguridad.

2.9.13. Para seleccionar el sensor IPS en una política de seguridad - gestor basado en web

1. Ir a la Policy>Polícy> Polícy.
2. Seleccione una política, “Policy”
3. Seleccione el ícono Editar.
4. Habilite la opción IPS.
5. Seleccione el perfil basic_ips de la lista.
6. Seleccione Aceptar para guardar la directiva de seguridad.

2.9.14. Aplicación de IPS en nuestro caso de estudio

Para la aplicación de IPS en nuestra solución propuesta tenemos que seguir los siguientes pasos:

- Nos dirigimos hacia el menú de configuraciones (lado izquierdo).
- Escogemos la opción de UTM Profiles.
- Desplegamos la opción de IntrusionProtection.
- Escogemos la opción IPS Sensor.
- Escogemos el sensor que viene por predeterminado le damos en editar.

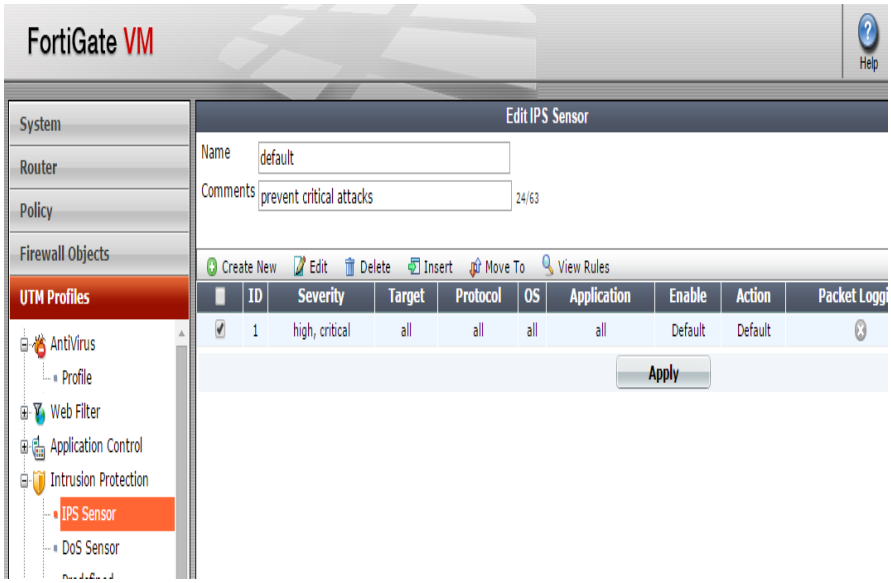


Figura 2.7Configuración de IPS en Firewall Fortigate

Al dar editar en el IPS nos va a mostrar todas las políticas que viene preestablecida para el control de los intrusos, simplemente podemos dejar activa todo lo que está ya predefinido.

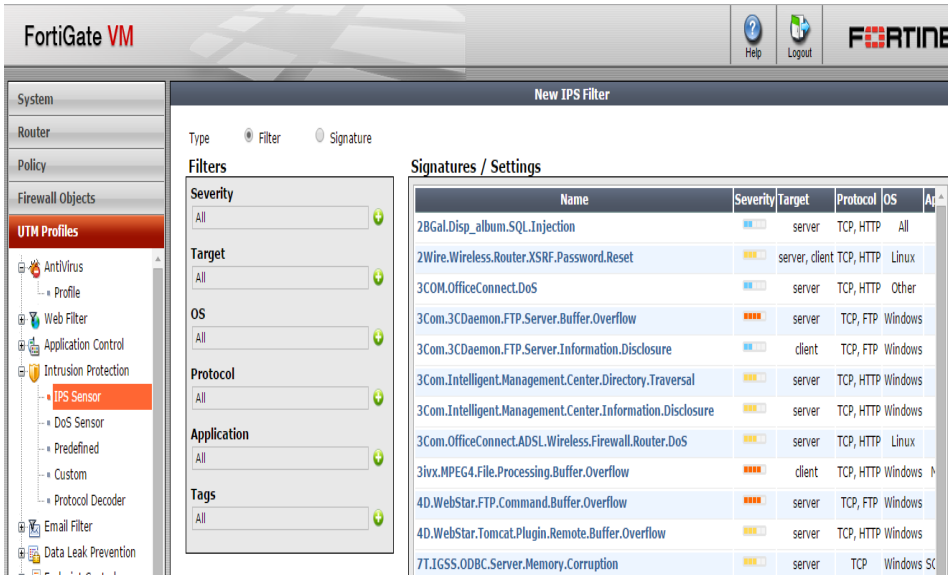


Figura 2.8Políticas preestablecidas del IPS

Para poder establecer nuestras propias reglas, podemos escoger las opciones de los filtros y cambiarlas de acuerdo a nuestras necesidades. En nuestro caso lo dejamos de la siguiente manera.

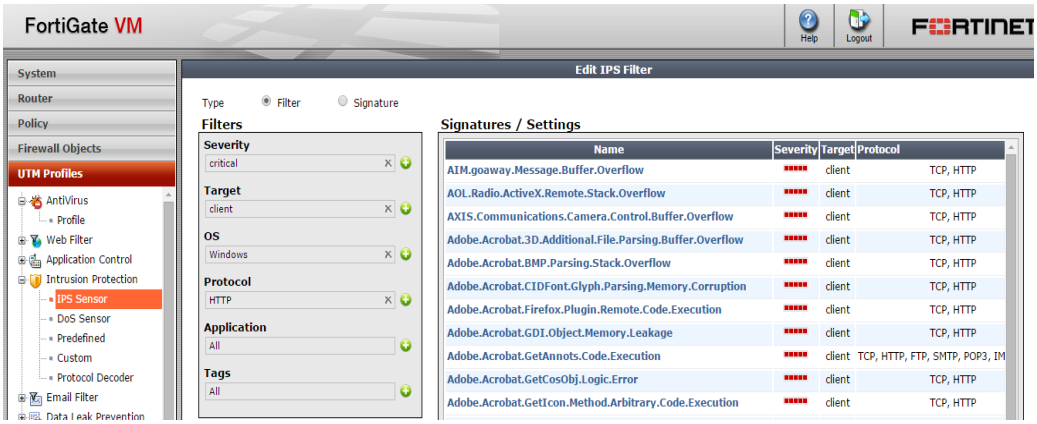


Figura 2.9 Configuración de IPS

2.10. Análisis de la seguridad en la red mediante el uso de normas AAA

Vensur S.A. al ser una empresa grande y en constante crecimiento necesita implementar un sistema de seguridad que proteja sus redes y servicios de red frente a accesos no autorizados para poder garantizar el control de quien se conecta a la red y que están autorizados a realizar los usuarios conectados y al mismo tiempo debe permitir tener un registro de toda actividad de la red.

Las normas AAA que son conformadas por protocolos como Radius y Tacacs+ (ambos desarrollados por cisco) y algunos otros fueron creados para resolver los problemas antes mencionados, es gracias a las normas AAA que se puede permitir el acceso de los usuarios legítimos e impedir todo acceso no autorizado.

2.10.1. Normas AAA

Cuando se trata de seguridad informática, al mencionar lasnormas AAA nos referimos a un conjunto de protocolos que realizan tres funciones dentro de una red, autenticación, autorización, auditoría (en inglés, *Authentication, Authorization and Accounting*) de ahí su nombre.

2.10.2. Autenticación

La autenticación se define como el procedimiento mediante el cual una entidad prueba su identidad a otra, usualmente la primera entidad suele ser un cliente o un usuario y la segunda un servidor configurado para reconocer la identidad de la primera entidad.

La autenticación se logra a través de una o más pruebas de identidad presentando por ejemplo un nombre de usuario y demostrar una credencial que compruebe el mismo, por ejemplo una contraseña, un token (llave electrónica), certificado digital, etc, pero los métodos de autenticación modernos permiten demostrar la posesión de las credenciales requeridas sin la necesidad de transmitirlas por la red, lo cual lo hace más seguro, ejemplo huella dactilar, escáner de retina.

2.10.3. Autorización

El termino autorización se refiere a la asignación de permisos a una entidad basándose en su identidad sobre los permisos que solicita, estos permisos son generalmente basados en restricciones tales como horarias, restricción de localización y de acceso múltiple del mismo usuario.

Los privilegios que si son concedidos se basan en el uso de un determinado tipo de servicio, por ejemplo asignación de direcciones IP permitidas, asignación de rutas, parámetros de calidad de servicio, cifrado y asignación de ancho de banda.

2.10.4. Auditoría

La función de auditoría trata del seguimiento y control del consumo de los recursos de la red por parte de cada uno de los usuarios.

Esta información se podrá usar para la administración, planificación, facturación u otros propósitos.

La auditoría en tiempo real es en la que los datos que se generan son entregados al mismo tiempo mientras se produce el consumo de los recursos, por otra parte la auditoría por lotes, consiste en almacenar todos los datos del consumo de los recursos para su entrega y revisión en un momento posterior.

El mayor porcentaje de la información almacenada en la auditoría es aquella que registra la identidad del usuario así como también los tipos de servicio que se le proporcionan y cuando empezó y terminó de usarlos.

2.11. Seguridades aplicando AAA

Para aplicar el mecanismo de seguridad por medio de autenticación, autorización y auditoría se procederán a configurar los enrutadores ya existentes en la compañía para obtener de ellos el mayor provechoy a la vez se optimiza costos, se asignará un usuario y contraseña para cada miembro de la empresa y se le otorgaran los permisos respectivos.

2.11.1. Funcionalidades de AAA

- Autenticar y controlar el acceso a la red de cada miembro de la empresa mediante un usuario y contraseña establecidos.
- Autorizar un nivel de acceso a cada usuario. Ejemplo: administrador, usuario, invitado.

- Generar un informe detallado de lo que realiza cada usuario en cada ingreso de su respectiva sesión.

2.11.2. Configuración del enrutador para la aplicación de normas AAA

Para poder centralizar el manejo de cuentas de usuarios y acceder a los dispositivos de red utilizaremos 2 protocolos que son Tacacs+ Y Radius, una de las diferencias es que Tacacs+ cifra todo el tráfico desde que se solicita la comprobación del usuario hasta que termina, en cambio Radius solo cifra la contraseña.

En los enrutadores de la matriz y las sucursales se configurará el protocolo AAA de forma local, los comandos que se utilizan son los mostrados en la Tabla 13 y se demuestra en una simulación realizada en el software GNS3.

aaa new-model	Indica que se va a crear un nuevo modelo de autenticación (AAA).
aaa authentication login modelo 1 group tacacs+ local	Se configura el login, se puede crear varios modelos de autenticación, poniendo el nombre del modelo indicando que estará vinculado con el grupo tacacs+ además se indica que si falla el servidor AAA haga login mediante la base de datos local.
aaa authentication enable default group tacacs+	Configuración modo privilegiado enable con default y tacacs+ para respaldar si cae el AAA.
aaa authorization exec modelo 1 if-authenticated	Se autorizan los comandos execute con cada modo para que se pueda ejecutar comandos una vez autenticado.
tacacs+server host 192.168.1.3key 1234	Indica al router donde se encuentra el servidor informando lakey compartida que se introducirá en el server (debe ser la misma).

Tabla 13 Tabla de comandos en router para habilitar AAA

A continuación se simulará la configuración en el router:

Paso 1: Asignación de niveles de privilegio por usuario

Usuario nivel 0 – solo accede a modo usuario

Usuario nivel 1 a 14 – Se pueden asignar diferentes comandos para cada nivel

Usuario nivel 15 – Acceso a modo privilegiado completo

La configuración de diferentes niveles de acceso es particularmente útil en entornos en los que diferentes técnicos tienen asignadas a diferentes tareas.

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#hostname RouterMatriz
RouterMatriz(config)#username Administrador1 privilege 15 secret v3n$uR
RouterMatriz(config)#aaa new-model
RouterMatriz(config)#aaa authentication login default local none
```

Figura 2.10 Configuración de usuario administrador en el enrutador matriz

Paso 2: **Implementación de servicio AAA para el acceso de las líneas VTY usando la base de datos local.**

```
R2#
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#hostname RouterMatriz
RouterMatriz(config)#username Administrador1 privilege 15 secret v3n$uR
RouterMatriz(config)#aaa new-model
RouterMatriz(config)#aaa authentication login default local none
RouterMatriz(config)#aaa authentication login TELNET_LINES local
RouterMatriz(config)#line vty 0 4
RouterMatriz(config-line)#login authentication TELNET_LINES
```

Figura 2.11 Configuración enrutador matriz para acceso VTY

En el enrutador se configuró las normas AAA con su respectivo nombre de usuario y contraseña con servicio telnet el cual será accedido desde una PC. La configuración en el enrutador se la realiza tanto a nivel de consola y por líneas VTY para su respectivo acceso telnet.

Paso 3: Configuración AAA autenticación local usando cisco CCP

```
R2#
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#hostname RouterMatriz
RouterMatriz(config)#username Administrador1 privilege 15 secret v3n$uR
RouterMatriz(config)#aaa new-model
RouterMatriz(config)#aaa authentication login default local none
RouterMatriz(config)#aaa authentication login TELNET_LINES local
RouterMatriz(config)#line vty 0 4
RouterMatriz(config-line)#login authentication TELNET_LINES
RouterMatriz(config-line)#exit
RouterMatriz(config)#aaa new-model
RouterMatriz(config)#ip http server
RouterMatriz(config)#username Administrador1 privilege 15 secret v3n$uR
RouterMatriz(config)#ip http authentication local
RouterMatriz(config)#
```

Figura 2.22 Configuración líneas VTY

Paso 4: Observar autenticación AAA usando depurador cisco IOS

```
RouterMatriz#
*Jul 17 17:55:20.000: %SYS-6-CLOCKUPDATE: System clock has been updated from
01:09:33 UTC Fri Mar 1 2002 to 17:55:20 UTC Fri Jul 17 2015, configured from
console by console.
RouterMatriz#clock set 17:55:20 10 september 2015
RouterMatriz#
Sep 10 17:55:20.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 1
7:55:45 UTC Fri Jul 17 2015 to 17:55:20 UTC Thu Sep 10 2015, configured from
console by console.
RouterMatriz#
```

Figura 2.33 Depurador Cisco

Paso 5: Usar depuración para verificar el acceso a usuarios

```
RouterMatriz#debug aaa  authentication
AAA Authentication debugging is on
RouterMatriz#
```

Figura 2.44 Confirmación de activación de AAA

Paso 6: Configuración de SSH como método de acceso al enrutador y un usuario local.

```
RouterMatriz(config)#ip domain-name vensur.ec
RouterMatriz(config)#crypto key generate rsa
% You already have RSA keys defined named RouterMatriz.vensur.ec.
% Do you really want to replace them? [yes/no]: y
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 102
*Sep  2 00:46:50.735: %SSH-5-DISABLED: SSH 1.99 has been disabled
1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

*Sep  2 00:46:58.495: %SSH-5-ENABLED: SSH 1.99 has been enabled
RouterMatriz(config)#ip ssh time-out 60
RouterMatriz(config)#ip ssh authentication-retries 2
RouterMatriz(config)#aaa new-model
RouterMatriz(config)#line vty 0 4
RouterMatriz(config-line)#transport input ssh
RouterMatriz(config-line)#username ErickChavez secret 3PcL$
RouterMatriz(config)#
```

Figura 2.55 Configuración de SSH

La configuración de los servidores se muestra a continuación:

SERVIDOR TACACS+

1.- En el servidor se añaden los dispositivos que será cliente del servidor AAA tipo TACACS.

2.- Se crea una base de datos, con los usuarios que podrán autenticarse.

Se configuro el enrutador agregando su respectivo modelo AAA en este caso utilizamos el comando **tacacs+ server**con el fin de autenticarnos con el servidor.

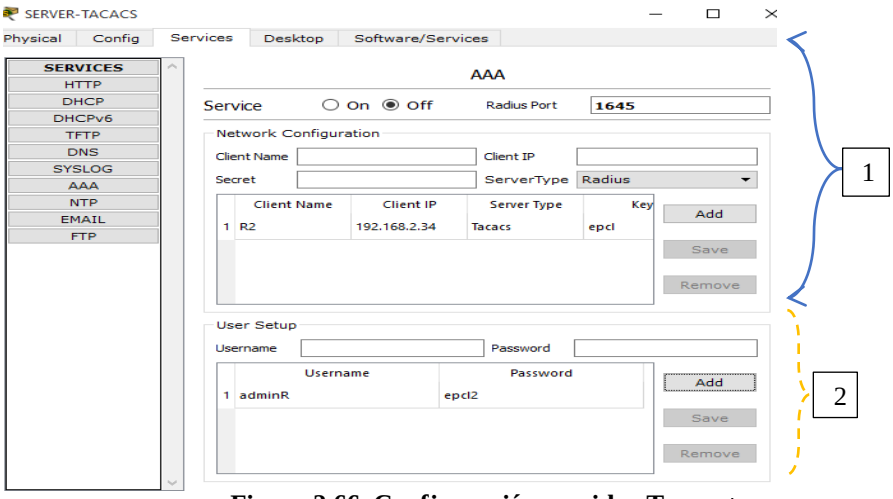


Figura 2.66 Configuración servidor Tacacs+

El primer comando autoriza localmente la ejecución de los comandos de nivel 15 utilizando la lista predeterminada. El segundo autoriza localmente algunos servicios de red utilizando una lista particular. El tercero registra remotamente los comandos de nivel 15 utilizando TACACS+ para la lista por defecto.

SERVIDOR RADIUS

Se configuro el enrutador 1 agregando su respectivo modelo AAA en este caso utilizamos el comando **radius-server host** con el fin de autenticarnos con el servidor

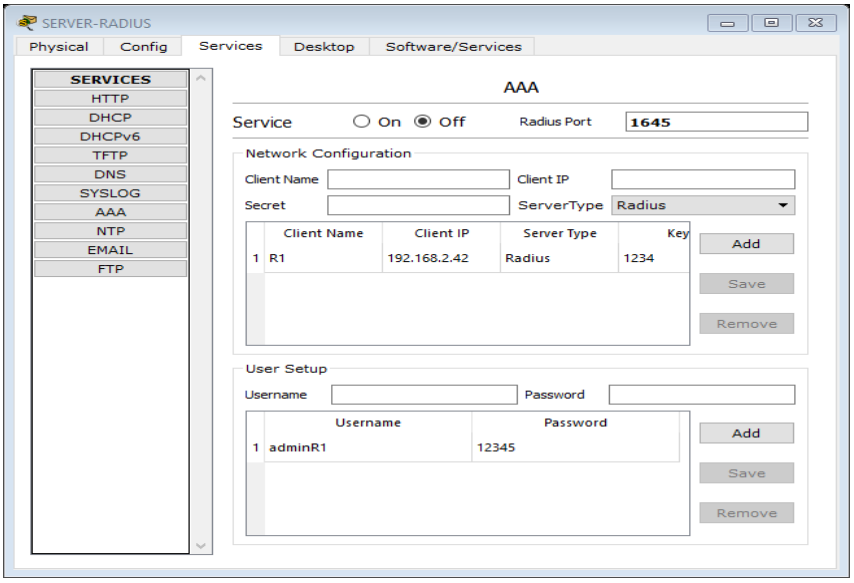


Figura 2.77 Configuración servidor Radius

Detalle de comandos utilizados en configuración AAA

Autenticación

En nuestro primer punto, vamos a usar el servidor Radius (192.168.1.5) para autenticar los accesos por SSH para la gestión del enrutador; para ello, usamos el usuario Administrador1 definido previamente por el Administrador, en el fichero User de Radius, no obstante, no usaremos certificados en nuestra configuración. Con el usuario ya definido, añadiremos un nuevo cliente al fichero clients.conf que se corresponderá con el enrutador de nuestra infraestructura

{

secret = password

shortname = router

nasstype = cisco

}

A continuación, nos conectamos al dispositivo de red e indicamos que la autenticación va a usar el servidor Radius. Para ello, seguimos los siguientes pasos:

```
RouterMatriz(config)#
RouterMatriz(config)#$er host 172.18.0.155 auth-port 1812 acct-port 1813
RouterMatriz(config)#radius-server deadtime 15
RouterMatriz(config)#radius-server key password
RouterMatriz(config)#
```

Figura 2.88 Autenticación Radius

Configuramos el método de autenticación. Es importante configurar varios métodos de autenticación por si no está disponible alguno de ellos, no perder el acceso al dispositivo. En este caso, el segundo método de autenticación es la base de datos local del propio equipo

```
RouterMatriz(config)#$er host 172.18.0.155 auth-port 1812 acct-port 1813
RouterMatriz(config)#radius-server deadtime 15
RouterMatriz(config)#radius-server key password
RouterMatriz(config)#aaa authentication login usergroup radius local
RouterMatriz(config)#
```

Figura 2.99 Configuración base de datos local

Configuramos el acceso al dispositivo por SSH autenticando mediante Radius:

```
RouterMatriz(config)#line vty 0 4
RouterMatriz(config-line)#login authentication usergroup
RouterMatriz(config-line)#
```

Figura 2.2010 Acceso SSH

Autorización

La siguiente funcionalidad será, para usuarios autenticados, poder autorizar que acciones puede realizar, por ejemplo, que comandos tienen disponibles para ejecutar en el dispositivo. Para nuestro escenario inicial, el usuario Administrador1 no dispone de privilegios de administración del dispositivo:

Primero, definimos permisos para el nivel 3 de privilegios del sistema

```
RouterMatriz(config)#privilege exec level 3 show running-config
RouterMatriz(config)#privilege exec level 3 configure terminal
RouterMatriz(config)#privilege configure all level 3 interface
RouterMatriz(config)#
```

Figura 2.21 Privilegios del sistema

Con estos comandos, Administrador1, como operador de red, podría gestionar las interfaces de red y ver su configuración en el dispositivo. A continuación, definimos que el equipo use Radius como sistema de autorización, al igual que hicimos en el apartado anterior:

```
RouterMatriz(config)#
RouterMatriz(config)#aaa authorization exec usergroup group radius local
RouterMatriz(config)#
```

Figura 2.22 Sistema de autorización

Finalmente, lo asociamos el servidor de autorización a la conexión remota al dispositivo:

```
RouterMatriz(config)#aaa authorization exec usergroup group radius local
RouterMatriz(config)#line vty 0 4
RouterMatriz(config-line)#authorization exec usergroup
RouterMatriz(config-line)#
```

Figura 2.23 Servidor de autorización

Auditoría

La última opción es la de auditoría, de las tres funcionalidades que hemos trabajado, ésta es la que menos se ha usado. También hay que tener en cuenta que algunos comandos en los dispositivos Cisco que no funcionan con servidores Radius (por ejemplo, el accounting de comandos), sino que sólo se pueden configurar usando un servidor AAA tacacs+.

Para este apartado, la configuración será similar a la configurada anteriormente: hay que definir Radius dentro de la configuración de auditoría. Para nuestro ejemplo, definimos algunas opciones de auditoría de acceso remoto:

```
RouterMatriz(config-line)#$ing send stop-record authentication failure
RouterMatriz(config)#aaa accounting update periodic 1
RouterMatriz(config)#aaa accounting exec usergroup start-stop group radius
RouterMatriz(config)#aaa accounting network usergroup start-stop group radius
RouterMatriz(config)#
```

Figura 2.24 Configuración auditoría

A continuación, aplicamos accounting para las conexiones remotas:

```
RouterMatriz(config)#line vty 0 4
RouterMatriz(config-line)#accounting exec usergroup
RouterMatriz(config-line)#
```

Figura 2.115 Auditoría para conexiones remotas

2.12. Análisis de la seguridad en la red mediante el uso del SIEM

Security Information and Event Management (SIEM) en español Sistema de Seguridad y Administrador de Eventos, es una combinación de dos sistemas de seguridad: SIM (securityinformationmanagement), administración de seguridad de la información) y SEM (securityevent manager), administrador de eventos de seguridad). La tecnología SIEM proporciona un análisis en tiempo real de las alertas de seguridad generadas por el hardware y software de red. Las soluciones SIEM pueden venir como software, hardware, o administración de servicios, y también son utilizados para monitorear datos de seguridad y generar reportes para fines de cumplimiento.

Las siglas SEM, SIM y SIEM se han utilizado indistintamente, aunque hay diferencias en el significado y las capacidades del producto. El segmento de gestión de la seguridad que se ocupa del monitoreo en tiempo real, correlación de eventos, notificaciones y vistas de la consola que comúnmente se conoce como gestión de eventos de seguridad (SEM). La segunda área ofrece almacenamiento a largo plazo, el análisis y la comunicación de los datos de registro, y se conoce como gestión de seguridad de la información (SIM).

El término Información de seguridad y gestión de eventos (SIEM), dado por Mark Nicolett y Amrit Williams, de Gartner, en 2005, detalla las capacidades de los productos de la recopilación, análisis y presentación de información de la red y los dispositivos de seguridad, las aplicaciones de gestión de identidades y accesos, gestión de vulnerabilidades y los instrumentos de política de cumplimiento, sistema operativo, base de datos y registro de aplicaciones. Un objetivoprincipal es monitorear y ayudar a controlar los privilegios de usuario, servicios de Active Directory (AD), y otros cambios de configuración del sistema, así como el abastecimiento de auditoría de registro, revisión, y respuesta a incidentes.

2.12.1. Capacidades de un SIEM:

– Agregación de datos: SIEM/LM (administración de eventos) soluciones para administración de eventos desde muchas fuentes, incluyendo redes, seguridad, servidores, bases de datos, aplicaciones, proporcionando la capacidad de consolidar los datos monitoreados para ayudar a prevenir la pérdida de los acontecimientos cruciales.

– Correlación: busca los atributos comunes, y relaciona eventos en paquetes o incidentes. Este mecanismo proporciona la capacidad de realizar una variedad de técnicas de correlación para integrar diferentes fuentes, con el fin de convertir los datos en información. La correlación es típicamente una función de la parte de gestión de la seguridad en una solución SIEM completa.

– Alerta: el análisis automatizado de eventos correlacionados y la producción de alertas, para notificar a los destinatarios de los problemas inmediatamente. Una alerta puede ser un tablero de instrumentos, o enviarse a través de canales de terceros, tales como el correo electrónico.

– Cumplimiento: Las aplicaciones SIEM se pueden emplear para automatizar la recopilación de datos y la elaboración de informes que se adapten a los procesos existentes de seguridad, gobernabilidad y auditoría.

– Retención: SIEM / SIM emplea soluciones a largo plazo de almacenamiento de datos para facilitar la correlación de datos con el tiempo, y para proporcionar la retención necesaria para los requisitos de cumplimiento. Un largo plazo de retención de registros de datos es crítica en la investigación forense, ya que es poco probable que el descubrimiento de una violación de la red sea en el momento de la infracción se produzcan.**[14]**

2.12.2. Seguridades aplicando SIEM

Para la visualización de los logs y administración de eventos se requiere de un sistema SIEM, el cual nos ayudará en la monitorización de los mismos, para esto hemos optado por un sistema SIEM Open Source llamado OSSIM basado en sistema LINUX, el cual es muy eficaz ya que está compuesta por una integración de herramientas muy útiles como el Snort, OSSEC, Nagios y muchas otras. Para esta herramienta se procederá a adquirir un servidor con las características adecuadas en donde puede desarrollarse este servicio con total normalidad.

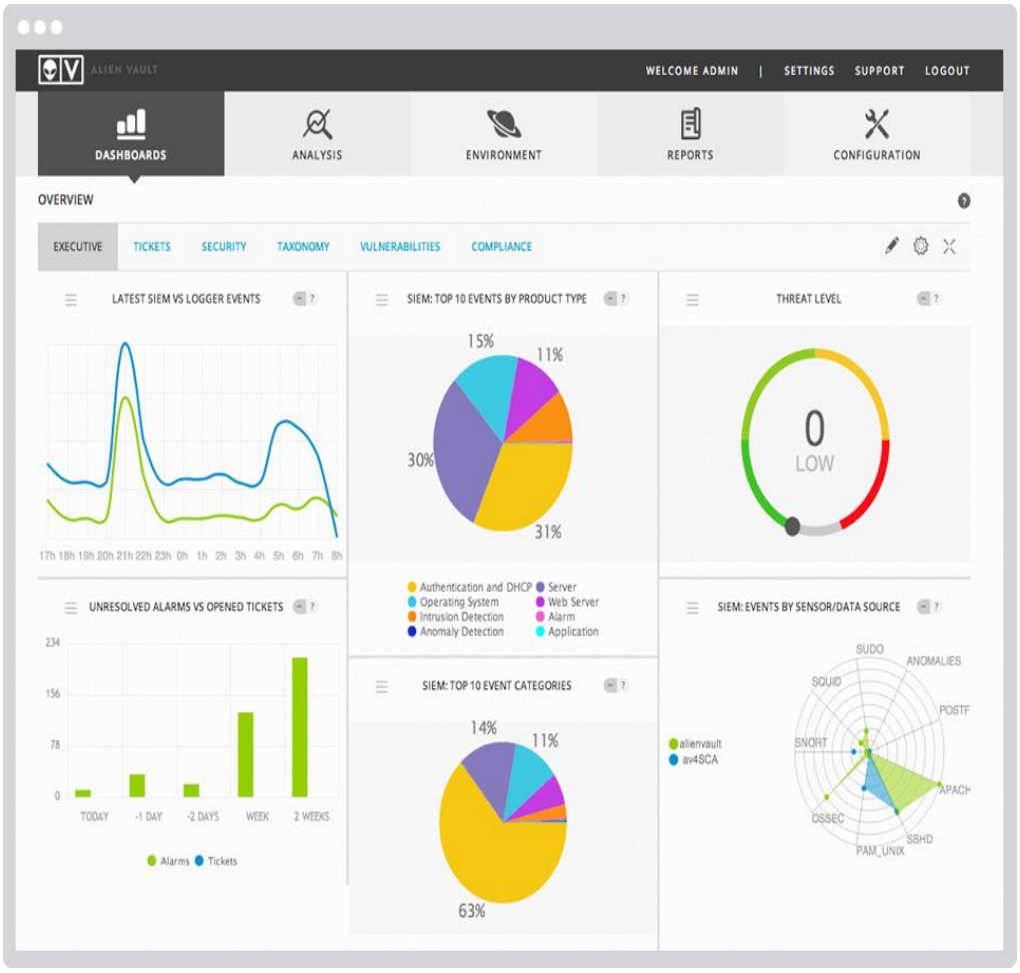


Figura 2.126 Interfaz gráfica SIEM

2.12.3. Requisito para el SIEM

Para realizar la implementación del sistema SIEM es necesario adquirir un servidor de buenas características para su óptimo funcionamiento aquí describimos las características del servidor a adquirir:

Especificaciones

HP 638180-001, ProLiant. Frecuencia del procesador: 2,13 GHz, familia de procesador: Intel Xeon 5000, modelo del procesador: E5606, memoria interna: 4 GB, tipo de memoria interna: DDR3-SDRAM, memoria interna máxima: 192 GB, características de red: Gigabit Ethernet, versión de entradas de PCI Express: 2.0, tipo de chasis: torre (5U), tipo de unidad óptica: DVD-ROM.

2.12.4. Beneficios del SIEM OSSIM

- Es un sistema de código abierto.
- Integra en una única consola todos los dispositivos y herramientas de seguridad para su monitoreo.
- Actúa como IDS e IPS.
- Constantemente está evolucionando.
- Podemos obtener información de eventos almacenados.
- Obtener datos estadísticos según ciertos parámetros de medidas.

2.12.5. Instalación y configuración de sistema SIEM

Para nuestro caso hemos tomado como sistema SIEM al software OSSIM, que es una aplicación de código abierto (Open Source) y que constantemente está en evolución y que nos brinda muchas bondades, ya que integra muchas herramientas que nos ofrece importantes servicios para el control y monitoreo de los eventos ocurridos en la red en tiempo real.

Entre los pasos para la instalación del Sistema OSSIM tenemos lo siguiente:

1. Con la imagen ISO procedemos con la instalación del sensor y del servidor SIEM

Figura 2.137 Instalación sensor SIEM

Luego de escoger el tipo de plataforma a instalar nos pide escoger el idioma.

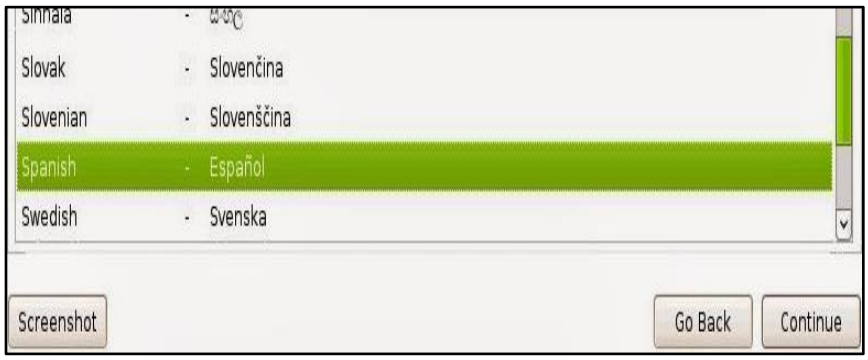


Figura 2.148 Selección de idioma en SIEM

Después colocamos la dirección IP, la cual nos servirá para el acceso web al servidor del SIEM.

Figura 2.159 Asignación dirección IP en SIEM

Se nos pedirá una clave que será la clave del superusuario o root, esta debe ser colocada 2 veces.

Figura 2.30 Clave súper usuario en SIEM

Al completarla instalación nos pedirá agregar la clave anteriormente colocada.

Figura 2.161 Login en el SIEM instalado

CAPÍTULO 3

3. PLAN DE TRABAJO Y ESTUDIO ECONÓMICO

En este capítulo se realiza un estudio económico detallado, en donde se describe el proceso que conlleva la implementación de la solución antes propuesta detallando el tiempo estimado y el costo de la implementación.

3.1. Análisis de factibilidad

En el Análisis de factibilidad se detalla la adquisición de los equipos a usar con su costo y descripción además el análisis del tiempo de trabajo.

3.1.1. Factibilidad Técnica

Recomendamos los siguientes equipos ya que es factible por su precio y además por los grandes beneficios que se adquirirán después de su implementación.

Función	Precio	Descripción	Ubicación
Firewall – IPS	5.500	**Firewall Fortigate 300C x 1** 22 Puertos 10/100/1000 Mbs 1 RJ-45 Serial Console 16 Gb Internal Storage 2.5 Millones Máxima Cantidad de Sesiones Concurrentes	Rack Principal,

Firewall – IPS	650.00	**Firewall Fortigate 70D x 3** Firewall Throughput 3.5 Gbps Concurrent Sessions 2 Million New Sessions/Sec 4,000	Sucursales: Machala, Portoviejo y Cuenca
SIEM	1600.00	**Servidor HP ProLiant ML350 G6 x 1** **Procesador:** Quad-Core Intel® Xeon® Processor E5520 (2.26GHz, 8M Cache, 80 Watts, 1066MHz) Memoria: 4Gb Ram	Matriz

Tabla 15 Factibilidad técnica

3.1.2. Factibilidad Económica

El costo de instalación, configuración y capacitación a la empresa Vensur S.A. es de $2,500.00 (dos mil quinientos 00/100), el costo total es de $11,550.00 (Once mil quinientos 50/100).

3.1.3. Factibilidad Operativa

Descripción	Tiempo
Fase de análisis de red LAN y WAN Técnico en Redes Analista de Soporte	5 días
Fase de diseño de red WAN Técnico en Redes Analista de Soporte	5 días
Fase de implementación de red WAN Técnico en Redes Analista de Soporte	7 días
Fase de prueba de red WAN Analista de Soporte	3 días
Fase de Documentación Técnico en Redes Analista de Soporte	3 días

Tabla 16 Factibilidad Operativa

3.2. Propuesta

- Diseñar solución de control de intrusos a la red configurando IPS.
- Proponer un sistema SIEM indicando su configuración y manejo.
- Proponer el uso de un firewall hardware robusto y realizar las configuraciones más adecuadas al caso.
- Implementar normativas de seguridad con ayuda de normas AAA.

3.3. Forma de Pago

Se plantea el pago de la siguiente manera:

- 60 % al momento de la aceptación de la propuesta.
- 40% en la fase de documentación.

3.4. Ventajas

- Mayor seguridad en la transmisión de información
- Control en el acceso a los servicios que se ejecutan
- Monitoreo en tiempo real del rendimiento de la red
- Subredes eficientes y manejables.
- No habría pérdida de comunicación y transmisión al contar con un Soporte tolerante a fallas.
- Convergencia de los enrutadores, aprovechamiento del ancho de banda.
- Respaldo del enlace de datos.

3.5. Beneficios

- Una red más segura y confiable
- Tener un registro de las actividades ante cualquier anomalía de la red.
- Descongestionamiento de la red, mejor rendimiento.
- Garantizar la continuidad de los servicios que ofrece la red.
- Aprovechar al máximo los recursos de la red.
- No se depende de un solo proveedor de datos.

3.6. Garantías

Una garantía de un año en lo que se refiere al buen funcionamiento de la red, la garantía del hardware es la que ofrece el fabricante, la empresaFortigate, es de dos años ante daños de fábrica.

3.7. Diagrama de Gantt

	Proyecto Vensur S.A.	34 días	mar 01/09/15	lun 19/10/15
	Inicio proyecto	0 días	mar 01/09/15	mar 01/09/15
	Analisis red Lan y Wan	5 días	mar 01/09/15	lun 07/09/15
	Identificación de riesgos	2 días	mar 01/09/15	mié 02/09/15
	Determinar controles existentes	1 día	jue 03/09/15	jue 03/09/15
	Análisis de riesgos	2 días	vie 04/09/15	lun 07/09/15
	Diseño de red wan	5 días	mar 08/09/15	lun 14/09/15
	Diseño	5 días	mar 08/09/15	lun 14/09/15
	Implementacion de red Wan	10 días	mar 15/09/15	lun 28/09/15
	Instalación en matriz	2 días	mar 15/09/15	mié 16/09/15
	Instalación sucursales	8 días	jue 17/09/15	lun 28/09/15
	Fase de prueba de red Wan	5 días	mar 29/09/15	lun 05/10/15
	Probar vulnerabilidades	1 día?	mar 29/09/15	mar 29/09/15
	Correcciones o ajustes de red	1 día?	mar 29/09/15	mar 29/09/15
	Fase de capacitación a personal	5 días	mar 06/10/15	mar 13/10/15
	Capacitación a matriz y sucursales	5 días	mar 06/10/15	mar 13/10/15
	Fase de Documentacion	3 días	mié 14/10/15	vie 16/10/15
	Recolección de datos	3 días	mié 14/10/15	vie 16/10/15
	Redactar reporte	1 día	mié 14/10/15	mié 14/10/15
	Entrega de proyecto	0 días	lun 19/10/15	lun 19/10/15

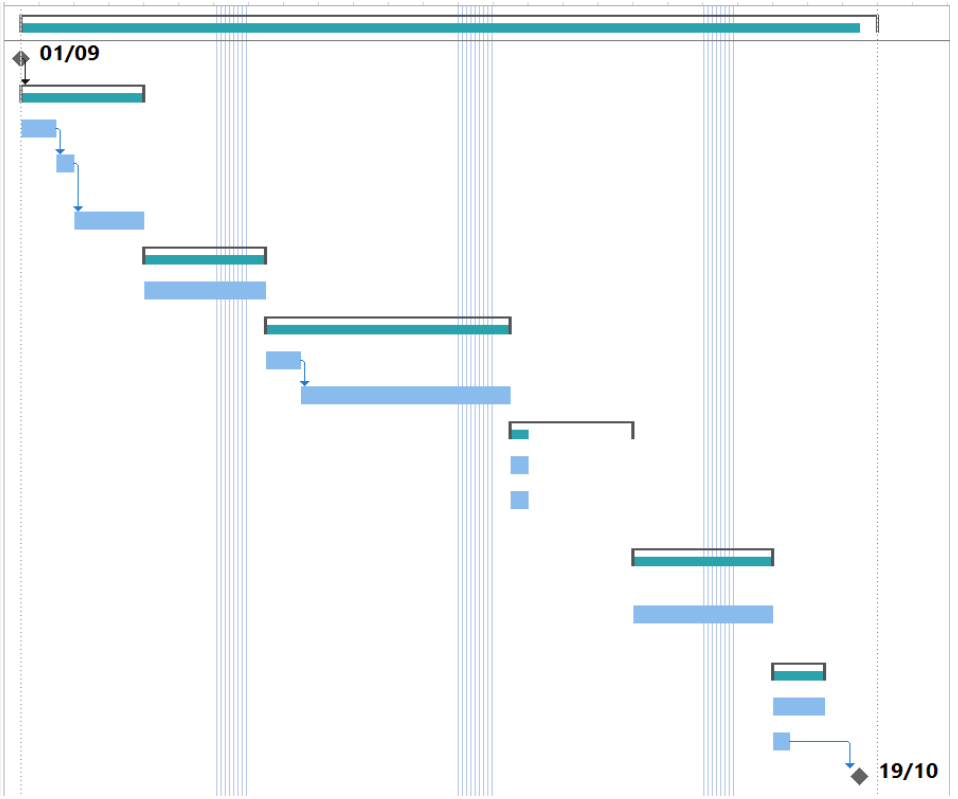


Figura 3.1 Diagrama de Gantt

CAPÍTULO 4

4. RESULTADOS Y PRUEBAS

Con la aplicación de este proyecto podemos garantizar a la compañía VENSUR S.A toda la mayor seguridad en toda su red, puesto que con la implementación de los mecanismos de seguridades aquí propuestos se establece reglas y políticas de transferencia de paquetes de datos teniendo así una red consistente y fiable.

4.1. Resultados al aplicar Firewall

La red de Vensur S.A. al contar con un firewall en cada oficina logrará administrar todos los accesos de datos provenientes de internet hacia la red privada, permitirá al administrador de red mantener fuera de la red privada a los usuarios no autorizados, también tendrá una bitácora donde se registrará el tráfico más significativo que pase a través de él.

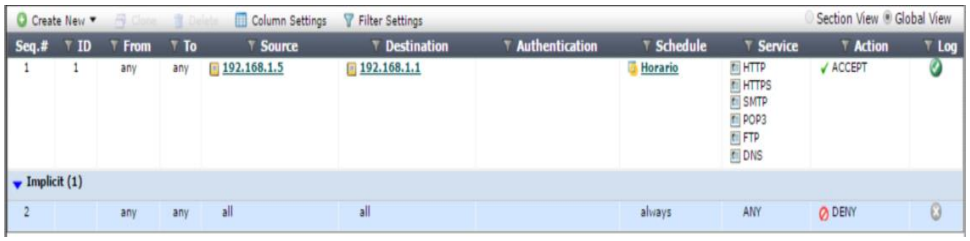


Figura 4.1Protocolos permitidos por el firewall Fortinet

En la figura se muestran los protocolos que si serán permitidos en la red de la empresa Vensur S.A., se permitirán los correos electrónicos, la transferencia de archivos entre los usuarios internos, navegación de internet, y la asignación de nombres de dominio a cada dirección IP.

4.2. Resultados al aplicar AAA

Con la ayuda de las normas AAA se logrará un nivel de seguridad corporativo muy alto ya que cada miembro de la empresa Vensur S.A. se regirá a un proceso de autenticación de su usuario y contraseña al momento de utilizar la red siéndole

asignado los permisos que cada uno necesite, por ejemplo un usuario del departamento de ventas no podrá tener acceso a la administración y el administrador del sistema tendrá permiso de configurar enrutadores y servidores, por último la persona encargada de la red tendrá un registro de todos los eventos que cada miembro del personal lleve a cabo con el fin de minimizar cualquier amenaza y poder llevar un control adecuado del uso de la red.

4.2.1. Demostración de restricciones aplicando normas AAA

Las tres imágenes siguientes muestran la configuración del router de la matriz de la empresa Vensur S.A. con el comando: show run

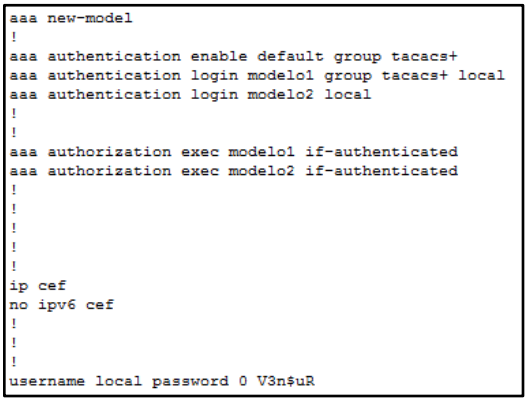
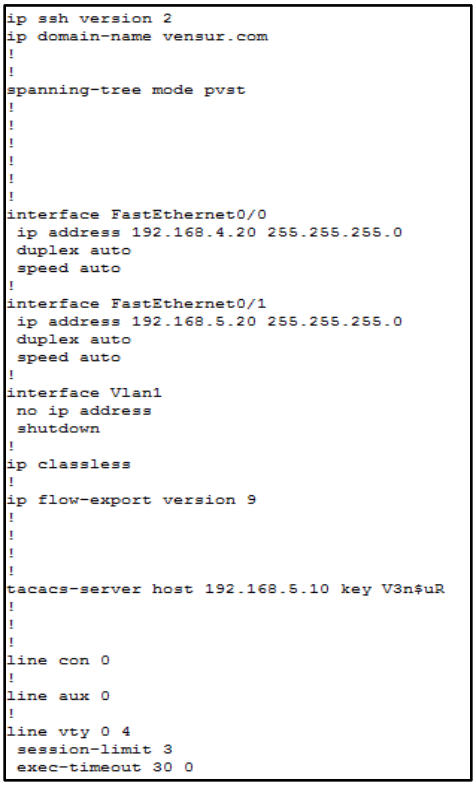


Figura 4.2Modelo AAA activado

Se activa el modelo AAA en la configuración del enrutador, luego de esto ingresamos el comando **aaa authentication enable default group tacacs+**el cual nos habilita la autenticación AAA por defecto en el grupo tacacs+.

Habilitamos el comando **AAAautenticación login modelo1 grupo tacacs+ local** el cualnos permite hacer login en nuestro enrutador de manera local

Comoúltimo comando autorizamos al modelo1 y modelo 2 para que solamente ellos puedaningresar.



```
ip ssh version 2
ip domain-name vensur.com
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.4.20 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.5.20 255.255.255.0
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
!
tacacs-server host 192.168.5.10 key V3n$uR
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 session-limit 3
 exec-timeout 30 0
```

Figura 4.3Habilitación comando IP SSH

Habilitamos el comando **IPSSH versión 2** este protocolo se asegura nuestra conexión remota a un enrutador mediante mecanismos criptográficos, agregamos direcciones IP a nuestras interfaces, el comando **tacacs server host** nos ofrece información contable y control administrativo flexible sobre los procesos de autenticación y autorización, agregamos el comando **line vty 0 4** para una conexión remota desde pc a router con una sesión límite de tres intentos.

```
tacacs-server host 192.168.5.10 key V3n$uR
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 session-limit 3
 exec-timeout 30 0
 login authentication modelo1
 transport input ssh
!
!
!
end


Erick#
```

Figura 4.4 Autenticación local

Agregamos el comando **login authentication modelo1** el cual haremos login de manera local en el enrutador y como último comando agregamos **transport input ssh**en el cual define que protocolos puedan conectarse

La configuración siguiente es un ejemplo del ingreso en el servidor de cada uno de los usuarios miembros tanto de la matriz como de las sucursales basándose en las normas AAA.

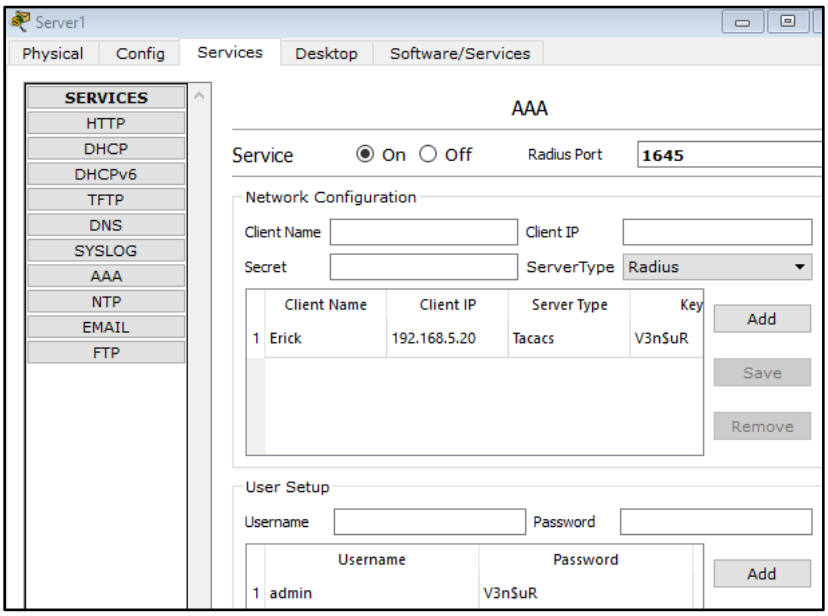


Figura 4.5 Ingreso servidor AAA

Con esta configuración tanto el servidor deberá autenticarse para agregar más usuarios, y de la misma manera se logra que cada miembro de la empresa se autentique con su propio usuario y contraseña.

Ahora una demostración de la seguridad implementada en el acceso al router desde una PC con el comando CMD o PROMT. El mismo fue configurado solo para que se permita tres intentos de acceso.

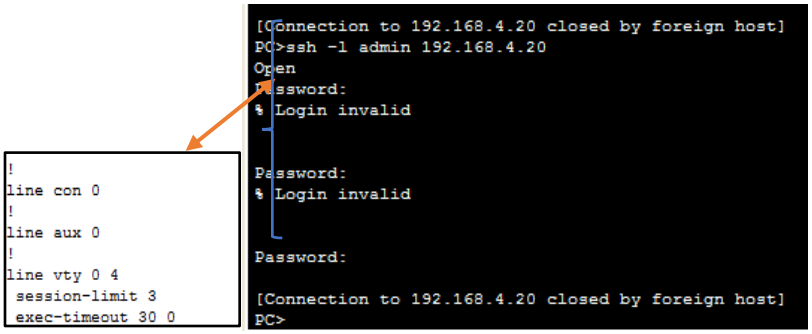


Figura 4.6Pruebas de acceso al router con contraseñas erróneas

Como se muestra en la figura, después del tercer intento de acceso la conexión al router se deniega.

Al momento de poner la contraseña del enrutador correcto, nos solicitará un usuario y una contraseña con privilegios para configurar el mismo.

```
PC>ssh -l admin 192.168.4.20
Open
Password:
Erick>ena
Username:
Password:
Erick#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
Erick(config)#
```

Figura 4.7 Prueba en PC

Se ingresó la clave del router (V3n$uR), y posteriormente el usuario (admin) y la contraseña (V3n$uR) que tiene el permiso para poder acceder y modificar el enrutador.

De la misma manera en el caso cuando se quiera acceder desde el servidor al enrutador se utilizara para esta demostración la dirección 192.168.5.20 y también se limitará hasta un máximo de tres intentos.

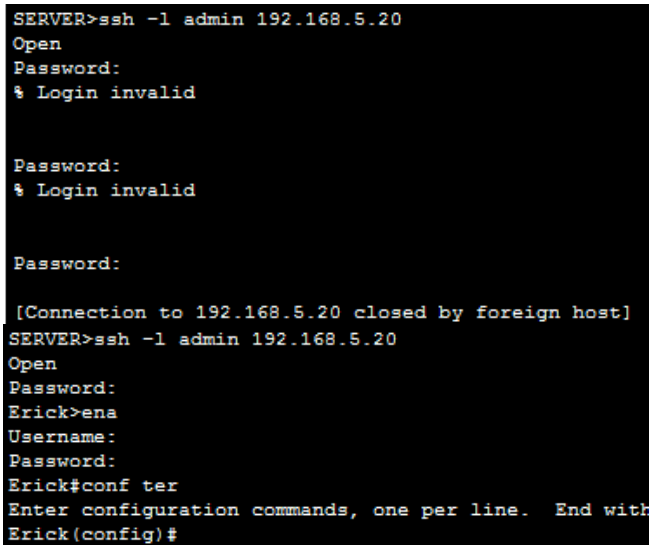


Figura 4.8 Acceso al enrutador desde el servidor

4.3. Resultados al Aplicar IPS

Entre los resultados al aplicar IPS tenemos:

4.3.1. Beneficios

- Una red más segura
- Protección preventiva antes de que se dé un ataque
- Protección más completa, ante vulnerabilidades del sistema operativo, puertos, tráfico de IP, códigos maliciosos e intrusos.
- Fácil instalación, configuración y administración
- Es escalable y permite la actualización de dispositivos a medida que crece la empresa

- No requiere tanta dedicación como un IDS tradicional; esto en consecuencia requeriría menos inversión en recursos para administrar y operar estos sistemas (en comparación con un IDS).

4.3.2. Mecanismo de aplicación

La aplicación del Sistema IPS es aplicado mediante el firewall Fortigate que será ubicado en la matriz y en las sucursales. Esto proveerá a las distintas sucursales la mayor seguridad en su acceso a la red.

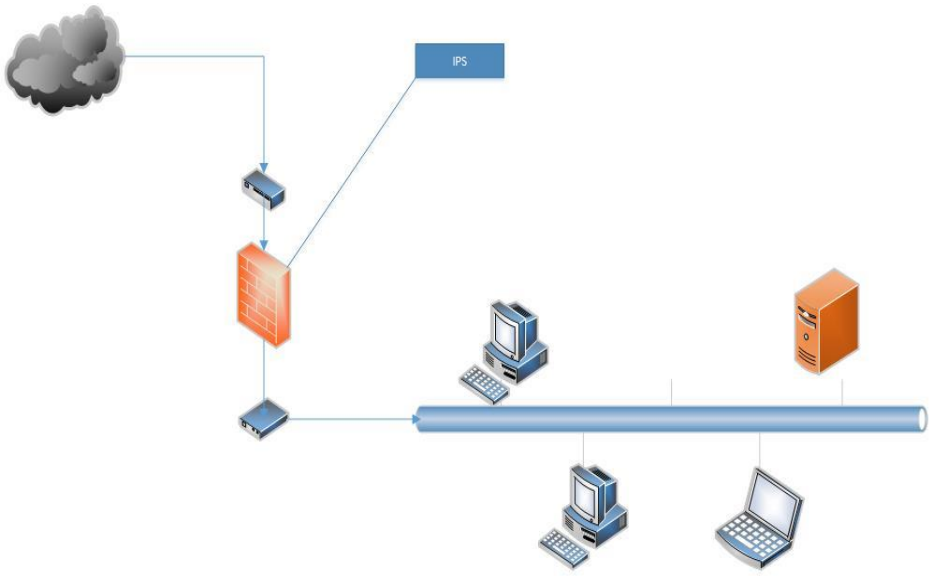


Figura 4.9Seguridad IPS en una red LAN

4.3.3. Prueba real del IPS en firewall Fortinet

Para confirmar que un IPS se encuentre correctamente configurado se realiza una prueba básica de inyección SQL (SQLI) para poder verificar que bloquee correctamente.

El SQLI es un mecanismo de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para ejecutar operaciones sobre una base de datos.

La prueba consistirá en colocar una aplicación web vulnerable **Damn vulnerable web app (DVWA),** la cual es indicada para este tipo de verificación.

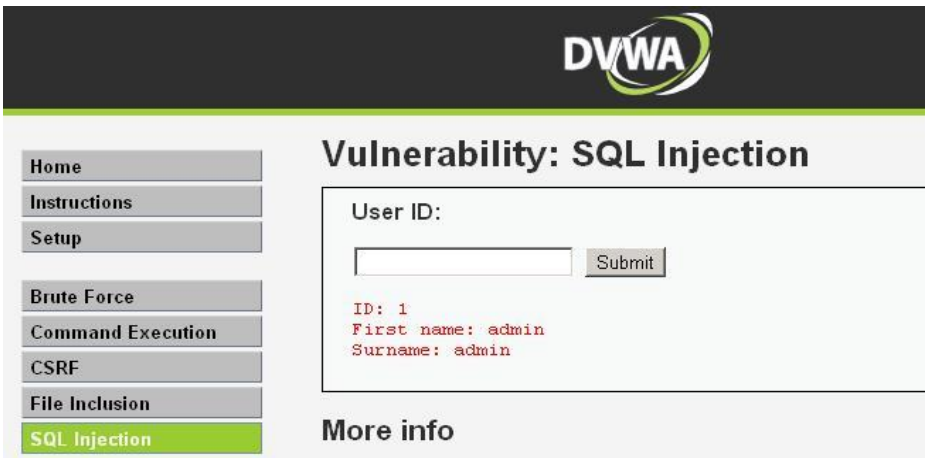


Figura 4.10Ejecución de prueba IPS

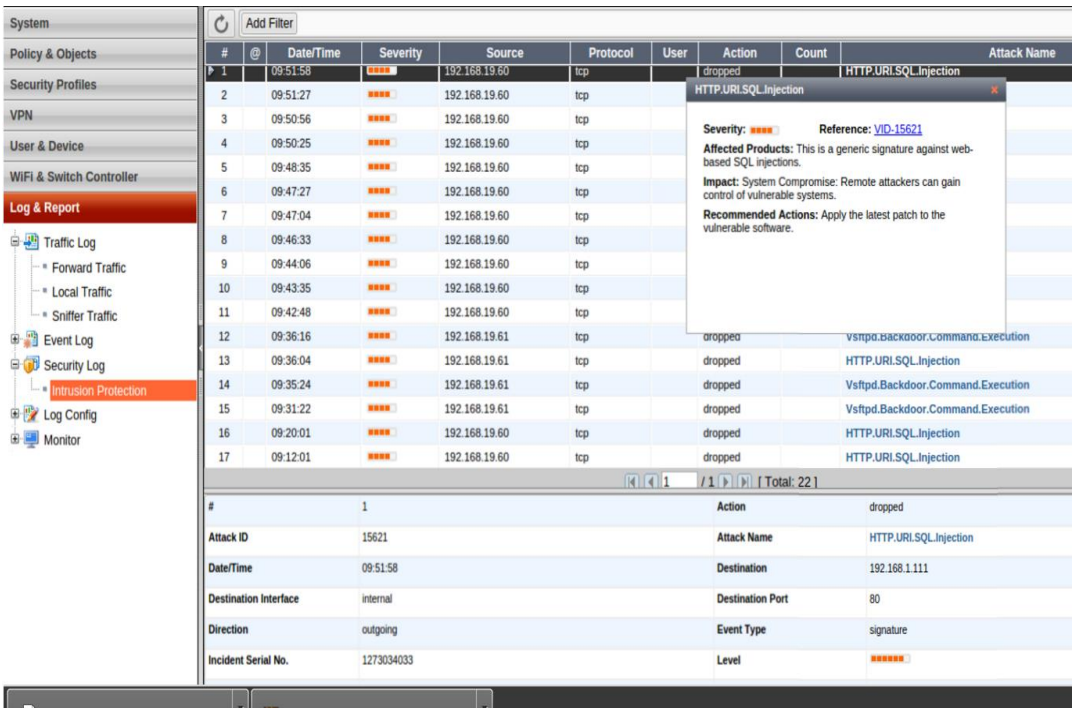


Figura 4.11Ejecución de prueba IPS

El IPS del firewall Fortinetdetecta el patrón del ataque SQL y lo bloquea correctamente.

Otra prueba para comprobar el funcionamiento del IPS es creando un ataque con **SQLMAP** que es una herramienta de pruebas de penetración de código abierto que automatiza el proceso de detectar y explotar los errores de inyección SQL y hacerse cargo de los servidores de bases de datos.

Figura 4.12Ejecución de prueba con SQLmap

Figura 4.13Ejecución de prueba con SQLmap 2

El IPS si detecta el ataque de SQLMAP y la bloquea, para que el IPS pueda bloquear estos tipos de amenazas no solo basta en realizar las

configuraciones correctas en el firewall, también es importante que se ejecute pruebas para comprobar su buen funcionamiento.

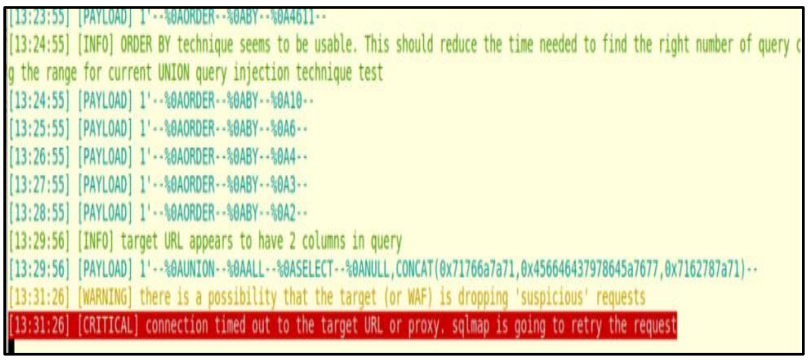


Figura 4.14 Pruebas SQL map

Desde la perspectiva de nosotros no es posible decir que la seguridad del equipo firewall Fortinet es perfecta, pero en el escenario de ataques SQLI es muy efectivo pero siempre se recomendarán más pruebas en otros escenarios para estar más conforme.

4.4. Resultados al Aplicar SIEM

Al aplicar el mecanismo del SIEM estamos estableciendo una seguridad Preventiva puesto que esta herramienta nos permite monitorear en línea todos los eventos que ocurren en el momento actual en la red, de esta manera si el visor nos muestra un mensaje de alerta podemos actuar al instante sabiendo por medio de la aplicación cuál es el daño y que acción tomar para su solución.

4.4.1. Beneficios de Aplicar Sistema SIEM OSSIM

- Monitoreo en línea de los eventos suscitados en la red.
- Detección de Intrusos.
- Prevención de Intrusos.
- Sistema de código libre.
- Constantemente está en evolución.

- Se puede obtener datos estadísticos según las referencias dadas.
- Podemos almacenar información y luego consultarlas.

4.4.2. Funcionalidades del SIEM

Entre las funcionalidades que podemos obtener al hacer uso del SIEM OSSIM tenemos:

- Monitor de sensor de alarmas.
- Monitor de logs en tiempo real.
- Reportes de eventos.
- Visor de dispositivos.
- Reportes general.

4.4.3. Monitor de Sensor de Alarmas

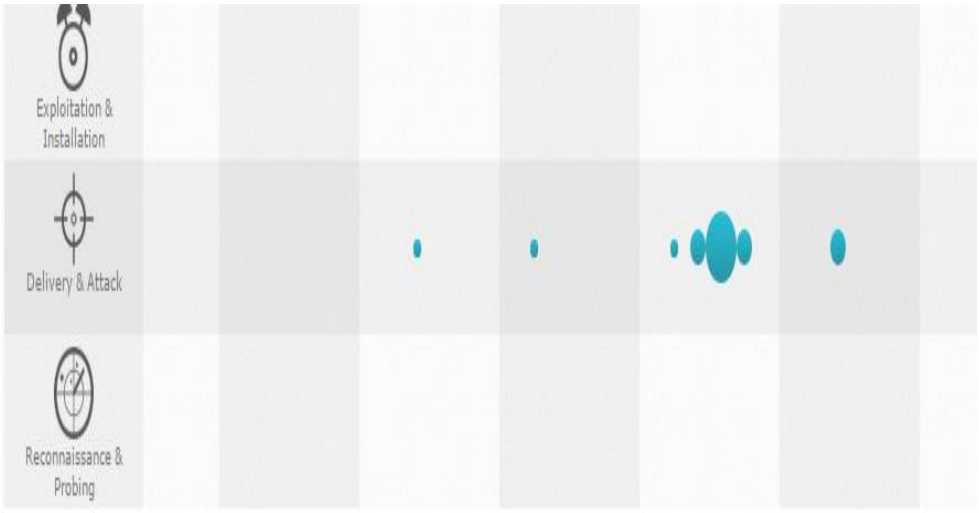


Figura 4.15 Monitor de sensor de alarmas

El monitor de sensor de alarmas mostrado en la Figura 4.15 nos permite tener un gráfico en línea que nos muestra una alarma en el instante en que se presenta una anomalía, indicándonos en ese momento la situación del estado, su proveniencia y su destino. Con todo ese detalle podemos acudir al origen de la detección para analizar cuál es el riesgo que puede causar.

Figura 4.16 Detección de tráfico

4.4.4. Monitor de logs en tiempo real

Otro de los grandes beneficios que nos ofrece la herramienta OSSIM es que nos permite monitorear en tiempo real los eventos que se está suscitando a través de la red, indicándonos en esta parte la fecha en que se realiza el evento y la hora, el nombre del evento que es detectada a través del software integrado OSSEC, también nos indica el servidor de sensor en este caso el OSSIM “alientvault” y finalmente nos indica el nombre de equipo de origen y destino.

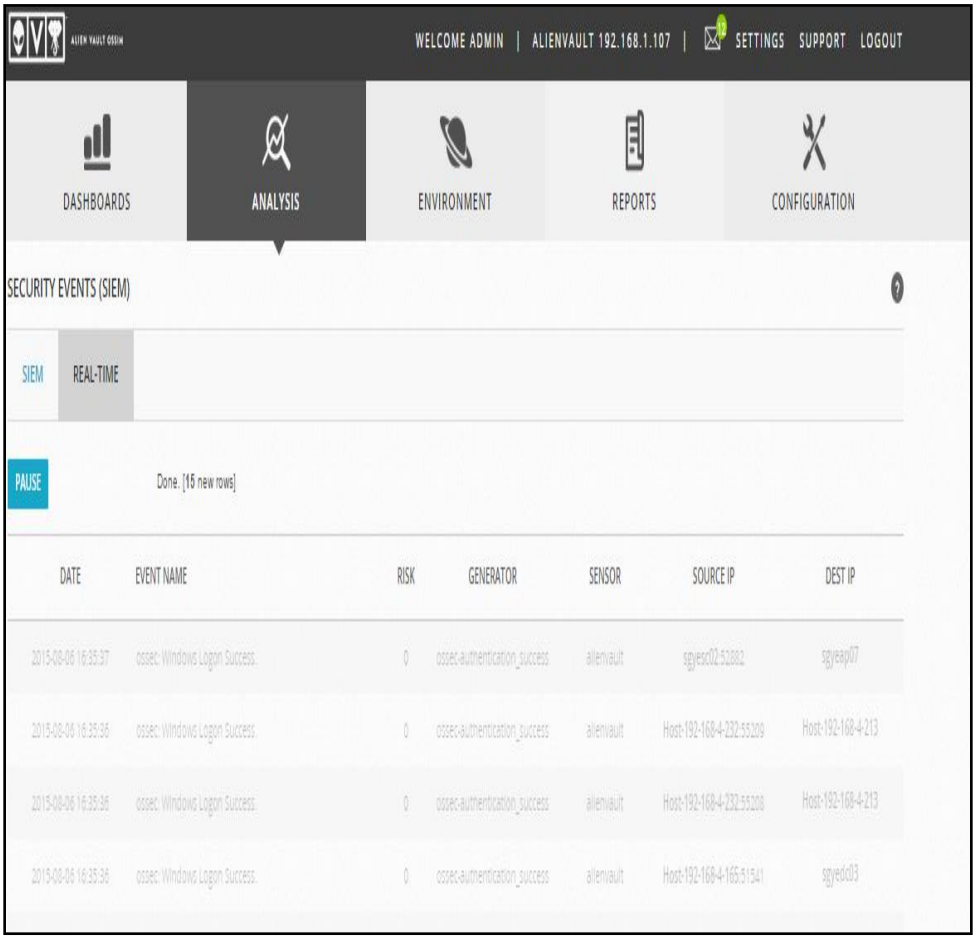


Figura 4.17Monitor de Log en tiempo real

En la figura 4.17 se muestran los eventos suscitados en la red en tiempo real, en donde podemos observar los riesgos que estos representan indicándonos la IP del origen del paquete como la IP de destino.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. La tecnología siempre está evolucionando, y con ello aumentan los medios o mecanismo para provocar una amenaza en una red.
2. Por los diversos tipos de amenazas, ataques y vulnerabilidades es imprescindible implementar ciertos mecanismos de seguridad que ayuden al control y gestión del tráfico en la red.
3. La falta de equipos apropiados para la seguridad en la compañía han provocado estar siempre en riesgo ante cualquier tipo de amenaza.
4. La falta de conocimiento apropiado por parte del administrador para mejorar la seguridad en la red, han hecho que la red se vea expuesta a ciertos tipos de riesgos.
5. Para prevenir los diversos tipos de ataques y amenazas que en los últimos años se han dado en la compañía VENSUR S.A se establece mecanismo de seguridad como el Firewall y IPS
6. Para monitorear de forma constante la red y estar siempre atentos ante cualquier tipo de novedad que pudiera presentarse se implementa un Sistema SIEM.
7. Para tener los equipos de comunicación siempre controlados ante el posible acceso no autorizado se implementa mecanismo de seguridad mediante los protocolos AAA
8. Este trabajo de tesis contribuye de manera eficiente a la compañía Vensur S.A a mantener siempre una red segura y de esta manera lograr que la información sea

siempre confiable, íntegra y disponible ya que la alteración de la información conlleva a resultados nefastos para la compañía

Recomendaciones

1. Se recomienda contar con otro proveedor de datos y de internet diferente al actual para establecer un sistema de respaldo en caso de fallo.
2. Se debe monitorear la consola de administración del antivirus para estar atentos ante cualquier novedad presentada. Además de mantener siempre la base actualizada y con licencia activa, esto ayudaría en la protección de equipos y de la red.
3. Dar el mantenimiento apropiado a los equipos para evitar futuras anomalías en especial en equipos de comunicación así como los switch, routers y servidores.
4. Realizar Auditorías a la seguridad informática de la compañía para tener un conocimiento de sus vulnerabilidades y que procedimientos seguir para minimizar los riesgos.
5. Invertir en capacitación del personal en medidas de seguridad informática.
6. Dentro del Departamento de sistemas debe existir una o varias personas cuyas funciones sean las de administrar la seguridad informática en la empresa.
7. La compañía Vensur S.A debe realizar un análisis de riesgo cada cierto tiempo para evaluar las posibles causas de vulnerabilidades que pudieran presentarse en la red.

8. Deberán establecerse Políticas de seguridad en base a los resultados del análisis de riesgo. Estas políticas serán claras para el correcto entendimiento y de conocimiento de todo el personal.

BIBLIOGRAFÍA

[1] https://www.fortinet.com/sites/default/files/productdatasheets/FortiGate-100D.pdf (Fortinet)

[2]http://www.cisco.com/web/LA/ofertas/catalyst/pdfs/switches_cisco_catalyst_serie_2960_x.pdf (Switch 2960)

[3] http://www8.hp.com/h20195/v2/GetDocument.aspx?docname=c04123249 (Hp Pro 3400)

[4] http://www.seguridadx.com/que-es-un-siem-que-es-prelude-siem/siem

[5] Wikipedia Categoría Redes Informáticas | Protocolos; 15 de junio del 2011; Modelo TCP/IP; <http://es.wikipedia.org/wiki/Modelo_TCP/IP>; Última Revisión: Marzo 201 1

[6] Cisco Networking Academy <CCNA Exploration 4.0: WAN > 2007-2008; Última Revisión: Abril 2011

[7] Categoría Protocolos de internet | Protocolos de nivel de transporte; <http://es.wikipedia.org/wiki/Categor%C3%ADa:Protocolos_de_nivel_de_transporte>;Última revisión: Marzo 2011

[8] Redes de Datos, Instructivo Laboratorio 1; Curso 20100 Montevideo-Uruguay; <http://iie.fing.edu.uy/cursos>; Última Revisión: Marzo 2011

[9] Wikipedia Categoría Redes Informáticas | Protocolos; 15 de agosto del 2015; OSSIM; <http://es.wikipedia.org/wiki/Modelo_TCP/IP>; Última Revisión: Marzo 2014

[10] Curso de seguridad y sistemas de información es.slideshare.net/nyzapersa/curso-seguridad-en-sistemas-de-informacion

[11] Tipos de amenazas informáticas https://windsofthesky.wordpress.com/.../tipos-de-amenazas-informaticas/

[12] Programa regional andino para la mitigación de riesgos http://www.disaster-info.net/PED-Sudamerica/leyes/leyes/suramerica/ecuador/otranorm/PLAN_ESTRATEGICO_REDUCCION_RIESGO.pdf

[13] http://www.cybsec.com/upload/ESPE_IDS_vs_IPS.pdf

[14]http://docsegacy.fortinet.com/fos50hlp/50/index.html#page/FortiOS%25205.0%2520Help/ips_chapter.152.01.html

[15] http://www.seguridadx.com/que-es-un-siem-que-es-prelude-siem/

ANEXOS

GLOSARIO

Firewall: Cortafuegos en español, es una parte de un sistema o de una red que está diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo las comunicaciones autorizadas.

Normas AAA: Son un conjunto de protocolos que realizan tres funciones, autorización, autenticación y auditoria.

IPS: Sistema de prevención de intrusos, es un programa que ejerce el control de acceso en una red informática para proteger los sistemas computacionales de ataques e intromisiones.

SIEM: Información de seguridad y administración de eventos, la tecnología SIEM proporciona un análisis en tiempo real de las alertas de seguridad generadas por el hardware y software de red.

OSSIM: Gestión de seguridad de la información de código abierto, es un conjunto de herramientas diseñadas para ayudar a los administradores de red en la seguridad de las computadoras.

LAN: Red de área local, son un grupo de equipos que pertenecen a la misma organización y se encuentran conectados dentro de un área geográfica pequeña a través de la red, generalmente con la misma tecnología que comúnmente es Ethernet.

Router: Enrutador, es un dispositivo que proporciona conectividad a nivel de red, su función principal consiste en enviar o encaminar paquetes de datos de una red es decir interconectar redes.

Software: Son un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora.

Hardware: Son el conjunto que conforman la parte material o los componentes físicos de una determinada tecnología.

Radius: Protocolo de autenticación que cifra la contraseña proporcionado de la persona que solicita autenticarse.

Tacacs+: Protocolo de autenticación que cifra usuario, contraseña y todos los datos asociados a la autenticación de una persona.

Modelo OSI: Sistema de interconexión abierto, es un modelo de referencia para los protocolos de red y la arquitectura en capas.

DMZ: Zona desmilitarizada, es una zona segura que se ubica entre la red interna de una organización y una externa, generalmente en internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ solo se permitan a la red externa.

Fortigate: Hardware cortafuegos de la empresa Fortinet.

ABREVIATURAS

AAA: Authentication Authorization Accounting, autorización autenticación auditoria.

IPS: Intrusion Prevention System, sistema de prevención de intrusos.

SIEM: Security Information and Event Management,

LAN: Local Area Network, Red de Área Local

WAN: Wide Area Network, Red de Área Extensa

WLAN: Wireless Local Area Network, Red de Área Local Inalámbrica

RAM: Random Access Memory, memoria de acceso aleatorio.

PC: Personal Computer, Computadora personal.

OSI: Open System Interconection, Sistema de Interconexión Abierto

DHCP: Dynamic Host Configuration Protocol, Protocolo de Configuración Dinámica de Host

DNS: Domain Name System, Sistema de Nombres de Dominio

DoS: Denegation of Service**,** Denegación de Servicio

FTP: File Transfer Protocol, Protocolo de transferencia de archivos

HTTP: Hypertext Transfer Protocol, Protocolo de Transferencia de Hipertexto

HTTPS: Hyper Text Transfer Protocol Secure, Protocolo Seguro de Transferencia de Hipertexto

ICMP: Internet Control Message Protocol, Protocolo de Mensajes de Control de Internet

NTP: Network Time Protocol, Protocolo de Tiempo de red

POP3: Post Office Protocol version 3, Protocolo de la Oficina de Correo

RAM: Random-Access Memory, Memoria de Acceso Aleatorio

RTP: Real Time Protocol, Protocolo de Tiempo Real

SMTP: Simple Mail Transfer Protocol, Protocolo Simple de Transferencia de Correo

SSH: Secure Shell, Intérprete de Órdenes Seguras

TCP: Transmission Control Protocol, Protocolo de Control de Transmisión

TELNET: Telecommunication Network, Red de Telecomunicaciones

TLS: Transport Layer Security, Seguridad de la Capa de Transporte

UDP: User Datagram Protocol, Protocolo de Datagrama del Usuario