Adaptación de un Módulo que garantice la Alta Disponibilidad del IDS/IPS Snort

Nelson Herrera Conforme [(1)], Carlos Sánchez Quiñonez [(2)], Marco Rodríguez Pozo [(3)]
Facultad de Ingeniería en Electricidad y Computación (FIEC)
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil, Ecuador
nherrera@fiec.espol.edu.ec [(1)], csanchez@fiec.espol.edu.ec [(2)], mrodriguez@fiec.espol.edu.ec [(3)]
Escuela Superior Politécnica del Litoral (ESPOL) [(3)], Ingeniero en Computación [(3)], jaranda@espol.edu.ec [(3)]

Resumen

Este proyecto tiene como finalidad el diseño y la implementación de una de las soluciones al problema más común de las empresas que brindan o dependen de un servicio; disponer siempre y a toda hora del servicio mencionado, en el caso que a continuación presentamos, disponer siempre del servicio de seguridad en la red, que está vigilado por la herramienta de código abierto SNORT. Para este propósito y luego de un profundo análisis se decidió el uso de una combinación de varias herramientas open source para cumplir el objetivo propuesto (alta disponibilidad). La mayoría de sistemas de información se encuentran en servidores. Estos servidores no se encuentran libres de inconvenientes, el hardware puede fallar o un error humano puede ocasionar que nuestro sistema quede fuera de servicio durante un tiempo. La falla de un sistema informático puede producir pérdidas en la productividad y de dinero. Por eso es necesario evaluar los riesgos ligados al funcionamiento incorrecto o falla de uno de los componentes de un sistema informático y crear recursos para poder anticipar los medios y medidas y así evitar incidentes o restablecer el servicio en un tiempo aceptable. La alta disponibilidad consiste en una serie de medidas tendientes a garantizar la disponibilidad del servicio, es decir, asegurar que el servicio funcione durante las veinticuatro horas los 365 días del año.

Palabras Claves: *seguridad, informática, análisis, disponibilidad, servicio, open source, sistemas.*

Abstract

This project aims to design and implement a solution to one of the most common problem of companies that provide or rely on a service; count on and always have at all hours the service mentioned above. In the case presented below, always have the security service in the network which is monitored by SNORT, an open source tool. For this purpose and after a deep analysis it was decided to use a combination of several open source tools to accomplish the proposed objective (high availability). Most information systems are in servers. These servers are not free from drawbacks, hardware could fail or human error may cause your system out of service for a while. The failure of a computer system can cause losses in productivity and money. Therefore it is necessary to evaluate the risks associated with malfunction or failure of one component of a computer system and create resources to anticipate the means and measures to avoid incidents and restore service in an acceptable time. High availability is a series of measures to ensure the availability of service which means the service Works 24/7 and 365 days a year.

Keywords*: security, computer, analysis, integrity, availability, service, open source, systems.*

1. Introducción

El presente proyecto es una solución a uno de los problemas más comunes que existe en las empresas las cuales dependen de un servicio o brindan un servicio a usuarios.

Snort es un detector de intrusos el cual es usado por muchas compañías para dar seguridad a su red, debido a que es un sistema muy importante es de vital importancia tener un plan de contingencia para que la red nunca deje de estar monitoreada.

Para nuestro caso vamos a usar una combinación de herramientas open source las cuales garantizarán la alta disponibilidad del (IDS/IPS) Snort.

2. Generalidades

2.1. Antecedentes

Con el avance de la tecnología y la alta demanda de varios de los servicios ofrecidos por diferentes empresas y la necesidad de las mismas de ofrecer un servicio garantizado y sin interrupciones, es de vital importancia tener un plan de contingencia (BACKUP), el cual asegurará fiabilidad para los usuarios y tranquilidad para las personas encargadas del servicio ofrecido. Las fallas de hardware o software suelen suceder en cualquier momento sin previo aviso al igual que un desastre natural o una falla en el fluido eléctrico.

Para el caso de los sistemas que controlan y censan el trafico en una red de computadores en busca de amenazas, estos sistemas se vuelven muy cotizados y requeridos por las compañías que buscan la protección de sus archivos y redes, un valor agregado que se ofrece junto a estos sistemas es la redundancia o alta disponibilidad ya que una falla podría perjudicar enormemente el trabajo o el servicio de la empresa. El presente proyecto plantea una forma de asegurar la alta disponibilidad específicamente en uno de los sistemas IDS/IPS OpenSource, más usados en la actualidad "SNORT".

2.2. Objetivo General

El objetivo del presente proyecto es garantizar la alta disponibilidad del servicio que nos proporciona el IDS/IPS Snort.

2.3. Objetivos Específicos

Se especifica a continuación los objetivos específicos planteados para el desarrollo e implementación del proyecto.

Adaptación de un módulo usando heartbeat para garantizar alta disponibilidad y drbd para la replicación de datos entre servidor primario y backup.

Adaptación de un módulo usando acoplamiento de interfaces de red (bonding), el cual proveerá tolerancia a fallos en las interfaces de red.

3. Fundamentación Teórica

3.1. Sistemas IDS/IPS

Los IDS/IPS o también conocidos como IDPS, nacen de la unión de dos importantes sistemas:

- IDS (Sistemas de detección de Intrusos).
- IPS (Sistemas de Prevención de Intrusos).

Los IDPS están diseñados para cumplir dos funciones principales:

- Evitar una infiltración a los sistemas informáticos de una empresa, sirviéndose de un sistema captación de pruebas.
- Realizar seguimientos exhaustivos del ente infiltrado y de los pasos que sigue el mismo, para en un futuro realizar las acciones más adecuada

De manera más sencilla los IDS/IPS fueron creados por tener la necesidad de proteger toda información digital que sea de importancia para una empresa o entidad, por estas características a los IDS/IPS se los denominan sistemas "AntiHacker".

3.2. Snort

Snort es un Sistema de detección de intrusos basado en red (NIDS). 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 aprovechar alguna vulnerabilidad, análisis de protocolos, conocidos.

3.3. Virtualización

La virtualización es un conjunto de técnicas de abstracción de recursos computacionales que a través de una capa virtual permite que múltiples maquinas virtuales con sistemas operativos heterogéneos puedan ejecutarse individualmente en las misma maquina física.

Cada máquina virtual dispone de su propio hardware virtual (memoria RAM, CPU, etc.), con el cual se gestiona el sistema operativo y las aplicaciones.

3.4. Alta Disponibilidad

3.4.1 Introducción

La alta disponibilidad consiste en una serie de medidas tendientes a garantizar la disponibilidad del servicio, es decir, asegurar que el servicio funcione durante las veinticuatro horas los 365 días del año.

3.4.2 Heartbeat

Es un daemon que provee una infraestructura de clúster de alta disponibilidad con sus clientes. Se comunica en todo momento con los nodos del clúster mediante pings y notificaciones cada cierto tiempo que indican si el servidor está vivo o no.

3.4.3 DRBD

Software que permite hacer réplica de los datos de una partición entre varias máquinas.

DRBD es frecuentemente usado junto con el Heartbeat, a pesar de que se puede integrar con otros marcos de gestión de clúster.

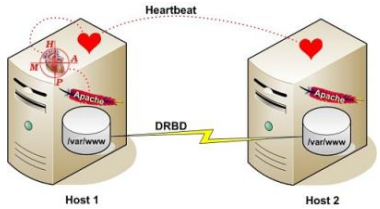

Figura 1. Esquema de heartbeat y drbd

3.5. Bonding

3.5.1 Introducción

Bonding consiste en hacer trabajar varias tarjetas de red como si fuera una, lo que conlleva a que comparten la misma dirección MAC, que puede ser cualquiera del juego de tarjetas que se está uniendo. El resultado final es un aumento de la velocidad bastante considerable, y mediante una interfaz virtual todas las tarjetas de red obedecen a una sola ip.

3.5.2 Modelos de implementación para la HA

Modelo 1

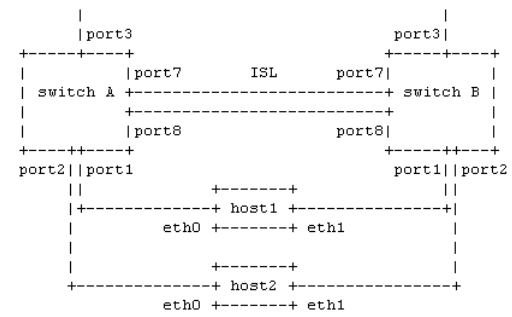

Figura 2. Modelo de múltiples host y switch's

Modelo 2

Figura 3. Modelo con múltiples tarjetas de red conectados a un switch

4. Especificaciones y herramientas para la Solución

4.1. Especificaciones técnicas

Las características o requerimientos básicos que debe tener el servidor para un buen rendimiento y funcionamiento son las siguientes, ver la **Tabla 1**.

Tabla 1. Características del servidor

No	Dispositivo	Requerimiento	
		Mínimo	Recomendado
1	Procesador	Pentium IV de 32bits	Intel Dual Core de 64bits
2	RAM	2 GB	4 GB
3	Disco Duro	160 GB	350 GB
4	Tarjeta de Red	10/100 Mbps	10/100/1000 Mbps
5	Tarjeta Analógica	2 puertos	4 puertos

En la Tabla 2 se presentan los componentes de software.

Tabla 2. Componentes del servidor

No	Componente	Nombre
1	Plataforma	Linux
2	Distribución	Centos 5.5
3	IDS/IPS SNORT	Snort 2.8.6.1
4	DBMS	MySQL 5.0
5	Servidor Web	Apache Tomcat 5.0

4.2. Herramientas de propósito general

4.2.1 MySQL

MySQL es una herramienta OpenSource, se la utiliza en conjunto con el sistema Snort (IDS/IPS) para manejar la interacción con la base de datos, este gestor de base de datos nos permitirá registrar: alertas, eventos y anomalías las mismas que son capturadas por el sistema Snort.

4.2.2 Snort

Es un IDS/IPS con el cual se está implementando la solución del proyecto, este sistema nos permite registrar, alertar y responder ante cualquier anomalía previamente definida como patrones que corresponden a ataques, vulnerabilidades y amenazas que se presentan en el proceso de escaneo y barrido de puertos en un dominio de colisión determinado.

4.2.3 Heartbeat

Es un servicio que trabaja enviando latidos (pings), los cuales verifican si el **servidor principal (Master)** está activo o no, estos pings enviados por heartbeat requieren una respuesta por parte del **servidor principal (Master)**, si al cabo de un cierto tiempo el servidor no responde dichos pings, heartbeat determina que ese servidor se encuentra inactivo, y automáticamente activa al **servidor secundario (Mirror)** que actúa como backup, para que asuma el control de la red.

4.2.4 DRBD

El Dispositivo de Bloques Replicado y Distribuido, nos permite realizar la réplica de la data del **servidor principal (Master)** al **servidor secundario (Mirror)** y viceversa esto depende de que, servidor se vea afectado para que se realice la réplica de la información. Esta replica es transparente para las demás aplicaciones en los sistemas de los equipos.

4.2.4 Monit

Es un software que nos permite realizar un monitoreo exhaustivo de los servicios de mysqld y snortd en cada servidor respectivamente.

4.2.5 Virtualbox

Herramienta de virtualización la cual hacemos uso para efectos de implementación del proyecto, con esta herramienta montamos nuestro ambiente virtualizado de dos equipos uno actúa como servidor principal y el otro como servidor secundario.

5. Diseño e Implementación

5.1. Alta Disponibilidad (Heartbeat–DRBD/ Snort)

Modelo de Clúster Activo - Pasivo

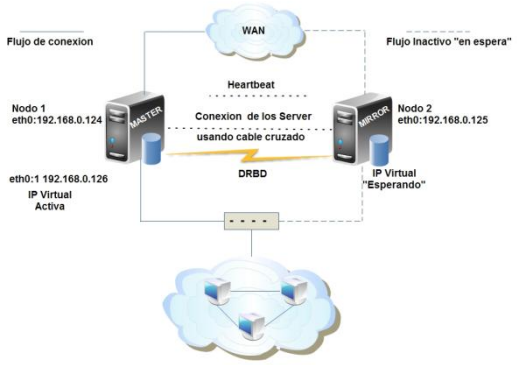

Figura 4. Esquema funcionamiento normal HA

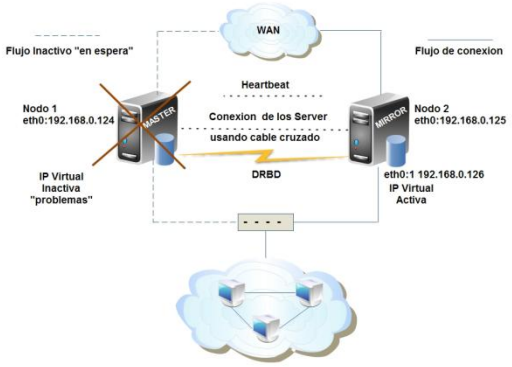

Figura 5. Esquema funcionando en modo backup (HA)

5.2. Alta Disponibilidad con bonding

Para la implementación de esta solución utilizamos el parámetro mode con valor 1 (mode=1), el cual proporciona tolerancia a fallos.

Todo el tráfico se transmite a través de una tarjeta de red y solo se utilizará la otra interfaz en caso de que falle la primera, de esta manera estamos logrando alta disponibilidad a nivel de hardware.

6. Análisis de resultados

6.1. Servicios o procesos no disponibles

En este escenario el servidor principal tiene uno o los dos procesos no disponibles, el monitor de servicios (monit) intenta reiniciarlos por tres veces consecutivas al no lograr su objetivo ejecuta un script que detiene el servicio de heartbeat; el servidor secundario detecta que no hay comunicación con el servidor principal e inmediatamente procede a tomar el control y reanudar las actividades.

Esta tarea donde el servidor secundario es ahora el encargado de realizar las actividades con total normalidad, también conocido como **failover**, se lo realiza con un tiempo de respuesta aproximadamente de 10 seg, cabe recalcar que durante este tiempo se sincronizaron los datos y se iniciaron los servicios necesarios. Este tiempo puede variar y es proporcional a la cantidad de datos a sincronizar.

Una vez que el servidor primario se encuentre nuevamente activo, el servidor secundario establece comunicación con este e inmediatamente detiene los servicios que se estaban ejecutando y da paso a la sincronización de los datos. El servidor primario inicia los servicios necesarios y vuelve todo a la normalidad; el tiempo que toma esta tarea, también conocida como **failback**, es aproximadamente de 30 seg.

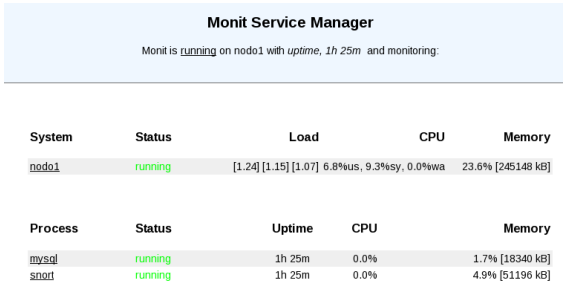

Figura 6. Esquema de servicios monitoreados

6.2. Tarjeta de red defectuosa

Una parte vital de nuestra solución es la comunicación directa entre los servidores que se realiza mediante un cable de red. Si una de las tarjetas de red presentara algún fallo no se podría seguir trabajando normalmente. Para dar solución a este problema se ha implementado un bypass en las tarjetas de red de cada servidor a nivel de software también conocido como bonding.

Si una de las tarjetas de red de cualquiera de los dos servidores presentara algún problema, bonding manejara el siguiente procedimiento. Las dos tarjetas de red se encuentran acopladas a una interfaz virtual con una sola ip.

Esta interfaz verifica por intervalos de tiempo el estado de las tarjetas y si alguna se encuentra inactiva redirige el tráfico a la que este funcional garantizando el servicio continuo.

7. Conclusiones

[1] Con la solución propuesta se cumple en su totalidad con el objetivo propuesto. Es decir, contamos con el servicio las 24 horas del día los 365 días del año; por ende se cuenta con un sistema tolerante a fallos, fiable y confiable.

[2] En la actualidad disponer o hacer uso de los servicios de un sistema tiene una importancia muy significativa, es por eso que la alta disponibilidad o tolerancia a fallos es un requerimiento muy tomado en cuenta al momento de adquirir o implementar un sistema computacional en una empresa.

[3] Las soluciones OpenSource como puede ser Snort está actualmente muy valorada y suponen un ahorro de costes considerablemente respecto a las soluciones comerciales como pueden ser las de Cisco por ejemplo.

[4] La implementación realizada para dar alta disponibilidad a un servicio como es en el caso de Snort, se realizaron concentrándonos en dos puntos vitales en el mundo de la informática, esto es dar alta disponibilidad, a nivel de hardware y software, para los servidores que provean el servicio de Snort, cubriendo de esta manera los dos aspectos por el cual el servicio de Snort puede verse afectado, de manera directa e indirecta, aunque no se abarco todos los escenarios para estos dos niveles, se ha encontrado varias soluciones a los problemas más comunes que podrían afectar el correcto funcionamiento de los servidores.

[5] Durante el desarrollo de este proyecto se puede concluir que debido a la importancia que toma día a día la alta disponibilidad, es más frecuente encontrar todo tipo de soluciones: gratis, de bajo costo e incluso unas de valores sumamente elevados.

8. Recomendaciones

[1] Existen muchas soluciones que ofrecen alta disponibilidad de servicios pero hay que tener en cuenta que no todas se adaptan o son las adecuadas para nuestra infraestructura. Por tal razón siempre hay que analizar muy profundo de lo que se requiere hacer.

No necesariamente una empresa grande va a requerir una solución costosa que incluya beneficios que nunca serán usados.

[2] Es importante resaltar que un adecuado posicionamiento del IDS/IPS Snort en la red, influenciaría mucho para que realice mejor su trabajo teniendo una mayor eficiencia en la recuperación de fallas, eventos, alertas o posibles ataques.

[3] El alcance de alta disponibilidad no solo se limita a los servidores comprometidos, es recomendable que los elementos como switch's y routers a los que se encuentran conectados estos servidores también tengan alta disponibilidad. Ya que si solo se cuenta con un solo switch la alta disponibilidad entre los servidores pierde su efectividad cuando suceda algún fallo en dicho switch.

[4] Se recomienda instalar todas las dependencias necesarias para no tener problemas con la instalación y la configuración de las herramientas basadas en software.

9. Referencias

[1] Sitio oficial de Snort, http://www.snort.org/, Agosto del 2010.

[2] IDS / IPS, http://www.kineticsl.com/html/idsips.html, Agosto del 2010.

[3] Sistemas de Detección de intrusos y Snort, http://www.maestrosdelweb.com/editorial/snort/, Agosto del 2010.

[4] Alta disponibilidad con heartbeat, http://blogs.ua.es/labseps/2010/07/13/alta-disponibilidad-con-heartbeat/, Agosto del 2010.

[5] Sitio oficial de DRBD, http://www.drbd.org/home/what-is-drbd/, Agosto del 2010.

[6] DRBD how to Red Hat / Centos, http://www.adminso.es/wiki/images/3/31/Pfc_Fransico_cap4.pdf, Agosto del 2010.

[7] DRBD how to Red Hat / Centos, http://wiki.itlinux.cl/doku.php?id=cluster:drbd, Febrero del 2011.

[8] Instalar y configurar monit para Linux, http://agarzon.php.com.ve/instalar-y-configurar-monit-para-linux/, Mayo del 2011.

[9] Acoplamiento de tarjetas de red (bonding), http://blogofsysadmins.com/como-configurar-acoplamiento-de-tarjetas-de-red-bonding, Junio del 2011.