Universidad de Cienfuegos "Carlos Rafael Rodríguez"

Facultad de Ingeniería

Carrera de Ingeniería Informática

Propuesta de un modelo de diseño de red LAN seguro aplicado a las capas 2, 3 y 7 del modelo OSI, basado en tecnología Huawei y Software Libre.

Trabajo de Diploma para optar por el título de Ingeniería en Informática

Autora:

Arahí Yolanda Conyedo Pérez.

Tutores:

MsC. Karina Leonor Fernández Sánchez.

MsC. Jorge Luis Rivero Pérez.

Cienfuegos,Cuba

Curso 2012-2013

Pensamiento

Debe hacerse en cada momento lo que en cada momento es necesario.

José Martí

Agradecimientos:

A mis compañeros de aula que han compartido conmigo estos cinco años de estudio, en especial a los que han estado siempre luchando junto a mí.

A mi compañera de aula y por demás amiga incondicional Yaleidy Martínez Tapia que ha compartido todos estos momentos de dudas e inestabilidad, por su amistad sincera, por toda su ayuda y comprensión. Por darme ánimo cuando lo necesite para seguir adelante. Por considerarme su amiga todos estos años.

A mi amiga Arianna porque a pesar de estar lejos puedo contar con su apoyo absoluto, por mantenerme presente en su corazón, por siempre estar pendiente de mí y preocupada por mi tesis.

A mi tutora Karina que no tengo palabras como agradecerle todo lo que ha hecho por mí, gracias por su guía, esmero, paciencia y su apoyo incondicional durante todo este tiempo.

A mis padres por quererme, por su presencia en cada momento de mi vida y comprensión, por hacer de mí la persona que soy hoy, por su preocupación constante. Por darme su apoyo. Gracias a los dos por ser esos padres maravillosos de los cuales estoy extraordinariamente orgullosa. Por que son todo lo más importante que tengo y son mi razón de ser.

A mi familia que aunque no es muy grande siempre puedo contar con ellos, por su comprensión y presencia.

A mí querido compañero Julián que me ha demostrado que cuando existe algo verdaderamente grande e importante en la vida todo se puede. Por estar a mi lado en este momento especial y único en mi vida y soportar mis momentos de desesperación.

A todos los que de una manera u otra han contribuido con su apoyo.

Dedicatoria

Dedicado a toda mi familia y amigos, en especial mis padres que se lo merecen por ser mi luz inspiradora, por su amor y por haber luchado siempre conmigo para que este sueño se hiciera realidad, ya que sin su ayuda nunca lo hubiera podido alcanzar.

Resumen:

El desarrollo empresarial constituye una fuente importante de ingresos a la economía de nuestro país. Una alternativa para alcanzar este desarrollo se expone en la implementación de un modelo donde con la utilización de tecnologías alcanzables a nuestro país, se logre una mejor seguridad en las redes.

Muchos de los equipos necesarios para implementar las redes informáticas de las empresas cubanas y de las aplicaciones propietarias que ayudan a complementar un mejor funcionamiento de esta, tenemos que adquirirlos por terceros países, muchas veces de menor calidad y con precios más elevados, por causa del bloqueo económico en contra de nuestro país.

Las empresas cubanas podrían obtener con facilidad equipamiento Huawei y herramientas de seguridad basadas en Software Libre. Aunque existe documentación técnica sobre estos aspectos a tener en cuenta al diseñar las redes informáticas, no aparecen diseños basados solamente en estas tecnologías.

Teniendo en cuenta esta situación se propone implementar un modelo de diseño de red LAN seguro aplicado a las capas 2, 3 y 7 del modelo OSI, basado en tecnología Huawei y Software Libre.

El valor potencial de la investigación radica en sus implicaciones prácticas puesto que con la aplicación de este modelo de diseño se logrará una mayor seguridad en las redes de cualquier empresa con igual característica de la red y por tanto una mayor eficiencia y calidad en los servicios prestados en ella.

Índice

Índice de Figuras

Introducción:

En la economía actual, el desarrollo tecnológico es el que provoca el cambio y la reducción de costos más importante. La informática juega el papel preponderante de este desarrollo. Dentro de la tecnología informática el campo que más ha impulsado a la economía mundial ha sido el de las redes de comunicación y sus usos comerciales.

El amplio entorno en que se aplican las tecnologías de la información, trae consigo la necesidad de intercambiar información entre sistemas cuyas tecnologías son muy diferentes entre sí, lo que llevó a la ISO (International Standard Organization) a buscar la manera de regular dicho intercambio de información. El modelo de referencia OSI (Open Systems Interconnection) surge en el año 1983 y es el resultado del trabajo de la ISO para la estandarización internacional de los protocolos de comunicación.

El modelo OSI es un marco de referencia para la definición de arquitecturas en la interconexión de los sistemas de comunicaciones.[1]

Una normativa formada por siete capas que define las diferentes fases por las que deben pasar los datos para viajar de un dispositivo a otro sobre una red de comunicaciones. Este modelo está dividido en: La capa Física, de enlace de datos, en la capa de Red, de Transporte, de Sesión, de Presentación y de Aplicación.

El contínuo y rápido avance de la informática, también plantea un gran desafío en materia de **seguridad informática** para todos los que forman parte de cualquier actividad o mercado.

Se entiende por seguridad informática al conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información.[2]

Sucede que muchas veces no se es consciente de los riesgos a los que una empresa o entidad está expuesta en materia de seguridad de la información y también se desconocen los altísimos costos que puede tener aparejado no tener una cobertura correcta contra posibles ataques informáticos.

Este desarrollo de la informática es posible por la unión de los ordenadores en entornos de red.

Una red de computadoras, también llamada red de ordenadores o red informática, es un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten Información (archivos), recursos (CD-ROM, impresoras, etc.), servicios (acceso a internet, E-mail, chat, juegos), etc. [3]

La planificación de la seguridad en el diseño de la red es de suma importancia pues de esto depende el buen desempeño de ésta, evitando trabajo posterior, pérdida de datos y posibles daños a la red. En ocasiones se considera el tema de seguridad fuera de tiempo lo cual trae consecuencias de gastos excesivos y posibles pérdidas de información.[4]

Las redes de computadoras deben diseñarse para entornos específicos, donde es fundamental tener la configuración correcta en los equipos de escritorio, pero aun más importante son los dispositivos de red, Switch, Router, Access Point, dado que estos nos proveen de la conectividad y el enlace hacia el resto del mundo.

Estos dispositivos de red sin la configuración correcta y adecuada no tan solo pueden darnos problemas de conexión, además vulnerabilidad en la red, permitiendo que agentes externos ingresen a esta, logrando ver, modificar e incluso eliminar archivos.

Por este motivo, es importante no descuidar la seguridad de los datos corporativos. Frecuentemente se invierte en alarmas, seguros, vigilancia, etc… pero se escatima en gastos a la hora de proteger los datos.

Las Tecnologías de la Información y la Comunicación (TIC) se han convertido, desde su llegada a los escenarios nacionales, en un elemento indispensable para establecer las líneas de desarrollo de la sociedad cubana.[5]

Pero al igual que en otras esferas también ha sido afectada por la aplicación de las injustas medidas, donde se incluyen las restricciones impuestas al acceso de Cuba a Internet.

La ejecución de cada proyecto incluye la compra de equipamiento

imprescindible como servidores, conectores, conmutadores de redes, cables, computadoras. Cada uno de ellos tenemos que adquirirlo en el otro lado del mundo, muchas veces de menor calidad y con precios más elevados.[5]

La confección de la red está dada por múltiples componentes y en su fabricación entra a jugar un papel importante los diferentes proveedores que existen, entre ellos podemos encontrar a Huawei que se convirtió en 2010 en el segundo del sector en el mundo, tras la europea Ericsson, por sus resultados financieros.[6]

En total, mantiene acuerdos de cooperación con 45 de las 50 mayores operadoras de telecomunicaciones del Mundo.

China es para Cuba un socio estratégico en el campo de la informática y las telecomunicaciones, así como el mayor proveedor de bienes de capital y consumo de la mayor de las Antillas. Más de 200 empresas chinas tienen relaciones comerciales con Cuba, y más de 20 empresas y organismos de la isla caribeña están acreditados en el país asiático.[7]

Huawei ofrece productos de calidad, que permiten implementar medidas de seguridad a tener en cuenta al diseñar redes informáticas. En nuestro país podemos adquirir switchs Huawei de varios modelos, entre los que podemos mencionar los *Quidway S3300* y *S5300.* Este equipamiento permite definir diferentes mecanismos de seguridad a nivel de las capas 2 y 3 del modelo OSI, temas que serán abordados en este trabajo.

El bloqueo económico, comercial y financiero de Estados Unidos contra Cuba, reiteradamente condenado por la mayoría abrumadora de los países miembros de la ONU y por organizaciones, instituciones y personalidades de reconocido prestigio internacional, obstaculiza seriamente nuestro acceso a las tecnologías de la información y las comunicaciones.

Las leyes estadounidenses prohíben exportar o reexportar a determinados países, entre los que figura Cuba, productos de Software de empresas norteamericanas.

Por este motivo, Cuba se ve obligada también a comprar las licencias de Software, sus actualizaciones y la transferencia de tecnología a través de

terceros países.[8]

Esto hace más costoso y difícil nuestro trabajo. Además muchas de las aplicaciones y herramientas importantes todavía están basadas en Software propietario.

Cuba responde potenciando desde el 2005 la migración al Software Libre en aras de alcanzar la soberanía tecnológica y la seguridad del país.

Existen múltiples herramientas de Software Libre para la seguridad de redes, imprescindibles a tener en cuenta en las redes cubanas. Al utilizarlas se atiende a la necesidad del país de migrar a dichas tecnologías y proteger la información de las empresas cubanas.

A nivel internacional son muchas las tecnologías de Software Libre que se utilizan según el ambiente de trabajo. Para implementar mecanismos de seguridad a nivel de la capa de aplicaciones del modelo OSI, se encuentra Open Source Security Information Management por sus siglas (OSSIM).

Qué es una colección de herramientas diseñadas para ayudar a los administradores de red en la seguridad de su centro de datos, detección de intrusos y prevención.[9]

Las empresas cubanas para implementar sus redes informáticas podrían adquirir con facilidad equipamiento Huawei y herramientas de seguridad basadas en Software Libre. Aunque existe documentación técnica sobre estos aspectos a tener en cuenta al diseñar las redes informáticas, no aparecen diseños basados exclusivamente en estas tecnologías.

Ante toda esta situación, se define como **problema a resolver** lo siguiente:

¿Se podrá definir un modelo de diseño de red LAN seguro que cubra las capas 2, 3 y 7 del modelo OSI, basado en tecnología Huawei y Software Libre?

Como **objeto de estudio** de la presente investigación se tiene la seguridad en diseño de redes en las capas 2, 3 y 7 del modelo OSI. El **campo de acción** es la seguridad en el diseño de redes basado en tecnología Huawei y OSSIM.

Como **idea a defender** se plantea que:

Con un modelo de diseño de red LAN seguro, aplicado a las capas 2, 3 y 7 del modelo OSI, usando tecnología Huawei y Software Libre, se logrará una mejor seguridad en las redes de las empresas cubanas que lo implementen.

Como **Objetivo General** se plantea: Elaborar una propuesta de un modelo de diseño de red LAN seguro, aplicado a las capas 2, 3 y 7 del modelo OSI, basado en tecnología Huawei y Software Libre.

Del mismo se derivan los siguientes **Objetivos Específicos**:

- Analizar el estado actual de los diseños de seguridad para redes LAN.
- Definir un modelo de diseño de red LAN seguro basado en tecnología Huawei y Software Libre aplicado a las capas 2 y 3 del modelo OSI.
- Complementar el diseño de red LAN con tecnologías de Software Libre a nivel de la capa 7 del modelo OSI.
- Validar el modelo de diseño propuesto en un escenario que lo implemente.

Para lograr esta investigación se desarrollarán las siguientes **Tareas Científicas:**

1. Estudio del estado del arte de los diseños de seguridad para redes LAN.
2. Recopilación del conocimiento y sugerencias a través de entrevistas y la literatura científico-técnica sobre el dominio que se aborda.
3. Revisión de las principales prácticas a tener en cuenta en un diseño de seguridad para redes LAN.
4. Aplicación de las prácticas estudiada en el diseño de seguridad.
5. Validación del modelo de diseño propuesto utilizando la herramienta Nessus en un escenario que lo implemente.

Para lograr una mejor comprensión de la presente investigación el documento quedó estructurado de la siguiente forma:

Capítulo 1: "*Marco teórico de los diseños de seguridad para redes LAN".*

En este capítulo se exponen aspectos teóricos del tema en análisis. Se incluyen los resultados del estudio de los equipos a utilizar en el modelo de diseño, así como el análisis de la herramienta de Software Libre que se propone utilizar para ayudar en la seguridad de las redes informáticas.

Capítulo 2: "*Diseño de seguridad para Redes LAN utilizando switch Huawei S5300 y OSSIM".*

En este capítulo se describirá la propuesta de la solución, mostrando como se pudieran definir las VLANs, proponiendo la utilización del IDS de OSSIM, que es el Snort y la implementación de un cortafuego perimetral que en este diseño utiliza las potencialidades del Switch Quidway 5300. Además para lograr con efectividad la propuesta se expondrán los comandos a realizar en los Switches Quidway 5300 y 3300. Se realizará un mejor análisis de los componentes, que se emplean en el diseño, de la herramienta OSSIM.

Capítulo 3: "*Validación del Diseño propuesto".*

Se describirá el escenario de prueba, una red LAN real que implementó el modelo propuesto. Además la validación de la propuesta mediante la exposición de los resultados de la herramienta antes y después de implementar el modelo. Describiendo como se comporta ante agresiones a partir de un estudio de vulnerabilidades con la herramienta Nessus.

Capítulo 1:"Marco teórico de los diseños de seguridad para redes LAN"

En el presente capítulo se exponen aspectos teóricos del tema en análisis. Se presentan algunas características del equipamiento que se entiende utilizar en el diseño propuesto. Además se realiza un análisis de la herramienta OSSIM, como una de las tecnologías de Software Libre para garantizar la seguridad en la red.

1.1 Introducción

Hoy en día las redes informáticas se utilizan en abundancia para interconectar recursos entre diferentes computadoras a través de un medio. Estos recursos, pueden ser tanto de Hardware como de Software. Estas redes informáticas pueden ser cableadas o inalámbricas.

Una red puede recibir distintos tipos de clasificación dependiendo de su estructura o forma de transmisión: alcance, tipo de conexión, por topología, etc. Basada en el alcance se encuentra, entre otras, las Redes de Área Local (LAN) por su traducción (Local Área Network).

Que son un grupo de equipos que pertenecen a la misma organización y están conectados dentro de un área geográfica pequeña a través de una red, generalmente con la misma tecnología.[10]

Estas redes son usadas para la interconexión de computadores personales y estaciones de trabajo. Se caracterizan por: tamaño restringido, tecnología de transmisión (por lo general multidifusión), alta velocidad y topología. Son redes con velocidades entre 10, 100, 1000 Mbps, tiene baja latencia y baja tasa de errores. [11]

El término red local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.

Básicamente, la comunicación dentro de una red informática es un proceso en el que existen dos roles bien definidos para los dispositivos conectados, emisor

y receptor, que se van asumiendo y alternando en distintos instantes de tiempo.[12]

También hay mensajes, que es lo que estos roles intercambian. La estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más extendido de todos, el modelo OSI.

1.2 Modelo OSI

Durante las últimas dos décadas ha habido un enorme crecimiento en la cantidad y tamaño de las redes. Muchas de ellas sin embargo, se desarrollaron utilizando implementaciones de hardware y software diferentes. Como resultado, muchas de las redes eran incompatibles y se volvió muy difícil para las redes que utilizaban especificaciones distintas poder comunicarse entre sí. Para solucionar este problema, la ISO realizó varias investigaciones acerca de los esquemas de red. Esta reconoció que era necesario crear un modelo de red que pudiera ayudar a los diseñadores de red a implementar redes que pudieran comunicarse y trabajar en conjunto y por lo tanto, elaboraron el modelo de referencia OSI. [13]

Figura 1: La Pila OSI.

El Modelo OSI, como se muestra en la figura, divide en 7 capas el proceso de

transmisión de la información entre equipo informáticos, donde cada capa se encarga de ejecutar una determinada parte del proceso global. Estas capas son:

1 – Capa Física: se encarga de las conexiones físicas de la red. Define los medios físicos por los cuales viajarán los datos, las características materiales y eléctricas que se usan en la transmisión de datos, características funcionales de la interfaz, transmisión del flujo de bits en el medio, maneja las señales eléctricas, garantiza la conexión, etc.

2 – Capa de Enlace de Datos: se encarga del direccionamiento físico de la red. Del acceso al medio, de la detección de errores, de la distribución ordenada de tramas y del control de flujo.

3 – Capa de Red: el objetivo de la capa de red es hacer que los datos lleguen desde el origen al destino, aún cuando ambos no estén conectados directamente. En este nivel se realiza el direccionamiento lógico y la determinación de la ruta de los datos hasta su receptor final.

4 – Capa de Transporte: se encarga de efectuar el transporte de los datos desde la máquina origen a la de destino, independizándolo del tipo de red física que se esté utilizando.

5 – Capa de Sesión: esta capa es la que se encarga de mantener y controlar el enlace establecido entre dos computadores que están transmitiendo datos de cualquier índole. Debe ser capaz de que la conexión establecida se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción.

6 – Capa de Presentación: el objetivo es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres los datos lleguen de manera reconocible.

7 – Capa de Aplicación: ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico, gestores de bases de datos y servidor de ficheros, etc. [13]

1.3 Papel de la Seguridad Informática en las Redes de computadoras.

La Seguridad Informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información. [14]

En Cuba los avances alcanzados en los últimos años en la informatización de la sociedad, a partir del incremento de tecnologías de la información en todos los sectores y en particular de las redes informáticas y sus servicios asociados, y el impulso orientado por la dirección del país al desarrollo acelerado de programas que multipliquen dichos logros, han impulsado la adopción de medidas que garantizan un adecuado nivel de seguridad, de protección y de ordenamiento. [15]

En nuestro país la seguridad de las organizaciones, sistemas y redes de información están constantemente amenazadas por diversas fuentes que incluyen ataques de distintos tipo y origen; la ocurrencia de catástrofes, errores de operación y negligencias, aumentan los riesgos a que están expuestos los servicios y protocolos utilizados, así como el contenido de la información tratada en dichos sistemas, todo lo cual afecta severamente la confidencialidad, integridad y disponibilidad de la información. [15]

La **seguridad informática** es el área de la informática que tiene como función proteger la infraestructura y los datos contenidos en esta.[16]

1.4 Diseños de redes LAN.

Para que una LAN sea efectiva y satisfaga las necesidades de los usuarios, se debe diseñar e implementar de acuerdo con una serie planificada de pasos sistemáticos. En esta sección se describen los siguientes pasos:

- Obtención de los requisitos y expectativas de los usuarios.

- Análisis de los requisitos.
- Diseño de la estructura LAN en las Capas 1, 2 y 3 (topología).
- Documentación de la implementación lógica y física de la red.[17]

1.4.1 Obtención de los requisitos y expectativa de los usuarios

El primer paso del diseño de una red es la obtención de los datos sobre la estructura de la organización, se puede incluir información sobre la historia y el estado actual de la empresa, el crecimiento previsto, las normas de funcionamiento, los procedimientos administrativos, los procedimientos y sistemas de oficina y sobre todo los puntos de vista de las personas que utilizarán la red, así como las necesidades de todos los usuarios que estén o no involucrados con el funcionamiento de la LAN.

El proceso de obtención de información ayudará a identificar los problemas que tiene la empresa. Se debe identificar los datos y operaciones críticos, ya que estos son considerados como información clave y el acceso a ellos es crítico en el desarrollo diario de la misma.

1.4.2 Análisis de los requisitos.

El siguiente paso en el diseño de una red consiste en analizar los requisitos de la red y de sus usuarios obtenidos en el paso anterior, se debe considerar que las necesidades de los usuarios van cambiando continuamente ya que el avance de la tecnología crece en forma exponencial.

La evaluación de los requisitos de los usuarios es un componente muy importante en la fase de diseño ya que una LAN que no ofrece a sus usuarios información puntual y precisa es de poca utilidad, por tanto es indispensable asegurarse de conocer todos los requisitos y necesidades de la empresa y sus trabajadores para evitar diseñar redes obsoletas.

1.4.3 Diseño de la estructura LAN en las capas 1,2 y 3 (topología).

1.4.3.1 Diseño de la Topología física de la red

Una vez que tenemos los requisitos globales de la red, el siguiente paso es decidir la topología general de la red, la misma que debe satisfacer los requisitos de los usuarios.

Considerando las topologías que más se usan en el mercado nos centraremos en dos topologías: Topología en Estrella y Topología en Estrella extendida.

Las partes más importantes del diseño de una topología LAN pueden dividirse en tres categorías únicas del modelo de referencia OSI: la capa de red, la capa de enlace de datos y la capa física.

1.4.3.2 Diseño de Capa 1

En este punto se examinará las topologías en estrella y estrella extendida de la capa.

1. Se analizará los componentes más importantes que se deben considerar al diseñar una red como son:
El cableado físico: se debe analizar el tipo de cableado a utilizar (UTP, cobre o Fibra óptica) y la estructura global del cableado. Si se esta diseñando una red nueva o recableado una existente se debe utilizar cable de Fibra Óptica en el Backbone y como mínimo cable UTP categoría 5 en los tendidos horizontales. Se debe considerar las normas más recientes sobre UTP de categoría 5e y 6.
Se debe tomar en cuenta el tiempo de vida para el cual se diseña la red y según esto elegir la calidad del cable. Además de esto las empresas deben garantizar que los sistemas están conforme a las normas industriales definidas, como las especificaciones TIA/EIA-568-B (norma de cableado).
La norma TIA/EIA-568-B específica que cada dispositivo conectado a una red debe estar enlazado a una ubicación central mediante cableado horizontal
Para la identificación de los MDF e IDF se debe determinar cuantos recintos de cableado se va ha necesitar; se requiere más de uno cuando las grandes redes se encuentran fuera del límite de los 100 metros del UTP de categoría 5. Al haber varios recintos se crean varias áreas de captación.

Los MDF incluyen uno o más patch panels HCC (conexión cruzada horizontal)
Los recintos de cableado principal se conocen como MDF y los secundarios como IDF, la conexión de los IDFs al MDF es mediante cableado vertical denominado cableado Backbone.
Y para interconectar los IDF externos con el MDF utiliza una conexión cruzada vertical (VCC) y como normalmente la longitud de los cables verticales supera los 100m de UTP de categoría 5, se utiliza fibra óptica.
La norma Fast Ethernet tiene diferentes normas basadas en el hilo de pares de cobre (100BASE-TX) y en cable de fibra óptica (100BASE-FX) y se utilizan para conectar el MDF al IDF.
Ethernet conmutada 10BASE-TX Ethernet de escritorio y los backbone Fast Ethernet son probablemente muy adecuadas para los requisitos de ancho de banda de muchas redes. Pero las redes más nuevas podrían optar por Gigabit Ethernet con fibra para el cableado vertical y por Fast Ethernet con categoría 5e en los enlaces horizontales.
Los elementos del diagrama lógico incluyen:

- Las localizaciones exactas de los recintos de cableado MDF e IDF.
- El tipo y la cantidad de cableado utilizado para interconectar los IDFs con el MDF.

- La documentación detallada de todos los tendidos de cable, los números de identificación y en que puerto de la HCC termina el tendido.

1.4.3.3 Diseño de la capa 2

Entre los dispositivos de la capa 2 se tiene al Switch LAN, estos dispositivos determinan el tamaño de los dominios de colisión y de difusión. En este punto se verá la implementación de la conmutación LAN en capa 2.

Con la Conmutación LAN se puede microsegmentar la red, eliminando las colisiones y reduciendo el tamaño de los dominios de colisión.
La microsegmentación significa utilizar switches para mejorar el rendimiento de un grupo de trabajo o de un backbone.

Entre las características importantes del Switch LAN tenemos la conmutación asimétrica es decir que puede asignar ancho de banda sobre una base por puerto que permite así más ancho de banda para el cableado vertical, los enlaces ascendentes y los servidores. Además la conmutación asimétrica permite conexiones conmutadas entre puertos de distinto ancho de banda, por ejemplo una combinación de puertos a 10 Mbps y a 100 Mbps o una combinación de 100 Mbps y a 1000 Mbps.

Si se instala conmutación LAN en el MDF y los IDF, y el cableado vertical entre el MDF y los IDF, el cableado vertical transportará todo el tráfico de datos entre el MDF y los IDF y al ser cableado backbone tendrá mayor capacidad que la de los tendidos entre los IDF y las estaciones de trabajo.

En los tendidos de cableado horizontal se utiliza UTP de categoría 5 o superior, teniendo en cuenta que ninguna derivación de cable debe superar los 100 metros, que permiten enlaces a 10, 100 o 1000 Mbps.

Al permitir los switch LAN asimétricos mezclar en un solo switch puertos a 10 Mbps y 100 Mbps o puertos a 100 Mbps y 1000Mbps, se debe determinar el número de puertos a 10Mbps, 100Mbps y a 1000 Mbps necesarios en el MDF y en cada IDF.

La determinación del número de puertos de Switch LAN dependerá de los requisitos de los usuarios, los mismos que serán referentes al número de derivaciones de cable horizontal por sala y al número de derivaciones en cualquier área de captación, junto con el número de tendidos de cable vertical.

Número de un Dominio de Colisión

Para determinar el número de un dominio de Colisión se debe determinar el número de hosts conectados físicamente a cualquier puerto de un switch.

Otra forma de implementar la conmutación LAN es instalar hubs LAN compartidos en los puertos del switch y conectar varios hosts a un solo puerto del switch.

Los hubs de medio compartido se utilizan normalmente en un entorno de switch

LAN para crear más punto de conexión final de los tendidos de cable horizontal, esta es una solución aceptable siempre que se asegure que los número de colisión sean pequeños y que los requisitos de ancho de banda al host se cumplan de acuerdo a los requerimientos obtenidos en la fase de obtención de información del proceso de diseño de la red.

Dispositivos de capa 2

Los hubs, algunos switches y los puentes están clasificados como dispositivos de capa 2 en el modelo OSI.

La segmentación es una técnica que ayuda a garantizar que no se degrade el rendimiento de una red al crecer.

Los usuarios se impacientan cuando una aplicación no se ejecuta rápidamente, y una de las formas más eficaces de solucionar este problema de la congestión es dividir la red en segmentos más pequeños, y esto lo pueden hacer los segmentos físicamente, utilizando un puente o un switch para limitar el número de dispositivos en el segmento de red.

Switch: concentra la conectividad, mientras consigue que la transmisión de datos sea más eficaz.

Hub Ethernet: todos los puertos se conectan a un plano trasero común o conexión física dentro del hub, y todos los dispositivos que están conectados al hub comparten el ancho de banda de la red.

Para conmutar tramas de forma eficaz entre las interfaces, el switch mantiene una tabla de direcciones y cuando una trama entra en el switch, éste asocia la dirección MAC de la estación emisora (origen) con la interfaz que la recibió.

Las principales funciones de los Switches Ethernet son:

1. Asistir el tráfico entre segmentos
2. Conseguir más ancho de banda por usuario creando números de colisión más pequeños.

Los switches Ethernet filtran el tráfico direccionando los datagramas hacia el puerto correcto basándose en las direcciones MAC de capa 2. La segunda función de un switch es garantizar que cada usuario tiene más ancho de banda

mediante la creación de números de colisión más pequeños.
Un Switch Fast Ethernet permite la segmentación de una LAN, dotando a cada segmento de un enlace de red dedicado de hasta 1000 Mbps. Con frecuencia en las redes actuales los switch Fast Ethernet o Giga Ethernet actúan como Backbone de la LAN.

En la actualidad las empresas se encuentra en constante crecimiento, y a medida que la red crece, la necesidad de ancho de banda también. En el cableado vertical entre el MDF y los IDF, las fibras ópticas no utilizadas se pueden conectar desde la VCC hasta los puertos a 100 Mbps del switch.

1.4.3.4 Diseño de la capa 3

Los routers son dispositivos de capa 3 (capa de red) se pueden utilizar para crear segmentos LAN únicos y permitir la comunicación entre segmentos basándose en el direccionamiento de la capa 3, como el direccionamiento IP. La implementación de estos dispositivos permite la segmentación de la LAN en redes físicas y lógicas únicas.

Los routers también se utilizan para la conexión con redes de área amplia (WAN) como Internet.
El router determina el flujo de tráfico entre los segmentos de red físicos únicos basándose en el direccionamiento de la capa 3, como la red y la subred IP. El router reenvía paquetes de datos basándose en las direcciones de destino, por lo que es considerado el punto de entrada y de salida de un dominio de difusión e impide que las difusiones alcancen otros segmentos de la LAN.
Conocer el número total de difusiones, como las peticiones de ARP (protocolo de resolución de direcciones) es muy importante en la red y mediante VLAN (LAN Virtuales) se puede limitar el tráfico de difusión al interior de una red y crear dominios de difusión más pequeños. Las VLAN se pueden utilizar también para proporcionar seguridad a la red al crear grupos VLAN según su función.
Una de las características de los routers es que proporcionan escalabilidad por que pueden servir como Firewall para las difusiones. Considerando que las

direcciones de capa 3 normalmente tienen estructura, los routers pueden ofrecer mayor escalabilidad dividiendo las redes y subredes, añadiendo así estructura a dichas direcciones.

Una vez que las redes se han dividido en subredes, se debe desarrollar y documentar el esquema de direccionamiento IP que se utilizará en la red.

El direccionamiento y el enrutamiento del protocolo de red proporcionan escalabilidad integrada.

Cuando se está decidiendo en utilizar routers o switch se debe considerar cual es el problema que se espera solucionar con la implementación de uno de ellos. Así si el problema está relacionado con el protocolo y no con la contención lo más adecuado son los routers.

Características de los Routers.- Estos dispositivos solucionan problemas relacionados con:

- Difusiones excesivas
- Los protocolos que no escalan bien
- Se pueden utilizar para crear subredes IP a fin de añadir estructura a las direcciones
- Temas de seguridad y
- El direccionamiento de la capa de red.

Sin embargo se debe considerar que son más caros y difíciles de configurar.[18]

1.4.4 Documentación de la implementación lógica y física de la red.

La documentación de diseño LAN es la siguiente:

- Mapa de topología de capa OSI.
- Mapa lógico de LAN.
- Mapa físico de la LAN.
- Planes de distribución.
- Mapa lógico de VLAN.
- Mapa lógico de Capa 3.
- Mapas de dirección. [17]

1.5 Equipamiento Huawei a utilizar en el diseño propuesto: Switches Quidway S5300 y Switches Quidway S3300.

En Cuba se puede adquirir variados equipos producidos por Huawei, en el diseño propuesto se utilizarán los switchs Quidway S5300 y S3300. A continuación se expondrán las características de ambos.

1.5.1 Quidway ® S3300 Series Switches

Los switches de la serie Quidway S3300 son la nueva generación de switches Ethernet desarrollado para llevar a diversos servicios en Ethernet, que ofrecen potentes funciones de Ethernet para operadores y clientes empresariales. Sobre la base de la nueva generación de hardware de alto rendimiento y Huawei versátil plataforma de enrutamiento (VRP), el S3300 ofrece la función mejorada selectivo QinQ y capacidad para replicar los paquetes multicast entre las VLAN a la velocidad de la línea, y es compatible con tecnologías de clase portadora de confiabilidad.

El S3300 se puede utilizar como dispositivos de acceso en edificios o aplicado a la capa de acceso y la capa de agregación de redes de campus. El S3300 es fácil de instalar. Es compatible con la configuración automática y plug-and-play, lo que reduce drásticamente los costes de despliegue de red.

El S3300 es un dispositivo en forma de caja con un chasis de 1 U de altura, siempre en versión estándar (SI), una versión mejorada (EI), y una versión avanzada (HI). SI soporta funciones de la Capa-2 y funciones básica de Capa 3. IE apoya los complejos protocolos de enrutamiento y características abundantes. HI soporta mayor especificación de las direcciones MAC, rutas y multicast en las entradas de la tabla, y las capacidades de hardware más potente.

Seguridad y calidad de servicio

El S3300 ofrece diversas medidas de protección de seguridad. Se puede

defender contra denegación de servicio (DoS), los ataques a las redes y los ataques a los usuarios. Los ataques DoS son ataques SYN Flood, ataques terrestres, ataques smurf, y los ataques de inundación ICMP. Los ataques a las redes se refieren a STP BPDU / ataques de root. En los ataques a los usuarios se incluye falsa del servidor de ataques DHCP, ataques *Hombre en el medio*, IP / MAC engañando ataques, ataques de pedidos DHCP inundación y DoS ataques cambiando el campo CHADDR de paquetes.

El S3300 escucha a la dirección MAC / IP, concesión de dirección, ID de VLAN, y el número de puerto de un usuario por DHCP estableciendo y manteniendo una tabla de inspección DHCP en unión. De esta forma, las direcciones IP y los puertos de acceso de DHCP de los usuarios, pueden ser rastreados. El S3300 directamente descarta paquetes inválidos que no coinciden con las entradas de unión, tales como ARP, suplantación de paquetes y paquetes con direcciones IP falsas, para evitar que los hackers o atacantes de iniciar man-in- el medio de ataque a redes de campus mediante el uso de paquetes ARP. La función de puerto de confianza de engaño del DHCP se utiliza para asegurar la validez del servidor DHCP.

El S3300 soporta en estricto ARP para que aprenda a evitar que los atacantes ARP de engaño agoten las entradas ARP para que los usuarios autorizados puedan conectarse a Internet. También es compatible con IP de origen de verificación para evitar los ataques de denegación de servicio causadas por MAC direcciones de engaño, falsificación de direcciones IP y MAC / IP engaño de direcciones. La función proporcionada por el URPF S3300 puede ver las formas de transmisión de datos para autenticar los paquetes recibidos, que puede proteger la red contra la propagación de ataques de suplantación de direcciones de origen.

El S3300 soporta autenticación centralizada de direcciones MAC y autenticación 802.1x. Información del usuario como la cuenta de usuario, dirección IP, dirección MAC, VLAN ID, número de acceso al puerto, y una bandera que indica si antivirus software está instalado en el cliente se puede enlazar estáticamente

o dinámicamente, y las políticas de usuario (VLAN, QoS, y ACL) se puede enviar de forma dinámica.

El S3300 puede limitar el número de direcciones MAC de origen obtenido en un puerto para evitar que los atacantes puedan agotar entradas de direcciones MAC mediante el uso de falsas direcciones MAC de origen. De esta manera, las direcciones MAC de los usuarios autorizados pueden ser aprendidas y las inundaciones se previenen.

El S3300 puede implementar clasificación de tráfico complejo basado en la siguiente información, la prioridad IP, TOS, DSCP tipo, protocolo IP, tipo ICMP, TCP de origen el número de puerto, VLAN ID, trama Ethernet tipo de protocolo, y CoS. El S3300 soporta ACLs entrantes y salientes. El S3300 soporta, basado en el flujo de doble tasa de tres colores, CAR. Cada puerto soporta ocho colas de prioridad, mecanismo WRED congestión prevención y la cola múltiple de algoritmos de programación tales como WRR, DRR, SP, SP + WRR, y RRD + SP. Esto asegura la calidad de voz, vídeo y Servicios de datos.

Considerado sin mantenimiento y de administración

El S3300 adopta un único diseño libre de mantenimiento y soporta la configuración automática (auto-config), liberando a los administradores de la red de carga de trabajo pesada en la configuración al implementar un lote de sitios.

El S3300 soporta BFD y proporciona milésima de segundo en su nivel de detección para protocolos como OSPF, IS-IS, VRRP, PIM y para mejorar la confiabilidad de la red. Cumpliendo con el estándar IEEE 802.3ah y 802.1ag, el S3300 soporta punto a punto Ethernet de administración de fallos para detectar fallos en los enlaces de los usuarios. Ethernet OAM mejora la gestión de la red y capacidades de mantenimiento de la Ethernet y garantiza una red estable. El S3300 soporta las estadísticas de tráfico basadas en puertos, VLAN y NQA, que permite a los administradores de red mejorar la gestión de las redes.

El S3300 soporta el Protocolo de registro GARP (GVRP). La tecnología GVRP

implementa dinámica en la configuración de las VLAN. En un entorno de red complejo, GVRP puede simplificar la configuración de VLAN y reducir fallas en la red de comunicación causados por la configuración incorrecta de la VLAN. Esto reduce el manual configuraciones de los administradores de red y asegura la correcta configuración de VLAN. [19]

1.5.2 Switches Quidway S5300

Los Switches Quidway S5300 serie de nueva generación son desarrollados por Huawei para cumplir con los requisitos de acceso de banda ancha y la convergencia de múltiples servicios Ethernet, ofreciendo funciones de gran alcance para operadores y clientes empresariales.

Basados en la nueva generación de hardware de alto rendimiento y la versátil plataforma de enrutamiento (VRP) de Huawei, el S5300 cuenta con gran capacidad e interfaces Gigabit de alta densidad, ofreciendo enlaces ascendentes a 10G y satisfaciendo las necesidades de los clientes con dispositivos de subida de alta densidad (1G y 10G).

Servicio de Soporte de gran alcance

El S5300 ofrece la mejor función del selectivo QinQ para añadir etiquetas VLAN a los paquetes, sin ocupar recursos de ACL. Además, el S5300 puede marcar de forma flexible las clases de QoS de diferentes servicios para llevar varios de los mismos.

Alta confiabilidad

Además de los tradicionales STP, RSTP y MSTP, el S5300 soporta la función de tecnologías Ethernet, tales como Smart Link y RRPP, además, implementa niveles de conmutación de protección para los enlaces, y asegura la calidad de la red. Smart Link y RRPP apoyan múltiples instancias para implementar el equilibrio de carga entre los enlaces, además de mejorar el uso de ancho de banda.

Políticas de calidad de servicio y perfecto mecanismo de seguridad

El S5300 ofrece múltiples medidas para proteger la seguridad de la información. Se puede defender contra los ataques DoS, ataques a las redes, y los ataques a los usuarios.

Fácil Administración

El S5300 soporta GVRP, que asigna dinámicamente, registra y propaga atributos de VLAN para reducir la carga de trabajo del administrador de red y garantizar la correcta configuración de VLAN's.

El S5300 soporta MUX VLAN. La función MUX VLAN se utiliza para aislar tráfico de nivel 2 entre las interfaces de una VLAN. MUX VLAN se aplica generalmente a la empresa dentro de la redes. Con esta función, una interfaz de usuario se puede comunicar con una interfaz de servidor pero no pueden comunicarse con otras interfaces de usuario. MUX VLAN impide la comunicación entre los dispositivos de red conectados a algunas interfaces o grupos de interfaz, pero permite que estos dispositivos puedan comunicarse con la pasarela por defecto.[19]

1.5.3 Vulnerabilidad de Cifrado débil en productos Huawei.

Se ha descubierto que cifra las contraseñas de sus productos de una manera muy débil.

Hay diferentes maneras de almacenar las contraseñas por parte de los dispositivos y sistemas. Una de las más comunes es utilizar un hast de la contraseña. En el momento de verificar si un usuario es quien dice ser, a la contraseña introducida se le aplica la misma función hash que se usa a la hora de almacenar la contraseña. Si la cadena resultante es igual a la cadena almacenada, se valida. Con este sistema no se guarda la contraseña en claro en ningún momento.

También es común usar "sal", para generar estos hashes. Así, una de las entradas de la función hash sería la clave y otra la "sal", (que solo se trata de

ciertos bit aleatorios). Con esto se consigue mitigar la eficacia de los ataques por diccionario.

Huawei no utiliza ninguno de estos métodos.

El problema descubierto es los dispositivos de Huawei es que usan un cifrado simétrico (algoritmo DES) con una misma clave de cifrado compartida entre todos los dispositivos (´\x01\x02\x03\x04\x05\x06\x07\x08´).

No se trata como de una vulnerabilidad, sino de un fallo de diseño por parte del fabricante por usar contraseñas comunes y no aleatorias para cada dispositivo.

El error ha sido confirmado por la familia Quidway y en los CX600 (router y switches), aunque puede existir en más productos afectados.

La empresa ha publicado un comunicado oficial, donde se recomienda:

- Limitar el acceso a los routers a los usuarios dentro de la red interna.
- Gestionar estrictamente los privilegios de las cuentas.
- Cambiar las contraseñas con regularidad.[20]

1.6 OSSIM una opción de Software Libre para la seguridad de redes.

El Software Libre, es aquel que una vez obtenido, puede ser usado, copiado, estudiado, modificado y redistribuido libremente. El Software Libre suele estar disponible gratuitamente, pero no hay que asociar Software Libre a software gratuito, o a precio del coste de la distribución a través de otros medios; sin embargo no es obligatorio que sea así y, aunque conserve su carácter de libre, puede ser vendido comercialmente. [21]

Análogamente, el "software gratis" o "gratuito" incluye en ocasiones el código fuente; no obstante, este tipo de software no es libre en el mismo sentido que el Software Libre, a menos que se garanticen los derechos de modificación y redistribución de dichas versiones modificadas del programa.[22]

El Software Libre ha ido ganando espacio en las empresas e instituciones impulsado en buena parte por ser una tecnología que permite ahorrar recursos en el pago de licencias, un ejemplo claro de esto es el OSSIM, que es un conjunto de herramientas creadas para facilitar el trabajo de los administradores de Red a la hora de controlar la Seguridad de una Red.

No se trata de una sola aplicación sino de un conjunto de módulos que permiten detectar anomalías o incidencias de seguridad en la Red, análisis forense, análisis de vulnerabilidades, detección de intrusiones, etc.

Su objetivo es el proporcionar una compilación comprensiva de los instrumentos que, trabajando juntos, conceden a un administrador de red/seguridad una vista detallada sobre todo y cada aspecto de sus dispositivos, servidores de acceso de redes, etc.[23]

Este proyecto consiste en una consola de seguridad central, que permite gestionar y saber el nivel de seguridad (métrica) que tiene nuestra empresa. Se trata de un proyecto Open Source, con lo que todo el mundo puede disfrutar de él sin ningún coste, además de poder colaborar en su código para formar parte de su evolución.[24]

OSSIM engloba más de 22 herramientas de seguridad. Además no sólo consigue englobar estas herramientas, sino que la fuerza real de OSSIM reside en su motor de correlación, gracias al cual podemos tener una red o varias con millones de alertas de diferentes dispositivos y mediante su potente motor disponer de alarmas reales, sin falsos positivos y de manera centralizada. [24]

Además de proveer de lo mejor de las herramientas más conocidas de código abierto, algunos de las cuales mencionamos debajo de estas líneas, OSSIM proporciona una correlación de las interfaces de visualización y herramientas de gestión de incidentes que facilitan la presentación de informes, trabajando con un conjunto de activos que se define como anfitriones, redes, grupos y servicios.

OSSIM contiene los siguientes componentes de software:

- Arpwatch, utilizados para la detección de anomalías en MAC.
- P0f, utilizadas para la detección de sistemas operativos y análisis de cambios.
- Pads, utilizado para el servicio de detección de anomalías.
- Nessus, utilizada para la evaluación de la vulnerabilidad y de correlación cruzada (IDS vs Security Scanner).
- Snort, IDS, utilizados para cruzar la correlación con Nessus.
- Spade, motor de estadística de paquetes para detección de anomalías. Se usa para obtener conocimientos sobre los ataques sin firma.
- Tcptrack, utilizado para analizar datos de la sesión de información útiles en la detección de ataques.
- Ntop, que permite monitorizar en tiempo real los usuarios y aplicaciones que están consumiendo recursos de red.
- Nagios, que alimentándose de la base de datos de activos, supervisa la disponibilidad del servicio.
- Osiris, es un sistema de Detección de Intrusos basado en Host. HIDS.
- OCS-NG, plataforma de inventario.[23]

1.6.1 Snort

Snort es un IDS o Sistema de detección de intrusiones basado en red. Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida como patrones que corresponden a ataques, barridos, intentos de aprovechar alguna vulnerabilidad, análisis de protocolos, etc conocidos. Todo esto en tiempo real. Snort Está disponible bajo licencia GPL, gratuito y funciona bajo plataformas Windows y UNIX/Linux. Es uno de los más usados y dispone de una gran cantidad de filtros o patrones ya predefinidos, así como

actualizaciones constantes ante casos de ataques, barridos o vulnerabilidades que vayan siendo detectadas a través de los distintos boletines de seguridad.

Los sistemas IDS y Snort buscan patrones previamente definidos que impliquen cualquier tipo de actividad sospechosa o maliciosa sobre nuestra red o Host. Aportan a la seguridad una capacidad de prevención y de alerta anticipada ante cualquier actividad sospechosa. No están diseñados para detener un ataque, aunque sí pueden generar ciertos tipos de respuesta ante éstos. Aumentan la seguridad de nuestro sistema, vigilan el tráfico de nuestra red, examinan los paquetes analizándolos en busca de datos sospechosos y detectan las primeras fases de cualquier ataque como pueden ser el análisis de nuestra red.[25]

1.6.2 Ntop

Ntop es una herramienta que nos permite conocer y analizar la composición del tráfico de nuestra red a un nivel de detalle impresionante. A diferencia de otras aplicaciones similares, Ntop analiza los paquetes de la red y los agrupa según las direcciones MAC o IP (según como esté configurado) de origen y destino, inclusive agrupa el tráfico según los protocolos establecidos en la capa de transporte presente en el Modelo TCP/IP. Esta herramienta es muy interesante porque nos permite conocer:

- Qué equipos están generando tráfico de red.
- De donde y hacia donde van los paquetes.
- La cantidad de paquetes y sus respectivos tamaños.
- Total de paquetes TCP, UDP y otros.
- Lo enviado y lo recibido.
- Los tipos de servicio utilizados.
- Los puertos a los cuales se ha conectado una u otra máquina.[26]

Permite monitorizar en tiempo real una red. Es útil para controlar los usuarios y aplicaciones que están consumiendo recursos de red en un instante concreto y

para ayudarnos a detectar malas configuraciones de algún equipo, o a nivel de servicio.[27]

Ntop nos facilita la labor de diagnóstico de nuestra red.

1.6.3 OCS Inventory NG

OCS Inventory es un Software Libre que permite a los usuarios administrar el inventario de sus activos de TI. OCS-NG recopila información sobre el hardware y software de equipos que hay en la red que ejecutan el programa de cliente OCS ("agente OCS de inventario").

OCS puede utilizarse para visualizar el inventario a través de una interfaz web. Además, OCS comprende la posibilidad de implementación de aplicaciones en los equipos de acuerdo a criterios de búsqueda. Además, tiene muchas opciones más como escanear la red por medio del IPDiscovery, o instalar aplicaciones remotamente creando Builds.

OCS se basa en los estándares vigentes. El diálogo entre los equipos clientes y el servidor se basan en HTTP y el formato de los datos se realiza en XML.[28]

OCS Inventory NG es un sistema de inventario y distribución de paquetes con interface web.

1.7 Conclusiones parciales

- Al diseñar redes LAN deben tenerse en cuenta aspectos de seguridad informática.

- Con los switches Quidway 5300 y 3300 se pueden implementar medidas de seguridad en las capas 2 y 3 del modelo OSI.

- OSSIM constituye una solución de Software Libre que integra múltiples herramientas que facilitan controlar la Seguridad de una Red.

Capítulo 2:"Diseño de seguridad para Redes LAN utilizando switches Huawei S5300 y OSSIM".

El presente capítulo abordará un análisis de los ficheros de configuración de los Switches Quidway S5300 y S3300 que se utilizarán en el diseño que se propone. Además se describe la propuesta de este trabajo. Se ejemplificará el uso e importancia del Software Libre, con algunas de las tecnologías que existen para facilitar el trabajo de los administradores de red en la seguridad de las computadoras.

2.1 Descripción del problema

La introducción y uso de las TIC ha sido un salto vertiginoso en el desarrollo científico técnico a escala mundial. Constituyendo un indicador en el progreso para los países.

Cuba ha incorporado el uso de estas tecnologías, a pesar que desde 1962, tiene prohibido el acceso a equipos de telecomunicaciones, aplicaciones informáticas y software de cualquier compañía o subsidiaria estadounidense, que son las más importantes en esta actividad.

Nuestro país apuesta por su utilización masiva en aras del desarrollo económico y social del país. Es por eso que se han creados alternativas a todas estos escenarios, la utilización de Software Libres.

Huawei Technologies es una empresa privada de alta tecnología que se especializa en investigación y desarrollo, producción y marketing de equipamiento de comunicaciones y provee soluciones de redes personalizadas para operadores de la industria de telecomunicaciones. Es el mayor fabricante de equipamiento de redes y telecomunicaciones de China y uno de los líderes mundiales en esta industria.[29]

Huawei provee redes de telefonía fijas, móviles, comunicaciones de datos, redes ópticas, software & servicios y terminales telefónicos, incluyendo módems --- conmutadores, redes de acceso integradas, transporte óptico, redes inteligentes, una serie completa de routers y conmutadores IP, videoconferencia y equipamiento a otros campos clave de la tecnología de telecomunicaciones.

Los productos de Huawei son instalados en más de 100 países, incluyendo Brasil, Estados Unidos, Alemania, Francia, Reino Unido y España. [29]

En las empresas cubanas es fácil obtener equipos Huawei y herramientas de seguridad asentados en Software Libre, para desarrollar redes informáticas de manera segura.

Indagando acerca de las soluciones que se usan en las empresas cubanas para garantizar la seguridad en la red, no se encontró información relevante ya que las empresas no dan información real de sus diseños, por no dar a reconocer las posibles vulnerabilidades asociadas a diseños no acertados. Como respuesta a la falta de referencia, la investigación se basa en una opción de tantas que se pueden emplear.

2.2 Fichero de Configuración (Capa dos)

Una vez expuesto en el capítulo anterior, algunas de las funcionalidades de este switchs se verán como es posible configurar estos switches.

Se hará un análisis primero del más sencillo, el capa dos, aquí simplemente se definirán las VLAN1 correspondientes y se especificará qué puertos del switch pertenecen a las VLANs, además se precisarán los puertos troncos que sean necesarios, aclaremos que pueden ser más de uno según se requiera, dicho(s) puerto(s) tronco permitirá pasar todas las vlans.

1 es una red de área local que agrupa un conjunto de equipos de manera lógica y no física.

El puerto asignado a la VLAN es independiente del usuario o dispositivo conectado en el puerto. Esto significa que todos los usuarios que se conectan al puerto serán miembros de la misma VLAN. Por lo general es el administrador de la red el que realiza las asignaciones a estas. Después de que un puerto ha sido asignado, a través de ese puerto no se puede enviar ni recibir datos desde dispositivos incluidos en otra VLAN.

Los puertos de un switch pueden ser de dos tipos, en lo que respecta a las características VLAN: puertos de acceso (access) y puertos troncos (trunk). Un puerto trunk puede ser miembro de múltiples VLANs. Por defecto es miembro de todas, pero la lista permitida es configurable.

Seudocódigo:

Fichero de configuración; configuración

Algoritmo:

Definir las VLANs

Determinar los puertos que pertenece a cada VLAN

Especificar qué puerto se utilizará como trunk

Fin programa

¿Cómo se define una VLAN?

Antes de ver como se define una VLAN se explicará los modos de vista. Existen dos modos de vista: el de usuario o user view y el de sistema o system-view. En cada uno de estas vistas solo se pueden emplear comandos de su propio nivel o inferiores.

Cuando se ingresa al prompt en el modo de vista usuario la petición de entrada aparece de la siguiente forma: <Quidway>.
En el **system-view** se ingresan todos los comandos de configuración (excepto

los de administración).

Al modo de vista de sistema se puede ingresar a partir del modo de vista de usuario digitando el comando **system-view** como se muestra a continuación:

```
<Quidway>system-view
 System View: return to User View with Ctrl+Z.
 [Quidway]
```

Para regresar al modo inmediato anterior se digita el comando **quit** y se puede utilizar desde cualquier vista. También se encuentra el comando **return** que nos permite salir de cualquier modo hacia el modo de vista usuario.

Todos los comandos relacionados con una interfaz pueden ser válidos sólo cuando se utilizan en la vista de la interfaz. El comando de **interface** permite entrar en la vista de la interfaz especificada.

Para crear una VLAN se debe ejecutar los siguientes comandos:

```
[quidway] vlan <número de la VLAN>
[quidway-vlan2]
 description <Breve descripción de la VLAN>
```

El <número de la VLAN> es un número entero que la identifica. Obviamente no es posible asignar el mismo número a dos VLAN.

El <descripción de la VLAN> es un descriptivo, por ejemplo, a qué departamento de la empresa está dando servicio.

Para poder entender se mostrará un ejemplo:

Una empresa "X" cuenta con tres subredes que brindan diferentes servicios. Sistemas del grupo de trabajo Contabilidad, los sistemas del grupo de trabajo Recursos humanos y los sistemas del grupo de trabajo Tecnologías de la información.

```
[quidway] vlan 1
[quidway-vlan1]
   description Sistemas del grupo de trabajo Contabilidad
```

```
[quidway] vlan 2

[quidway-vlan2]

  description  Sistemas del grupo de trabajo Recursos humanos

[quidway] vlan 3

[quidway-vlan3]

   description Sistemas del grupo de trabajo Tecnologías de la
información
```

Y así quedan definidas las VLANs.

¿Cómo se especifica qué puertos pertenecen a las VLANs?

```
[quidway013394] interface Ethernet 0/0/<puerto>

[quidway013394-Ethernet0/0/<puerto>]

      port link-type access

      port default vlan <número de la VLAN>
```

Dándole continuidad al mismo ejemplo tenemos que:

Los sistemas del grupo de trabajo Contabilidad se conectan a través de los puertos del 1-5.

Sistemas del grupo de trabajo Recursos humanos se conectan a través de los puertos del 6-12.

Sistemas del grupo de trabajo Tecnologías de la información se conectan a través de los puertos del 13-23.

Además se especifica qué puerto se utilizará como trunk, en este caso será el puerto 24.

Ejecutando los comandos la configuración queda de esta manera:

```
 [quidway013394] interface Ethernet0/0/1
[quidway013394-Ethernet0/0/1]
      port link-type access
      port default vlan 1
#
[quidway013394] interface Ethernet0/0/2
[quidway013394-Ethernet0/0/2]
      port link-type access
      port default vlan 1
#
[quidway013394] interface Ethernet0/0/3
[quidway013394-Ethernet0/0/3]
      port link-type access
     port default vlan 1
 #
[quidway013394] interface Ethernet0/0/4
[quidway013394-Ethernet0/0/4]
      port link-type access
      port default vlan 1
 #
[quidway013394] interface Ethernet0/0/5
[quidway013394-Ethernet0/0/5]
      port link-type access
      port default vlan 1
#
[quidway013394] interface Ethernet0/0/6
[quidway013394-Ethernet0/0/6]
      port link-type access
      port default vlan 2
 #
[quidway013394] interface Ethernet0/0/7
[quidway013394-Ethernet0/0/7]
      port link-type access
      port default vlan 2
#
[quidway013394] interface Ethernet0/0/8
[quidway013394-Ethernet0/0/8]
      port link-type access
     port default vlan 2
 #
[quidway013394] interface Ethernet0/0/9
[quidway013394-Ethernet0/0/9]
      port link-type access
     port default vlan 2
#
[quidway013394] interface Ethernet0/0/10
[quidway013394-Ethernet0/0/10]
      port link-type access
      port default vlan 2
```

```
 #
[quidway013394] interface Ethernet0/0/11
[quidway013394-Ethernet0/0/11]
      port link-type access
      port default vlan 2
#
[quidway013394] interface Ethernet0/0/12
[quidway013394-Ethernet0/0/12]
      port link-type access
      port default vlan 2
#
[quidway013394] interface Ethernet0/0/13
[quidway013394-Ethernet0/0/13]
      port link-type access
      port default vlan 3
#
[quidway013394] interface Ethernet0/0/14
[quidway013394-Ethernet0/0/14]
      port link-type access
      port default vlan 3
#
[quidway013394] interface Ethernet0/0/15
[quidway013394-Ethernet0/0/15]
      port link-type access
      port default vlan 3
 #
[quidway013394] interface Ethernet0/0/16
[quidway013394-Ethernet0/0/16]
      port link-type access
      port default vlan 3
#
[quidway013394] interface Ethernet0/0/17
[quidway013394-Ethernet0/0/17]
      port link-type access
      port default vlan 3
#
[quidway013394] interface Ethernet0/0/18
[quidway013394-Ethernet0/0/18]
      port link-type access
      port default vlan 3
#
[quidway013394] interface Ethernet0/0/19
[quidway013394-Ethernet0/0/19]
      port link-type access
      port default vlan 3
#
[quidway013394] interface Ethernet0/0/20
[quidway013394-Ethernet0/0/20]
      port link-type access
```

```
      port default vlan 3
#
[quidway013394] interface Ethernet0/0/21
[quidway013394-Ethernet0/0/21]
      port link-type access
      port default vlan 3
#
[quidway013394] interface Ethernet0/0/22
[quidway013394-Ethernet0/0/22]
      port link-type access
      port default vlan 3
#
[quidway013394] interface Ethernet0/0/23
[quidway013394-Ethernet0/0/23]
      port link-type access
      port default vlan 3
#
[quidway013394] interface Ethernet0/0/24
[quidway013394-Ethernet0/0/24]
      port link-type trunk
     description Tronco VLANs
     port trunk allow-pass vlan 1 to 4094

#
```

2.3 Fichero de Configuración. (Capa tres)

Los switchs capa tres son los switches que, además de las funciones tradicionales de la capa 2, incorporan algunas funciones de routing (enrutamiento)2, como por ejemplo la determinación de un camino basado en informaciones de capa de red y soporte a los protocolos de routing tradicionales.

En los switches capa tres ya es un poco más compleja la configuración veamos por qué.

Antes de entrar en lo que es la configuración se verá que el control de acceso está conformado por un conjunto de objetos como son: los clasificadores, los de comportamiento, los de tráfico de policía, las ACL3, VLAN y reglas que a continuación se explicarán.

Al igual que en la capa dos, se definirán primeramente las VLAN. Se le

2 es un dispositivo que proporciona conectividad a nivel de red o nivel tres.
3 es un conjunto de reglas.

asignaran el conjunto (IP, máscara) correspondientes a cada una, aquí se debe tener en cuenta que las VLAN son tratadas como interfaces, quedando de esta manera la sintaxis:

```
[quidway013394] interface Vlanif número
[quidway013394-Vlanif número]

     ip address (IP, Mascara)
```

Seguidamente se le asignaran los puertos pertenecientes de cada VLAN, en este se debe establecer un parámetro link-type que puede tomar dos valores access o trunk.

```
[quidway]interface GigabitEthernet 0/0/<puerto>
[quidway-GigabitEthernet0/0/<puerto>]
      port link-type access
      port default vlan <número de la VLAN>
```

Luego se definirán las rutas que no son más que determinar si vienes de una IP enviarla a un router específico.

Se crean un conjunto de reglas que conforman las ACL, las reglas contienen parámetros a establecer que pueden estar presentes o no. Cuando aparece un permit en ese mismo momento se libera el paquete.

Cuando se definen las ACL en ellas se establecen el nombre, su descripción y las reglas anteriormente mencionadas.

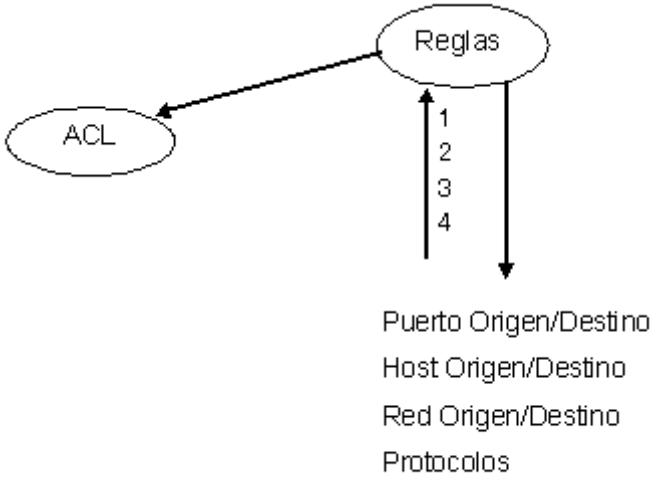

Figura 2: Definición de las reglas.

El clasificador (classifier) está conformado por listas de control de acceso (ACLs) de esta manera:

```
traffic classifier nombre operator and
      if-match acl nombre-acl
```

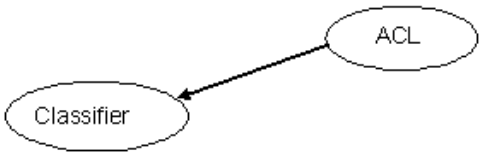

Figura 3: Definición del clasificador.

En el traffic policy se hace referencia al classifier y al behavior, este último tiene como parámetro el deny y el permit que es más conveniente utilizar.

El traffic policy puede estar en out o in.

```
traffic policy nombre.(out o in)
  classifier nombre-classifier behavior nombre-behavior
```

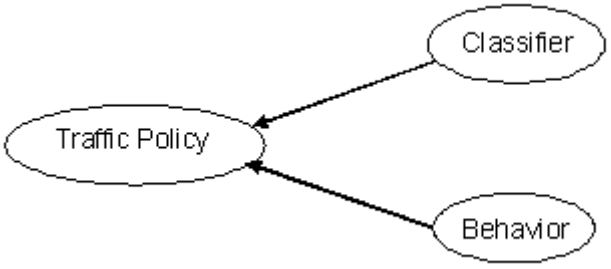

Figura 4: Definición del tráfico de policía.

Y las VLAN que ya fueron creadas están compuestas por un traffic policy.

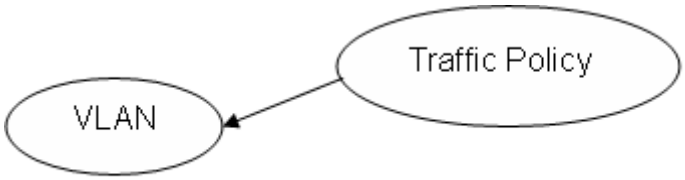

Figura 5: Definición de las VLAN.

Todo lo escrito anteriormente se resume en el siguiente diagrama:

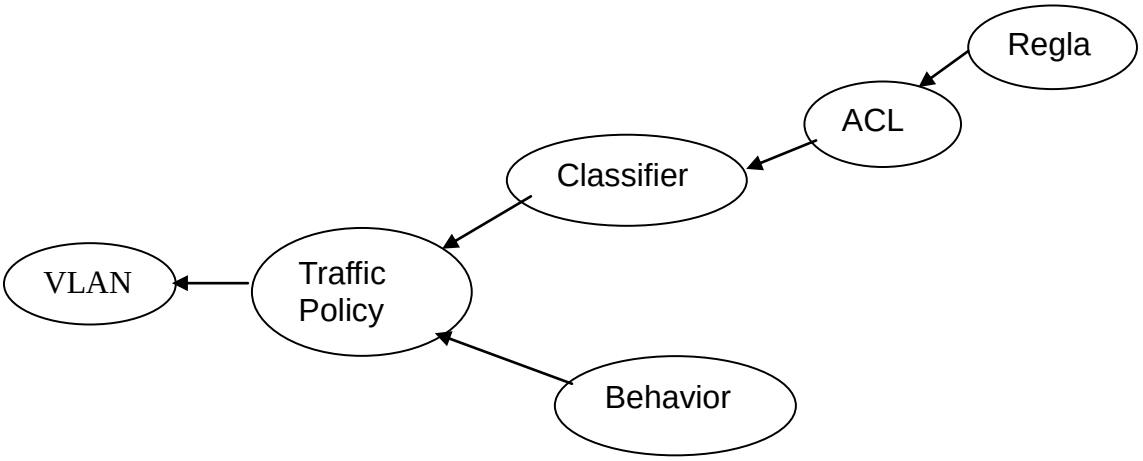

Figura 6: Comunicación de las ACLs con las VLANs.

2.4 Propuesta de Diseño seguro de red LAN.

Cuando se diseña e implementa una red de Área Local (LAN) la seguridad es una de las consideraciones más importantes. Debe ser tenida en cuenta tanto en la parte física como lógica del diseño.

La topología física de la red se refiere a la forma en que distintos componentes

de LAN se conectan entre sí. El diseño lógico de ésta se refiere al flujo de datos que hay dentro de una red. También se refiere a los esquemas de nombre y dirección que se utilizan en la implementación de la solución de diseño LAN.

2.4.1 Mapa Físico.

La red está integrada por diversos elementos físicos que suelen ser comunes en diversos escenarios empresariales. Debe quedar documentado con claridad la distribución del equipamiento y cómo es la conectividad entre ellos.

Esta propuesta de diseño asume como dispositivo de Capa 3 el switch Quidway 5300 y en la Capa 2 los switchs Quidway 3300.

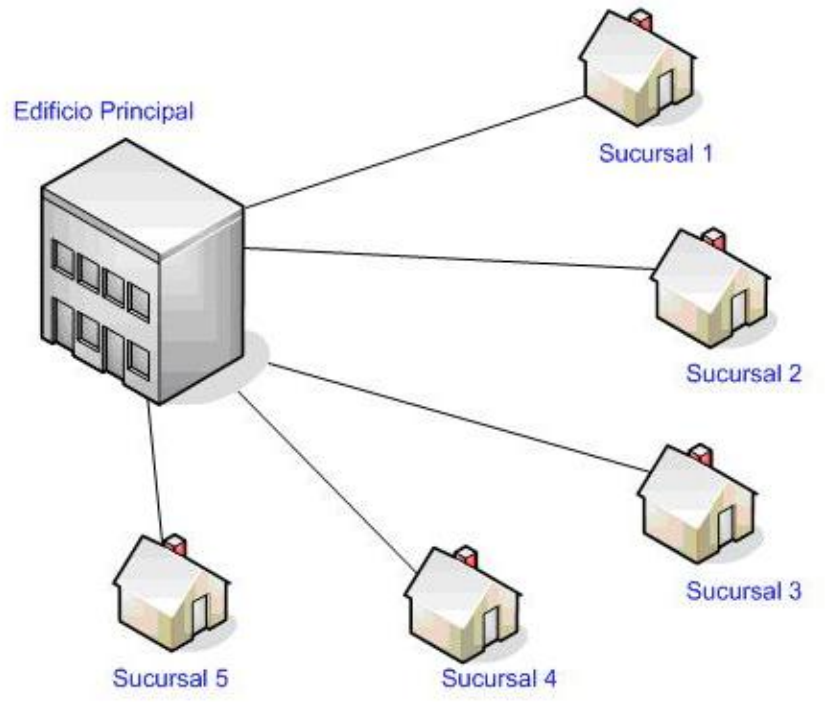

Figura 7: Diagrama de Distribución Geográfica.

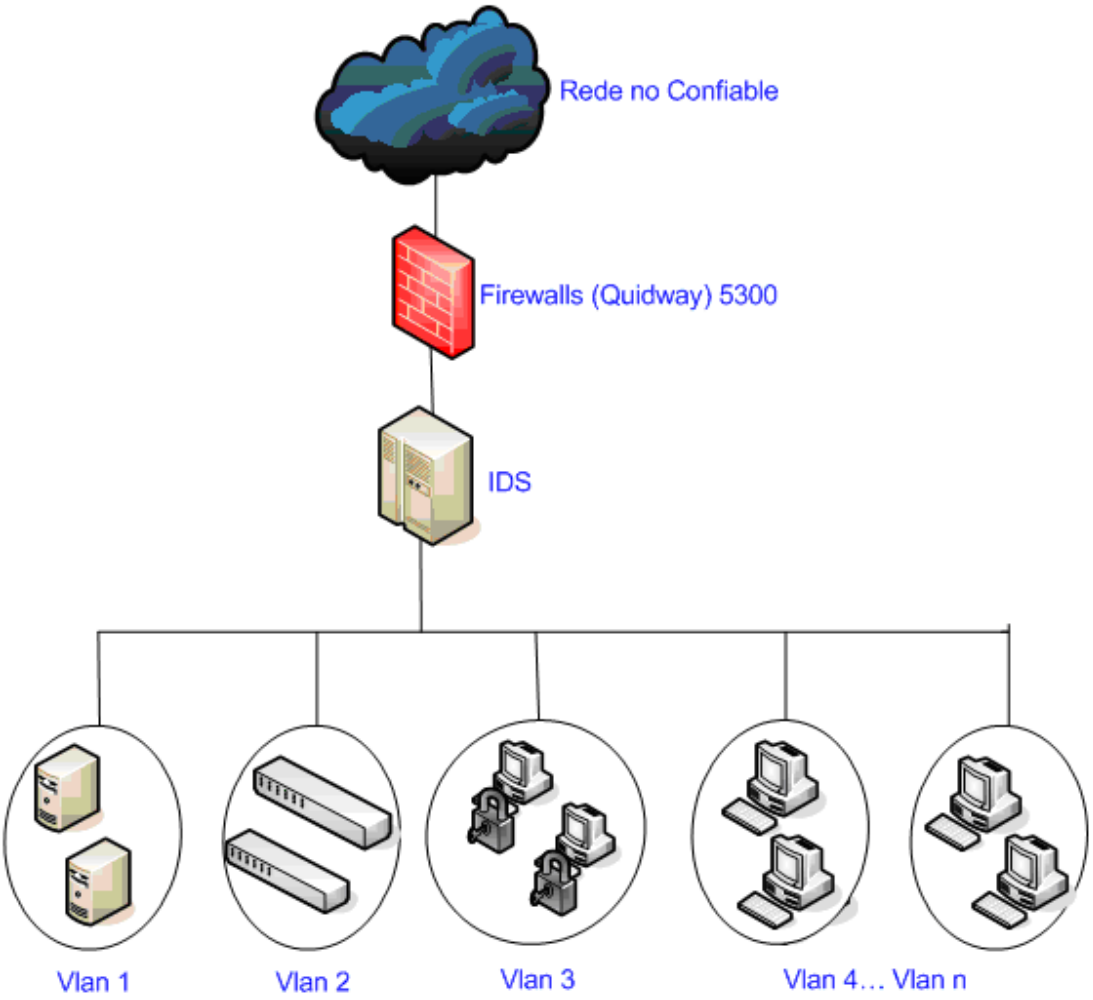

Figura 8: Diagrama de la Red.

2.4.2 Mapa lógico de VLANs. Su implementación en los switchs Quidways 3300.

En toda red LAN hay presente elementos comunes que pueden agruparse teniendo en cuenta los siguientes criterios:

- Servidores

- Equipos de conectividad gestionados por IP.
- Estaciones de administradores de la red.
- Equipos de los usuarios.

Siguiendo estos criterios puede asumirse la siguiente confección de VLANs:

- VLAN1: Contendrían los Servidores, para facilitar las reglas que filtren los accesos exclusivamente a los puertos de los servicios que prestan en la Red.
- VLAN2: Agruparían los equipos de conectividad, que suelen presentar vulnerabilidades asociadas a su gestión por la red y se reduciría el acceso a ellos de los usuarios.
- VLAN3: Destinada a los administradores de la Red y personal encargado de la seguridad, para que solo desde estos puedan administrarse servidores y equipos de conectividad, limitando el acceso a sus computadoras por parte de los usuarios.
- VLAN4…VLANn: Destinadas a las agrupaciones lógicas de las computadoras de los usuarios y se crearán las necesarias para la Empresa en cuestión.

Las VLANs son implementadas con facilidad en los switchs Quidways 3300. En el epígrafe 2.3.1 se detallan los comandos. Aquí se puntualiza como queda el fichero de configuración de este switch que puede resumirse en el siguiente, para el modelo planteado:

```
….
Vlan 1
 description Vlan  para servidores
vlan 2
 description Equipos de conectividad
vlan 3
 description Red de administracion
vlan 4
 description Grupo de usuarios 1
...
```

```
vlan N
 description  Grupo de usuarios N
```

2.4.3 Cortafuego perimetral en el switchs Quidway 5300.

La seguridad perimetral es un concepto emergente, asume la integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión y/o disuasión de intrusos en instalaciones. Ésta se utiliza para definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

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

El cortafuego perimetral propuesto en este diseño utiliza las potencialidades del switch Quidway 5300 de definir ACLs, que regirán la comunicación entre las VLANs definidas en el epígrafe anterior. De esta forma se limitan los accesos a los dispositivos de conectividad y equipos de los administradores tanto del exterior como de la red interna. Pudiendo definirse cuántas reglas sean necesarias de forma más fácil gracias a la agrupación de VLANs definida.
La configuración del switch Quidway 5300 se describe con los comandos que se detallan en el epígrafe 2.3.2, a continuación se muestra como queda el fichero teniendo en cuenta las VLANs propuestas y asumiendo que existen dos VLANs para usuarios:

```
acl name vlan.servidores.in 3995
 rule 1 permit tcp destination
 rule 2 permit icmp icmp


acl name vlan.equiposconectividad.out 3995
```

```
 rule 1 permit ip source 10.30.10.0 0.0.0.255 destination
192.168.80.128 0.0.0.127
 rule 2 permit ip source 192.168.81.224 0.0.0.7 destination
192.168.80.128 0.0.0.127

acl name vlan.administracion.out 3995
 rule 1 permit ip source 192.168.0.0 0.0.255.255
 rule 2 permit ip source 10.30.0.0 0.0.255.255

acl name vlan.usuario1.out 3995
 rule 1 permit ip source 192.168.0.0 0.0.255.255
 rule 2 permit ip source 10.30.0.0 0.0.255.255

acl name vlan.usuario2.out 3995
 rule 1 permit ip source 200.0.0.0 0.255.255.255
 rule 2 permit ip source 172.0.0.0 0.255.255.255

traffic classifier vlan.servidores.in operator and
 if-match acl vlan.servidores.in

traffic classifier vlan.equiposconectividad.out operator and
 if-match acl vlan.equiposconectividad.out

traffic classifier vlan.administracion.out operator and
 if-match acl vlan.administracion.out

traffic classifier vlan.usuario1.out operator and
 if-match acl vlan.usuario1.out

traffic classifier vlan.usuario2.out operator and
 if-match acl vlan.usuario2.out

traffic behavior permit
 permit

traffic policy vlan.servidores.in
 classifier vlan.servidores.in behavior permit

traffic policy vlan.equiposconectividad.out
 classifier vlan.equiposconectividad.out behavior permit

traffic policy vlan.administracion.out
 classifier vlan.administracion.out behavior permit


traffic policy vlan.usuario1.out
 classifier vlan.usuario1.out behavior permit

traffic policy vlan.usuario2.out
```

```
 classifier vlan.usuario2.out behavior permit

vlan 1
 description Vlan  para servidores
 traffic-policy vlan.servidores.in inbound

vlan 2
 description Equipos de conectividad
 traffic-policy vlan.equiposconectividad.out outbound

vlan 3
 description Red de administración
 traffic-policy vlan.administracion.out outbound

vlan 4
 description Grupo de usuarios 1
 traffic-policy vlan.usuario1.out outbound

vlan 5
 description Grupo de usuarios 2
 traffic-policy vlan.usuario2.out outbound
```

2.4.4 Configuración de herramientas de OSSIM para cubrir las necesidades de la red a partir de switch Quidways 5300.

Otro elemento importante en un diseño de seguridad es la presencia de sistemas de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) que es una aplicación usada para detectar accesos no autorizados a un ordenador/servidor o a una red. Estos accesos pueden ser ataques realizados por usuarios malintencionados con conocimientos de seguridad o a través de herramientas automáticas que podrían pasar las reglas del cortafuego.

OSSIM cuenta con un IDS reconocido por su eficiencia en el entorno internacional, SNORT, pero este necesita acceder a todo el tráfico de red que sea posible para evaluar con claridad el comportamiento de la misma. Una vez configurado adecuadamente (Ver Anexo 1) debe tener acceso al tráfico a partir de un puerto espejo del puerto trunk del switch Quidways 5300. Para ver como queda creado este puerto espejo en el fichero de configuración tenemos lo

siguiente:

Puerto espejo del tronco de VLANs que sale de la Empresa a la red…

```
observe-port 1 interface GigabitEthernet0/0/12

interface GigabitEthernet0/0/17
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 ntdp enable
 ndp enable
 bpdu enable
 port-mirroring to observe-port 1 both
```

De esta forma el diseño cubriría de forma suficiente el perímetro de la red diseñada, pero la protección contra ataques internos estaría incompleta. OSSIM ofrece entonces otras herramientas que darían mayores niveles de seguridad.

El SNORT configurado de esta forma se convierte en el IDS perimetral pero a nivel de host se pueden instalar agentes de OSSEC.

Este es un conocido HIDS que además de controlar modificaciones de ficheros, analiza logs de las máquinas monitorizadas en busca de algún evento que pueda ser signo de un ataque. Reconoce y parsea gran cantidad de tipos de logs y tiene un motor de reglas con capacidad de correlación. Esta es su funcionalidad habitual, aunque también puede ser realmente útil como herramienta para la investigación de un incidente. OSSEC tiene una herramienta que aunque originalmente sirve como diagnóstico del correcto funcionamiento de la aplicación, puede procesar un log recopilado en línea (offline) de un equipo no monitorizado inicialmente, y procesarlo en el motor de OSSEC con el fin de encontrar evidencias de forma muy sencilla.[30]

Este es un Host IDS opensource que incluye características que lo convierten en una herramienta muy interesante para asegurar un sistema, ya sea de la familia Unix o Windows.

Nace como sistema de detención de intrusos basado en logs pero en la actualidad ha evolucionado incluyendo otras funciones, entre ellas:

- **Control de integridad de ficheros**: verifica que los ficheros relevantes del sistema no sean alterados de forma no gestionada.
- **Control de integridad del registro**: igual al anterior, pero para claves del registro. De esta forma se puede monitorizar si se añade un nuevo servicio, y se conecta un dispositivo USB, si se agrega una aplicación para que arranque al inicio de windows, etcétera.
- **Detección de rootkits**: está basado en firmas y es un poco básico.
- **Respuesta activa**: actuando como IPS, puede añadir reglas al firewall para bloquear hosts que generen eventos determinados.

Aunque la parte más relevante es el análisis y sistema de alertas basado en los logs, para los que dispone de decenas de decodificadores que los procesarán con lógica. [31]

Otras herramientas para el control de la red en OSSIM que se proponen son:

- ARPWATCH

  Arpwatch es una herramienta sencilla que vigila las direcciones IP de la red y analiza cambios sospechosos. ARP construye una tabla que contiene las correspondencias entre los dispositivos de la red y las direcciones IP que usan.

  Arpwatch monitoriza las respuestas ARP en busca de cambios y envía un email al administrador en caso de ocurrir algo sospechoso. Además de proporcionar una forma sencilla de auditar el número de direcciones IP en uso en una red, es un sistema de detección temprana que se puede configurar para que escuche en varias interfaces a la vez.

  Los logs de Arpwatch guardan las direcciones MAC, las direcciones IP asociadas, las marcas de tiempo de las últimas actividades, los nombres de dispositivo (alias o nombres DNS), y las interfaces desde las que se observa dicha actividad. [32]

- OCSinventory NG

OCS Inventory NG es una herramienta que facilita el seguimiento de la configuración y el software instalado en los ordenadores de una red local, así como la instalación remota de aplicaciones desde un servidor web. Tiene la ventaja de ser software GPL y Open source.

Es una aplicación diseñada para ayudar al administrador del sistema o red a mantener la pista de la configuración y el software instalado en los computadores de la red. También permite el despliegue de paquetes en computadores Windows y Linux. [33]

2.5 Conclusiones parciales.

- Al utilizar una buena configuración de los switches esta nos ayudará en la obtención de un buen diseño de seguridad.

- Con una buena implementación del IDS se alcanzarán resultados más profundos ya que este es un elemento importante en un diseño de seguridad.

- Además del IDS, para completar la protección contra ataques internos OSSIM ofrece entonces otras herramientas que darían mayores niveles de seguridad.

Capítulo 3 - "Validación del modelo propuesto"

En el presente capítulo se describirá el escenario de prueba, una red LAN real que implementó el modelo propuesto. Describiendo como se comporta ante ataques externos e internos a partir de un estudio de vulnerabilidades con la herramienta Nessus antes y después de implementarlo.

3.1 Escenario de prueba

Se escoge una red LAN de una Empresa en la provincia de Cienfuegos, a la que en lo adelante se denomina *Empresa*. La red seleccionada es compleja, presentando variedad de equipamiento, sistemas operativos y aplicaciones.

Las computadoras están distribuidas por toda la provincia y dentro del municipio Cienfuegos en varias dependencias, para un total de aproximadamente 500 equipos de gestión IP. De éstos, varios realizan función de servidores, sustentando las aplicaciones clásicas como: directorio activo, web, DHCP, DNS, Bases de datos, etc.

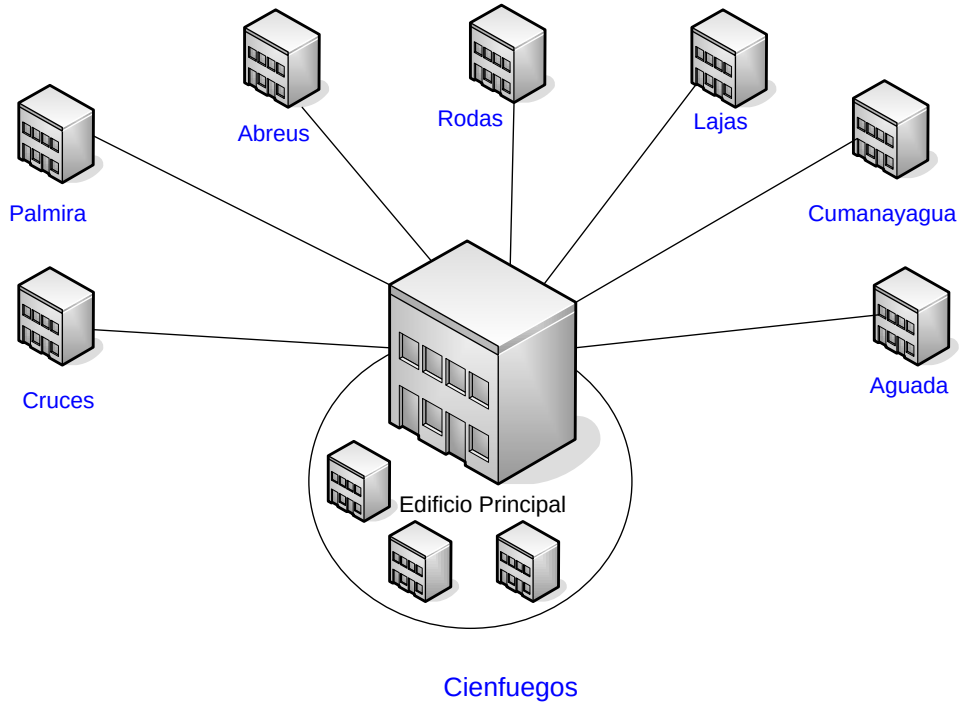

Figura 9: Diagrama de distribución geográfica de la Empresa.

Desde el punto de vista de estructura, la Empresa está dividida por Grupos que siguen la siguiente distribución: Directivos, Comercial, Recursos Humanos y Logística.

3.2 Situación antes de implementar el modelo de diseño propuesto.

La Empresa anteriormente presentaba dificultades en sus redes por la presencia de switches variados en tecnología y solo de capa 2. Ante esta situación se carecía de cortafuego perimetral.

Las VLANs solo tenían en cuenta las agrupaciones lógicas de los usuarios diseñadas para separarlos por departamento y funciones, regulando la comunicación entre ellas. Además de no estar separados los servidores, administradores y switches, estando accesibles desde cualquier punto de red.

Las vulnerabilidades asociadas a este diseño eran muchas, teniendo en cuenta que los dispositivos de gestión IP eran accesibles por todos y estos presentan múltiples vulnerabilidades conocidas.

Por las características del trabajo y la obsolescencia tecnológica de algunos equipos es necesario contar con software obsoletos que tienen documentadas varias vulnerabilidades críticas que atentan contra la seguridad de la Red.

Existía un IDS de Red (SNORT ubicado en el servidor OSSIM) pero que recibía eventos incompletos y el OSSEC no estaba implementado. Al realizarse ataques externos e internos solo eran detectados en minoría por el SNORT y en algunos casos por el Antihacker del antivirus Kasperky instalado en las PCs con Windows.

Se recibe entonces equipamiento Huawei que permitió sustituir los switches por Quidways 3300 y estandarizar así su administración. Además de un Quidway 5300 que permitió implementar un cortafuego perimetral.

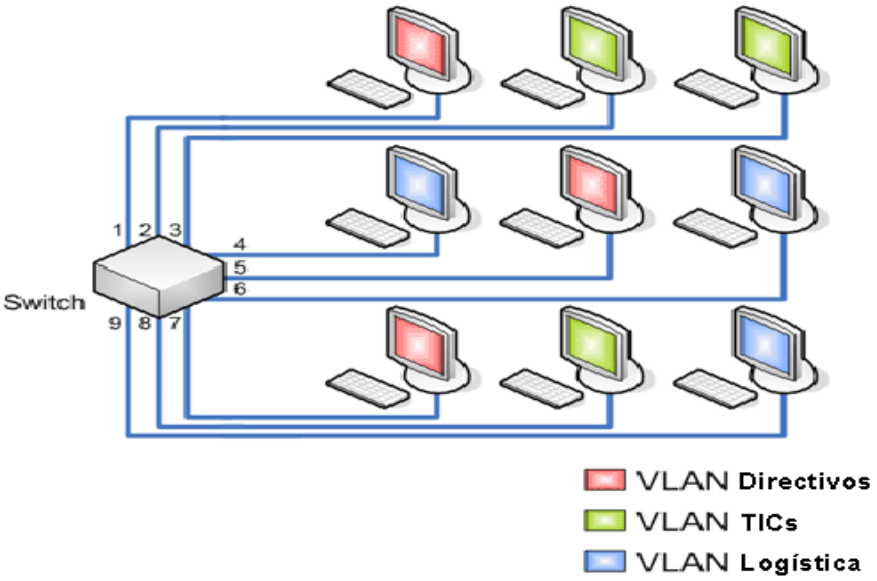

Figura 10: Distribución de VLANs antes de implementar el modelo.

3.3 Situación posterior al uso del modelo de diseño propuesto.

Al recibir el equipamiento Huawei, puede implementarse el modelo propuesto en la presente investigación. Se definen las siguientes VLANs a nivel de los switches Quidways 3300:

VLAN1: Integrada por los Servidores.
VLAN2: Para los equipos de red con gestión IP.
VLAN3: Agrupa a los administradores de la red.

A partir de la VLAN 4 se definen teniendo en cuenta la estructura de la Empresa.

VLAN4: Directivos de la Empresa.
VLAN5: Grupo Comercial.
VLAN6: Grupo de Recursos Humanos.
VLAN7: Grupo de Logística.

Esta distribución de VLANs permitió:

- Definir ACLs en el Quidway 5300 que regulen la comunicación entre las VLANS, limitando la posibilidad de administración de equipos de conectividad y servidores exclusivamente a los miembros de la VLANs de

administradores.

- Limitar el acceso a los dispositivos de conectividad por parte de los usuarios y posibles atacantes externos.
- Evitar suplantaciones de IP asociados a servidores, equipos de red y administradores, desde los puntos de red accesibles por los usuarios.

Las reglas definidas además solo permiten acceder a los servidores por los puertos asociados a los servicios que brindan, limitando así las posibilidades de explotar vulnerabilidades asociadas a los sistemas operativos obsoletos.

El diagrama de la red de la Empresa se describe en la siguiente figura:

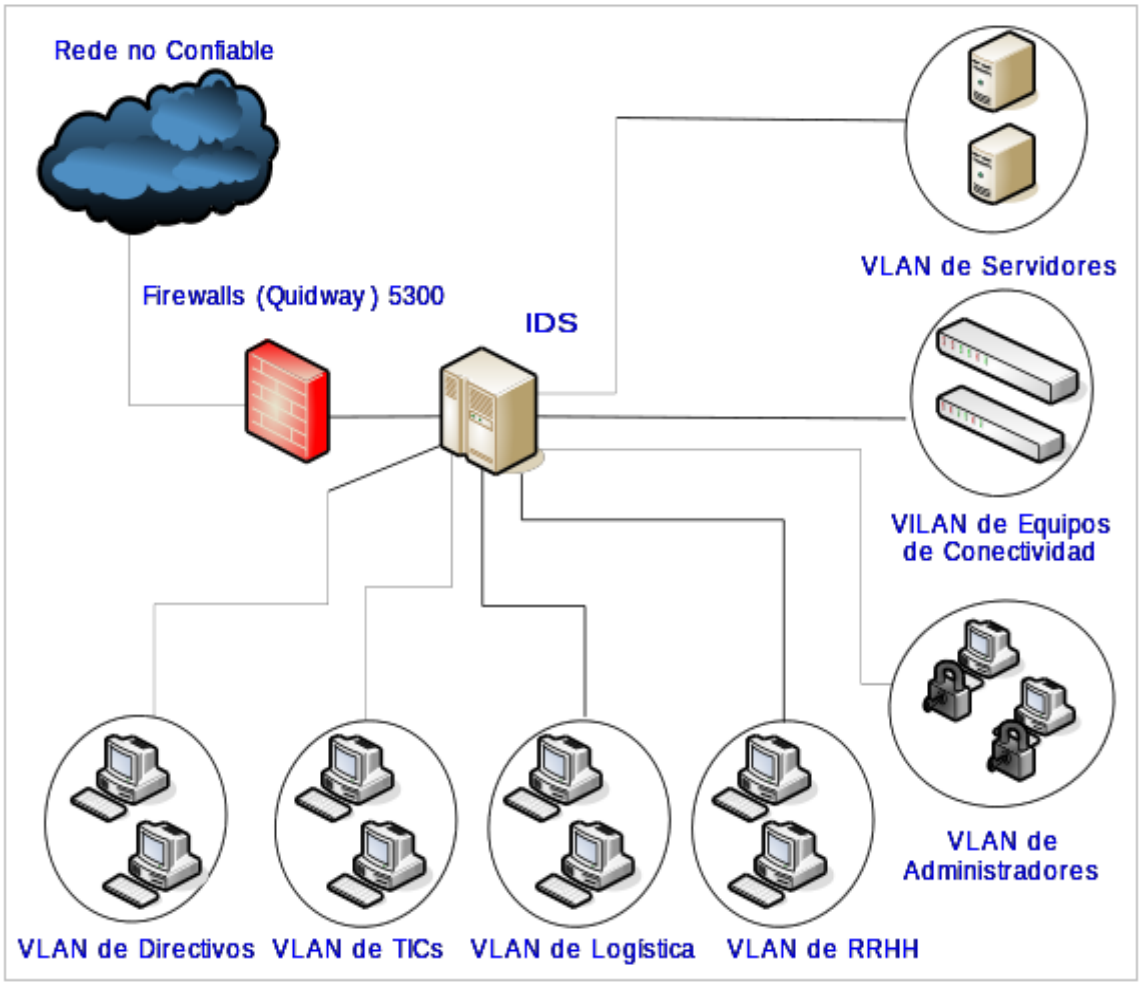

Figura 11: Diagrama de la red de la Empresa.

3.4 Estudio de vulnerabilidades utilizando la herramienta Nessus.

Nessus es una aplicación para el escaneo de vulnerabilidades, una herramienta indispensable para auditorías de seguridad informática, disponible para Linux, Windows, BSD, Mac OS X y Solaris. La principal característica de esta herramienta es que se basa en un modelo cliente/servidor. Está caracterizado por tener facilidades completas de informes, exploración de hosts y búsquedas de vulnerabilidades en tiempo real. En operación normal, nessus comienza escaneando los puertos con Nmap o con su propio escaneador de puertos para buscar puertos abiertos y después intentar varios Exploits para atacarlo.
En el estudio de validación realizado se empleó la versión 5.0 de Nessus con los plugins actualizados. A continuación se describirán las vulnerabilidades detectadas antes y después de aplicar el modelo propuesto.

3.4.1 Resultados de la herramienta Nessus antes de implementar el modelo.

Durante el proceso de escaneo las vulnerabilidades detectadas son variadas, en aras a comprender mejor a qué están asociadas, se agruparán según el siguiente criterio: equipos de conectividad, sistema operativo y de los servicios de red existentes en los servidores.

Vulnerabilidades de los equipos de conectividad

- **10264 – Es posible conocer el nombre del agente SNMP:** Es posible obtener los nombres de la comunidad predefinidos del servidor de SNMP remoto.
- **10267 - El tipo de servidor SSH y su versión:** Es posible obtener la información sobre el servidor de SSH remoto enviando una demanda de la autenticación vacía.
- **10281 - Detención de servidor de Telnet:** El equipo remoto está ejecutando un servidor de Telnet.

- **34022 - Descubrimiento de información de asignación de ruta en el SNMP:** Es posible obtener la información de la asignación de ruta sobre el equipo remoto enviando las demandas de SNMP. Un atacante puede usar esta información para ganar más conocimiento sobre la topología de la red.
- **35296 - Se detecta la versión del agente SNMP:** Enviando un SNMP, es posible determinar la versión protocolar del agente de SNMP remoto.
- **41028 - Agente SNMP con nombre de la comunidad por defecto (public):** Es posible obtener el nombre de la comunidad predefinido del servidor de SNMP remoto. Un atacante puede usar esta información para ganar más conocimiento sobre el equipo remoto, o para cambiar la configuración del sistema remoto (si la comunidad predefinida permite las tales modificaciones).
- **42263 - Servidor Telnet sin cifrado:** El equipo remoto está ejecutando un servidor de Telnet encima de un cauce sin cifrar. Telnet usado encima de un cauce sin cifrar no se recomienda como el logins, se transfieren contraseñas y órdenes en texto claro. Un atacante puede escuchar una sesión de Telnet y obtener credenciales u otra información sensible.

  El uso de SSH se prefiere hoy en día, ya que protege las credenciales de las escuchas y pueden crear un túnel de flujos de datos adicionales, como la sesión de X11.

Vulnerabilidades de los sistemas operativos

- **10757 – Se detecta servidor Webmin:** El servidor remoto ejecuta Webmin, una interfaz basada en web para la administración del sistema de Unix.
- **10940 - Windows tiene los Servicios Terminales habilitados:** Los Servicios terminales le permiten a un usuario de Windows obtener un login gráfico remotamente (y por consiguiente actúa como un usuario

local en el equipo remoto).

Si un atacante obtiene un nombre de usuario y contraseña válidos, puede ser capaz de utilizar este servicio para ganar aún más el acceso en la máquina remota. Un atacante también puede utilizar este servicio para montar un ataque de diccionario contra la máquina remota para intentar iniciar sesión de forma remota.

Tenga en cuenta que RDP (Remote Desktop Protocol) es vulnerable a los ataques *Hombre en el medio*, por lo que es fácil para los atacantes para robar las credenciales de usuarios legítimos haciéndose pasar por el servidor de Windows.

- **11936 - Es posible suponer el sistema operativo remoto:** Usando una combinación de sondas remotas, (TCP / IP, SMB, HTTP, NTP, SNMP, etc) es posible adivinar el nombre del sistema operativo remoto en uso, y, a veces su versión.
- **18405 – El protocolo de monitor remoto de Windows tiene la vulnerabilidad de *hombre en el medio*:** La versión a distancia del Protocolo de escritorio remoto Server (Terminal Service) es vulnerable a un *in-the-middle man-ataque* (MiTM). El cliente RDP no hace ningún esfuerzo para validar la identidad del servidor al configurar el cifrado. Un atacante con la capacidad para interceptar el tráfico desde el servidor RDP puede establecer encriptación con el cliente y el servidor sin ser detectado. Un ataque MiTM de esta naturaleza permitiría al atacante obtener información sensible transmitida, incluyendo las credenciales de autenticación. Existe este error porque el servidor RDP almacena una clave privada RSA codificada en la biblioteca mstlsapi.dll. Cualquier usuario local con acceso a este archivo (en cualquier sistema Windows) puede recuperar la clave y utilizarla para este ataque.

- **30218 - El nivel de encriptación del servicio de terminal no es compatible con FIPS-140:** La configuración de cifrado que utiliza el servicio de Servicios de Terminal remoto no es compatible con FIPS-140.

- **33850 – Sistema operativo Unix sin soporte:** Según su versión, el sistema operativo Unix remoto es obsoleto y ya no se mantiene por su vendedor o proveedor.

  La falta de apoyo implica que hay nuevos parches de seguridad que se darán a conocer por ella.
- **57690 – El nivel de cifrado del servicio de Terminales medio o bajo:** El servicio de Terminal remoto no está configurado para utilizar criptografía fuerte.

  Usando criptografía débil con este servicio puede permitir a un atacante espiar las comunicaciones más fácilmente y obtener capturas de pantalla y / o pulsaciones de teclas.
- **47709 – Detectado sistema operativo no soportado Microsoft Windows 2000:** El host remoto está ejecutando una versión de Microsoft Windows 2000.

  Este sistema operativo no está soportado por Microsoft. Esto significa no sólo que no habrá nuevos parches de seguridad para él, sino también que Microsoft es poco probable para investigar o acusar informes de vulnerabilidades en el mismo.

Vulnerabilidades de los servicios de red implementados en los servidores.

Las vulnerabilidades asociadas a los servicios y detectadas por la herramienta dependen del entorno específico en que se realice el estudio, pero el modelo propuesto no contempla su solución. Por este motivo no se detallan. Para una mejor comprensión, un ejemplo de las detectadas en la Empresa estudiada, se aclara que están asociadas a: servidores web, de bases de datos, configuraciones inadecuadas del LDAP, carpetas compartidas con permiso de escritura y la existencia de ftps sin autenticación. En total se detectan 7 vulnerabilidades de este tipo, para un total de 22.

La solución de dichas vulnerabilidades depende de implementar las buenas prácticas definidas para dichos servicios que incluyen utilizar versiones actualizadas y con los parches de seguridad disponibles.

3.4.2 Resultados de la herramienta Nessus después de implementar el modelo.

Al realizar el estudio con Nessus en la Empresa, posterior a la implementación del modelo, las vulnerabilidades asociadas a los equipos de conectividad y asociadas a los sistemas operativos de los servidores desaparecen. La realidad es que tanto los equipos como los servidores continúan con estos problemas, pero desde las VLANs de los usuarios estos no son detectados, eliminando la posibilidad de "explotarlos" un atacante.

Solo quedan abiertas las asociadas a los servicios, que en el epígrafe anterior se aclara persistirán en cualquier diseño de seguridad dependiendo de la adecuada configuración de estos servicios.

Una vulnerabilidad no detectada por la herramienta, pero presente en el diseño anterior que tenía la Empresa, es que desde los puntos de red de los usuarios podían suplantarse los IPs de servidores y equipos de conectividad, provocando denegación de servicios claves. Con el modelo propuesto se imposibilita dicha suplantación desde estos puntos.

Como puede observarse, las vulnerabilidades asociadas a las capas 2, 3 y 7 del modelo OSI, detectadas por la herramienta Nessus disminuyen un 68%. Solo se convive en la red con aquellas asociadas a los servicios que prestan los servidores y que dependen del entorno específico de cada entidad.

3.5 Comportamiento de los Detectores de Intrusos en la Red (IDS).

La Empresa siempre ha contado con IDS para detectar posibles ataques a la red, tanto internos como externos. Aunque se aprecia un notable incremento de los que son detectados gracias a la implementación del diseño propuesto. Es de suma importancia destacar la necesidad de que el IDS perimetral reciba el tráfico adecuado para su correcto funcionamiento.

Pruebas realizadas al sistema de IDS

Para verificar que los IDSs en la Red detectan diversos tipos de ataques, se

realizan diferentes pruebas que describiremos a continuación:

- **Ataque externos:** Desde la red externa de la Empresa se efectúan escaneos a diferentes subrangos de direcciones IP. Además de escaneos puntuales a servidores y computadoras.
- **Ataque internos:** Originados en cada una de las VLANs y desde computadoras que físicamente se encuentran ubicadas en diversos switches, hacia varios subrangos de direcciones IP internas, equipos puntuales (tanto windows como linux) y algunas Pcs de la red externa que son visibles.

Antes de implementar el modelo.

El IDS principal del sistema era el SNORT de OSSIM, pero recibía un tráfico insuficiente y asociado principalmente al intercambio con la red externa. Además, las computadoras con sistema operativo Windows a través del IDS de host que viene con el antivirus Kasperky detectaban algunos ataques puntuales. Las computadoras con Linux adolecían de IDS y solo el 45% de los ataques eran detectados.

Después de implementar el modelo.

Las potencialidades del sistema de detección de intrusos en la Empresa, mejoró sustancialmente al implementar el modelo propuesto. El tráfico que recibe el SNORT es desde un espejo al tronco que intercambia tráfico con la red externa, detectando entonces los ataques externos en el 95% de las pruebas realizadas. Al adicionar el OSSEC como IDS de host, el 92% de los ataques internos son detectados. Fuera de este sistema quedan aquellos realizados puntualmente a un host y con herramientas configuradas para generar pocos eventos.

3.6 Conclusiones parciales

- Al implementar el modelo propuesto, la Empresa estudiada redujo notablemente las vulnerabilidades que pueden ser explotadas desde los

puntos de red de los usuarios.

- El 93.2% de los ataques realizados a la Empresa (tanto internos como externos), fueron detectados por el sistema de IDS en la Empresa que implementó el modelo.

Conclusiones Generales

Con este trabajo se logra una propuesta de un modelo de diseño de red LAN seguro, aplicado a las capas 2, 3 y 7 del modelo OSI, basado en Tecnología Huawei y Software Libre, se han arribado a las siguientes conclusiones:

- Se realizó un análisis del estado actual de los diseños de seguridad para redes LAN.
- Como resultado se obtuvo un modelo de diseño de red LAN seguro basado en tecnología Huawei y Software Libre aplicado a las capas 2, 3 y 7 del modelo OSI.
- El diseño propuesto se implementó en una Empresa que mostró una disminución de un 68% de las vulnerabilidades detectadas en el proceso de validación en el estudio posterior a la implementación. Además de un notable cambio en los ataques detectados por el sistema de detección de intrusos.

Recomendaciones

Una vez concluido la propuesta de un modelo de diseño de red LAN seguro aplicado a las capas 2, 3 y 7 del modelo OSI, basado en tecnología Huawei y Software Libre, nos permitimos recomendar:

- Poner en práctica el modelo de diseño en empresas que deseen mejorar la seguridad en sus redes.
- Generalizar de igual manera el contenido de este trabajo, específicamente su resultado principal, utilizándolo con los fines para lo que fue elaborado, comenzando por las empresas de la provincia, así como las del resto del país.

Referencias Bibliográficas

[1] «Modelo OSI - EcuRed», 21-may-2013. [En línea]. Disponible en: http://www.ecured.cu/index.php/Modelo_OSI. [Accedido: 21-may-2013].

[2] Ríos,Julio, «Seguridad Informática - Monografias.com». [En línea]. Disponible en: http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica.shtml. [Accedido: 21-may-2013].

[3] «Red de computadoras - EcuRed», 21-may-2013. [En línea]. Disponible en: http://www.ecured.cu/index.php/Red_de_computadoras. [Accedido: 21-may-2013].

[4] Gutiérrez Prieto, Juventino, «Seguridad en redes de computadoras - Monografias.com», 2013. [En línea]. Disponible en: http://www.monografias.com/trabajos43/seguridad-redes/seguridad-redes.shtml. [Accedido: 24-abr-2013].

[5] García Chico, Leidys, «Cuba en Noticias (Festival Internacional del Nuevo cine Latinoamericano) - TIC por Cuba», *TIC por Cuba*, 03-jul-2010. [En línea]. Disponible en: http://old.cubahora.cu/index.php?tpl=coberturas/cultura/fest_cine/share-tpls/ver-not.tpl.html&newsid_obj_id=1037511. [Accedido: 21-may-2013].

[6] Emol., «Fabricante chino Huawei amenaza primacía de Ericsson en equipos de telecomunicaciones | Emol.com», 01-feb-2011. [En línea]. Disponible en: http://www.emol.com/noticias/economia/2011/02/01/461803/fabricante-chino-huawei-amenaza-primacia-de-ericsson-en-equipos-de-telecomunicaciones.html. [Accedido: 24-abr-2013].

[7] MOFCOM, «China acapara atención en Feria Informática de La Habana», 21-mar-2013. [En línea]. Disponible en: http://cl2.mofcom.gov.cn/article/chinanews/201303/20130300063294.shtml. [Accedido: 24-abr-2013].

[8] «Juventud Solidaria: El bloqueo de EUA contra Cuba en las TIC», 14-mar-2005. [En línea]. Disponible en: http://solidaria.blogspot.com/2005/03/el-bloqueo-de-eua-contra-cuba-en-las.html. [Accedido: 21-may-2013].

[9] «Integración Sistemas | RunSolutions - Open Source IT Consulting», *Open Source Security Information Management*. [En línea]. Disponible en: http://www.runsolutions.com/index.php?sec=50. [Accedido: 21-may-2013].

[10] «LAN (Red de área local)», feb-2013. [En línea]. Disponible en: http://es.kioskea.net/contents/initiation/lan.php3. [Accedido: 10-abr-2013].

[11] Bustillos Safe, Ali Alberto, «Las Redes - Monografias.com». [En línea].

Disponible en: http://www.monografias.com/trabajos15/redes-clasif/redes-clasif.shtml. [Accedido: 10-abr-2013].

[12] « ¿Qué es una red informática? - RedUSERS», *¿Qué es una red informática?*, 15-feb-2013. [En línea]. Disponible en: http://www.redusers.com/noticias/que-es-una-red-informatica/. [Accedido: 22-may-2013].

[13] *Redes de Computadoras*, Tercera Edición., vol. I, III vols.

[14] «SEGURIDAD INFORMÁTICA». [En línea]. Disponible en: http://auditoriadesistemas.galeon.com/productos2227783.html. [Accedido: 10-abr-2013].

[15] Rodríguez Pérez,Antonio, «La seguridad informática y el control interno en Cuba. Experiencias de la división Copextel Villa Clara | GestioPolis», 14-jul-2009. [En línea]. Disponible en: http://www.gestiopolis.com/administracion-estrategia/seguridad-informatica-y-su-control.htm. [Accedido: 10-abr-2013].

[16] «Seguridad Informatica». [En línea]. Disponible en: http://www.anerdata.com/seguridad-informatica.html. [Accedido: 21-may-2013].

[17] «Metodología de diseño de una LAN - ProgramoWeb.com: El Blog Tecnológico». [En línea]. Disponible en: http://programoweb.com/71586/metodologia-de-diseno-de-una-lan/. [Accedido: 11-abr-2013].

[18] «ANALISIS, DISENO DE LA RED Y ELABORACION DEL PLAN DE SEGURIDAD DE LA COOPERATIVA DE AHORRO Y CREDITO Capitulo1.pdf». .

[19] «Huawei Spain - Ethernet Switches». [En línea]. Disponible en: http://www.huawei.com/es/products/data-communication/ethernet-switches/. [Accedido: 22-may-2013].

[20] Fojo Comesaña,Luis, «Huawei y su pésimo cifrado compartido | Seguridad Informática». [En línea]. Disponible en: http://seguridadcastelao.wordpress.com/2012/12/07/huawei-y-su-pesimo-cifrado-compartido/. [Accedido: 09-abr-2013].

[21] «Definición de software libre». [En línea]. Disponible en: http://www.clerus.org/clerus/dati/2009-12/14-999999/software_libre.html. [Accedido: 21-may-2013].

[22] Atopo, Marisabel, «Software libre y software propietario - Monografias.com». [En línea]. Disponible en: http://www.monografias.com/trabajos89/sotware-libre-y-propietario/sotware-libre-y-propietario.shtml. [Accedido: 21-may-2013].

[23] «OSSIM Administra la Seguridad de su Informacion en Open Source», 10-abr-2009. [En línea]. Disponible en: http://softwarelibrevenezuela.blogspot.es/. [Accedido: 09-abr-2013].

[24] «OSSIM, la consola de seguridad central para las empresas», 05-abr-2005. [En línea]. Disponible en: http://www.belt.es/noticias/2005/abril/05/osimm.htm. [Accedido: 23-may-2013].

[25] «Snort - EcuRed», 10-abr-2013. [En línea]. Disponible en: http://www.ecured.cu/index.php/Snort. [Accedido: 10-abr-2013].

[26] Grabiel, «Instalación y configuración de Ntop en openSUSE | Tormenta de Bits», 08-jun-2012. [En línea]. Disponible en: http://www.tormentadebits.com/2012/06/ntop-en-linux-opensuse.html. [Accedido: 21-may-2013].

[27] «Introducción NTOP | syconet», 03-dic-2012. [En línea]. Disponible en: http://syconet.wordpress.com/2012/12/03/introduccion-ntop/. [Accedido: 21-may-2013].

[28] «OCS Inventory - EcuRed», 21-may-2013. [En línea]. Disponible en: http://www.ecured.cu/index.php/OCS_Inventory. [Accedido: 21-may-2013].

[29] «Huawei - Wikipedia, la enciclopedia libre», 01-may-2013. [En línea]. Disponible en: http://es.wikipedia.org/wiki/Huawei. [Accedido: 23-may-2013].

[30] «OSSEC como herramienta de Manejo de Incidentes», 25-feb-2013. [En línea]. Disponible en: http://www.vencert.gob.ve/index.php/vencert/noticias-home/1232-ossec-como-herramienta-de-manejo-de-incidentes. [Accedido: 23-may-2013].

[31] Ramos,Alejandro, «OSSEC: Introducción ~ Security By Default», 22-nov-2012. [En línea]. Disponible en: http://www.securitybydefault.com/2012/11/ossec-introduccion.html. [Accedido: 23-may-2013].

[32] Binnie, Chris, «Utilizamos herramientas de monitorización de ARP para buscar intrusos en nuestra red local Estrecha Vigilancia»,

[33] Parra,David, «SOPORTEAGROPATRIA - OCS INVENTORY», *OCS INVENTORY*. [En línea]. Disponible en: http://soporteagropatria.wikispaces.com/OCS+INVENTORY. [Accedido: 23-may-2013].

Bibliografía

« ¿Qué es una red informática? - RedUSERS», *¿Qué es una red informática?*, 15-feb-2013. [En línea]. Disponible en: http://www.redusers.com/noticias/que-es-una-red-informatica/. [Accedido: 31-may-2013].

JJ Velasco, «Alternativas en software libre a aplicaciones que usamos diariamente», 28-mar-2013. [En línea]. Disponible en: http://bitelia.com/2013/03/alternativas-en-software-libre. [Accedido: 31-may-2013].

«ANALISIS, DISENO DE LA RED Y ELABORACION DEL PLAN DE SEGURIDAD DE LA COOPERATIVA DE AHORRO Y CREDITO Capitulo1.pdf». .

García Chico, Leidys, «Cuba en Noticias (Festival Internacional del Nuevo cine Latinoamericano) - TIC por Cuba», *TIC por Cuba*, 03-jul-2010. [En línea]. Disponible en: http://old.cubahora.cu/index.php?tpl=coberturas/cultura/fest_cine/share-tpls/ver-not.tpl.html&newsid_obj_id=1037511. [Accedido: 31-may-2013].

«Cuba se prepara para la migración al Software Libre | Oficina del Software Libre», 29-feb-2012. [En línea]. Disponible en: http://www.softwarelibre.ulpgc.es/node/313. [Accedido: 31-may-2013].

MOFCOM, «China acapara atención en Feria Informática de La Habana», 21-mar-2013. [En línea]. Disponible en: http://cl2.mofcom.gov.cn/article/chinanews/201303/20130300063294.shtml. [Accedido: 31-may-2013].

«Definición de software libre». [En línea]. Disponible en: http://www.clerus.org/clerus/dati/2009-12/14-999999/software_libre.html. [Accedido: 31-may-2013].

«El modelo OSI – El modeloOSI.pdf». .

Fernández Galbán, Yohanna, «Estrategia para la introducción del Software Libre en la disciplina Ingienería y Gestión de Software del Plan de Estudio D para la carrera de Ingienería Informática.», Carlos Rafael Rodríguez, Cienfuegos, 2008.

Emol., «Fabricante chino Huawei amenaza primacía de Ericsson en equipos de telecomunicaciones | Emol.com», 01-feb-2011. [En línea]. Disponible en: http://www.emol.com/noticias/economia/2011/02/01/461803/fabricante-chino-huawei-amenaza-primacia-de-ericsson-en-equipos-de-telecomunicaciones.html. [Accedido: 31-may-2013].

Sánchez,Antonio, «Hispasec @unaaldia: Cifrado débil de contraseñas en productos Huawei», 15-nov-2012. [En línea]. Disponible en: http://unaaldia.hispasec.com/2012/11/cifrado-debil-de-contrasenas-en.html. [Accedido: 31-may-2013].

«Huawei - Wikipedia, la enciclopedia libre», 01-may-2013. [En línea]. Disponible en: http://es.wikipedia.org/wiki/Huawei. [Accedido: 31-may-2013].

«Huawei Spain - Ethernet Switches». [En línea]. Disponible en: http://www.huawei.com/es/products/data-communication/ethernet-switches/. [Accedido: 31-may-2013].

Fojo Comesaña, Luis, «Huawei y su pésimo cifrado compartido | Seguridad Informática». [En línea]. Disponible en: http://seguridadcastelao.wordpress.com/2012/12/07/huawei-y-su-pesimo-cifrado-compartido/. [Accedido: 31-may-2013].

«Instalación y configuración de Ntop en openSUSE | Tormenta de Bits», 08-jun-2012. [En línea]. Disponible en: http://www.tormentadebits.com/2012/06/ntop-en-linux-opensuse.html. [Accedido: 31-may-2013].

«Integración Sistemas | RunSolutions - Open Source IT Consulting», *Open Source Security Information Management*. [En línea]. Disponible en: http://www.runsolutions.com/index.php?sec=50. [Accedido: 31-may-2013].

«Introducción NTOP | syconet», 03-dic-2012. [En línea]. Disponible en: http://syconet.wordpress.com/2012/12/03/introduccion-ntop/. [Accedido: 31-may-2013].

«Juventud Solidaria: El bloqueo de EUA contra Cuba en las TIC», 14-mar-2005. [En línea]. Disponible en: http://solidaria.blogspot.com/2005/03/el-bloqueo-de-eua-contra-cuba-en-las.html. [Accedido: 31-may-2013].

Rodríguez Pérez,Antonio, «La seguridad informática y el control interno en Cuba. Experiencias de la división Copextel Villa Clara | GestioPolis», 14-jul-2009. [En línea]. Disponible en: http://www.gestiopolis.com/administracion-estrategia/seguridad-informatica-y-su-control.htm. [Accedido: 31-may-2013].

«LAN (Red de área local)», feb-2013. [En línea]. Disponible en: http://es.kioskea.net/contents/253-lan-red-de-area-local. [Accedido: 31-may-2013].

«Las 10 aplicaciones de software libre más populares». [En línea]. Disponible en: http://mundogeek.net/archivos/2009/10/28/las-10-aplicaciones-de-software-libre-mas-populares/. [Accedido: 31-may-2013].

Bustillos Safe, Ali Alberto, «Las Redes - Monografias.com». [En línea]. Disponible en: http://www.monografias.com/trabajos15/redes-clasif/redes-clasif.shtml. [Accedido: 31-may-2013].

«Metodología de diseño de una LAN - ProgramoWeb.com: El Blog Tecnológico». [En línea]. Disponible en: http://programoweb.com/71586/metodologia-de-diseno-de-una-lan/. [Accedido: 31-may-2013].

«Modelo OSI - EcuRed», 21-may-2013. [En línea]. Disponible en: http://www.ecured.cu/index.php/Modelo_OSI. [Accedido: 31-may-2013].

Feria Gerónimo,Arturo, «Modelo OSI - Monografias.com». [En línea]. Disponible en: http://www.monografias.com/trabajos13/modosi/modosi.shtml. [Accedido: 31-may-2013].

«OCS Inventory - EcuRed», 21-may-2013. [En línea]. Disponible en: http://www.ecured.cu/index.php/OCS_Inventory. [Accedido: 31-may-2013].

«OSSEC como herramienta de Manejo de Incidentes», 25-feb-2013. [En línea]. Disponible en: http://www.vencert.gob.ve/index.php/vencert/noticias-home/1232-ossec-como-herramienta-de-manejo-de-incidentes. [Accedido: 31-may-2013].

Ramos,Alejandro, «OSSEC: Introducción ~ Security By Default», 22-nov-2012. [En línea]. Disponible en: http://www.securitybydefault.com/2012/11/ossec-introduccion.html. [Accedido: 31-may-2013].

CANAIMA, «Ossim». .

«OSSIM Administra la Seguridad de su Informacion en Open Source», 10-abr-2009. [En línea]. Disponible en: http://softwarelibrevenezuela.blogspot.es/. [Accedido: 31-may-2013].

«OSSIM, la consola de seguridad central para las empresas», 05-abr-2005. [En línea]. Disponible en: http://www.belt.es/noticias/2005/abril/05/osimm.htm. [Accedido: 31-may-2013].

«Red de computadoras - EcuRed», 21-may-2013. [En línea]. Disponible en: http://www.ecured.cu/index.php/Red_de_computadoras. [Accedido: 31-may-2013].

Redes de Computadoras, Tercera Edición., vol. I, III vols.

Redes de Computadoras, Tercera Edición., vol. II, III vols.

Hernández Espinosa,Rafael A., «Reflexiones sobre el uso del Software Libre en Cuba. Ventajas - Monografias.com», 2006. [En línea]. Disponible en:

http://www.monografias.com/trabajos40/software-cuba/software-cuba.shtml. [Accedido: 31-may-2013].

Gutiérrez Prieto, Juventino, «Seguridad en redes de computadoras - Monografias.com», 2013. [En línea]. Disponible en: http://www.monografias.com/trabajos43/seguridad-redes/seguridad-redes.shtml. [Accedido: 31-may-2013].

«Seguridad Informatica». [En línea]. Disponible en: http://www.anerdata.com/seguridad-informatica.html. [Accedido: 31-may-2013].

«SEGURIDAD INFORMÁTICA». [En línea]. Disponible en: http://auditoriadesistemas.galeon.com/productos2227783.html. [Accedido: 31-may-2013].

Rios,Julio, «Seguridad Informática - Monografias.com». [En línea]. Disponible en: http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica.shtml. [Accedido: 31-may-2013].

«Snort - EcuRed», 10-abr-2013. [En línea]. Disponible en: http://www.ecured.cu/index.php/Snort. [Accedido: 31-may-2013].

Atopo, Marisabel, «Software libre y software propietario - Monografias.com». [En línea]. Disponible en: http://www.monografias.com/trabajos89/sotware-libre-y-propietario/sotware-libre-y-propietario.shtml. [Accedido: 31-may-2013].

Parra,David, «SOPORTEAGROPATRIA - OCS INVENTORY». [En línea]. Disponible en: http://soporteagropatria.wikispaces.com/OCS+INVENTORY. [Accedido: 31-may-2013].

Binnie, Chris, «Utilizamos herramientas de monitorización de ARP para buscar intrusos en nuestra red local Estrecha Vigilancia», .

Glosarios de Términos

TCP/IP: "Protocolo de control de transmisión/Protocolo de Internet".

OSI: Modelo de Interconexión de Sistemas Abiertos (Open System Interconnection).

GPL: Licencia Pública General (General Public Licence).

LAN: Redes de Área Local (Local Área Network).

UTP: Par trenzado no blindado (Unshielded Twisted Pair).

UDP: Protocolo de Datos de Usuario (User Data Protocol).

STP: Par Trenzado Apantallado (Shilded Twisted Pair).

BNC: del inglés Bayonet Neill-Concelman, por los apellidos de quienes lo inventaron.

MAC: Control de Acceso al Medio (media access control).

SQL: Lenguaje de Consulta Estructurado (Structured Query Language).

HTTP: Protocolo de Transferencia de Hipertexto (**H**iper**T**ext **T**ransfer **P**rotocol).

IP: Protocolo de Internet (Internet Protocol).

LDAP: Protocolo de acceso a Directorios Ligeros (Lightweight Directory Access Protocol).

Backbone: se refiere a las principales conexiones troncales de Internet.

MDF: Main Distribution Facility, servicio de distribución principal.

IDF: Servicios de Distribución Intermedia (Intermediate Distribution Services).

ONU: Organización de Naciones Unidas.

DNS: Sistema de Nombres de Dominio (Domain Name System).

XML: Lenguaje de Marcado Ampliable o Extensible (Extensible Markup Language).

DHCP: Protocolo de Configuración Dinámica de Máquinas (Dynamic Host Configuration Protocol).

Anexos

Anexo 1 “Configuración del Snort”.

Los administradores de sistema toman muy en cuenta la seguridad de sus equipos y sobre todo de su red, mucho más si dentro de ella existe información muy relevante, para eso hay que basarse en un sistema que pueda ofrecer este tipo de protección, en este caso tenemos a **Snort**, además de ser un software libre, nos puede ofrecer una seguridad garantizada configurándolo correctamente, para esto se deben seguir ciertos pasos.

En primer lugar para configurar Snort se van a crear los directorios que necesita para trabajar:

- Se crea el directorio de trabajo de snort:
  mkdir /etc/snort
- Se crea el directorio donde se van a guardar las firmas:
  mkdir /etc/snort/rules
- Se crea el directorio donde va a guardar el registro de actividad:
  mkdir /var/log/snort
  adduser snort
  chown snort /var/log/snort
- Se crea el fichero de configuración local:
  touch /etc/sysconfig/snort
- Se copia el ejecutable a su directorio de trabajo:
  cp /usr/local/bin/snort /usr/sbin

A continuación se deben copiar los ficheros necesarios para poder trabajar con Snort:

- Ficheros de configuración.
  Se copia el fichero snort.conf en /etc/snort/ de la siguiente forma:
  cp /root/snort-2.8.0.1/etc/snort.conf /etc/snort/

Se copia el fichero unicode.map en /etc/snort ejecutando:

cp /root/snort-2.8.0.1/etc/unicode.map /etc/snort/

Se copia el script de inicio del servidor:

cp /root/snort-2.8.0.1/rpm/snortd /etc/init.d/

chmod 755 /etc/init.d/snortd

- Firmas:

  Se deben de descargar las firmas de Snort desde www.snort.org y descomprimir las firmas en la carpeta /etc/snort/rules.

  Posteriormente se copian los archivos con la extensión .config en el directorio /etc/snort.

  Estos archivos son classification.config y references.config:

  cp /etc/snort/rules/*.config /etc/snort

- Preprocesadores:

1. Se crea la carpeta donde se van a guardar los preprocesadores ejecutando:

   mkdir /etc/snort/preproc_rules
2. Finalmente se copian los preprocesadores del directorio de las fuentes a la carpeta que hemos creado:

   cp /root/snort-2.8.0.1/preproc_rules/* /etc/snort/preproc_rules/

El fichero de configuración (/etc/snort/snort.conf) nos permite configurar el sistema para realizar las siguientes acciones:

Especificación de la red ó redes sobre las cuales actuará el snort. Se trata de definir el rango de direcciones de nuestra red local.

Configurar librerías dinámicas. Las librerías dinámicas son ficheros independientes que pueden ser invocados desde el ejecutable.

Configurar los preprocesadores. Los preprocesadores son plug-ins o partes del programa que definen una manera de analizar los paquetes y detectar un mal funcionamiento o un tipo de ataque.

Configurar los plugins de salida. Snort se puede configurar para que tenga varios modos de salida. Estos modos de salida son: por pantalla, en ficheros de log, en una base de datos, con syslog (servidor de eventos del sistema) y con varios formatos como en formato binario (para exportar datos a otros programas).

Directivas de configuración. Las directivas de configuración definen comandos y otras opciones de configuración de snort. El archivo snort.conf incluye el archivo classification.config (define las clasificaciones de las reglas) y el fichero reference.config (define sistemas de identificación de ataque externos).

Personalizar el conjunto de reglas. Snort usa un lenguaje de descripción de reglas simple y flexible para describir cómo se deben de manejar los datos.

Para realizar una configuración básica de Snort, se pueden hacer las siguientes modificaciones básicas sobre el archivo de configuración de Snort:

Se especifica el rango de direcciones de nuestra red interna modificando la variable HOME_NET:

var HOME_NET <Dirección de red> o ANY.

- Se indica el directorio donde se encuentran almacenadas las reglas, modificando variable:

  var RULE_PATH /etc/snort/rules.

- Se determina el directorio donde se encuentran los preprocesadores:

  var PREPROC_RULE_PATH /etc/snort/preproc_rules

- Se activan los preprocesadores que se desean utilizar.

Se habilitan las reglas que se quieren utilizar. Para ello se comentan o descomentan las reglas deseadas. Se recomienda mirar los ficheros de reglas antes de incluirlos, puesto que las reglas por defecto son muy restrictivas y generan demasiadas alertas. Como mínimo se desactiva la regla web_misc_rules.

Se guarda el archivo de configuración snort.conf.