Solución de Firewall con Alta Disponibilidad para Redes Corporativas Utilizando Vyatta con Virtualización

Felipe Andrés Ordóñez Galiano
Departamento de Eléctrica Electrónica, Escuela Politécnica del Ejército
Sangolquí, Ecuador
firoos@hotmail.com

***Prólogo*— Este proyecto analiza el desempeño de Vyatta que es un firewall, router y dispositivo de borde, en una configuración de alta disponibilidad por tanto tolerante a fallos, implementado en una plataforma virtual intentando usar los mínimos recursos físicos.**

I. Introducción

En la actualidad las redes de datos se han convertido en uno de los puntos más relevantes para el desarrollo de una organización, de tal manera que la misma debe tener grandes capacidades de desempeño y funcionalidad, debe ser tolerante a fallos como también tener sistemas de seguridad para mantenerla protegida de intrusos, ataques, etc.

Existen diversas soluciones para hacer que una red de datos este protegida, una de estas es usando un firewall, que es un sistema diseñado para permitir o denegar el paso de paquetes a través de la red de datos, dicho de diferente forma, es un sistema que delimita la conexión entre dos redes, limitar, cifrar, descifrar, el tráfico entre diferentes ámbitos sobre la base de un conjunto de normas y criterios.

II. Conceptos

A. Alta Disponibilidad

La alta disponibilidad es un protocolo o sistema diseñado que asegura un cierto grado absoluto de continuidad operacional durante un periodo de medición dado. Consiste en una serie de medidas tendientes a garantizar la disponibilidad del servicio. [1]

B. Virtualización

La virtualización es una técnica usada para crear una versión virtual de algún recurso tecnológico, como una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento u otros recursos de red. [2]

La virtualización permite crear sistemas más reactivos o de alta disponibilidad, ya que el servidor virtual no es más que un archivo en comparación con un equipo físico, entonces puede ser desplegado fácilmente de un servidor físico a otro servidor físico, el tiempo de no disponibilidad es de algunos minutos y se comienza de nuevo con un servidor idéntico al que acaba de caer, algunos sistemas de virtualización permiten el cambio en caliente, esto quiere decir que no existirá el periodo de no disponibilidad por tanto los datos o bien las configuraciones estarán siempre actualizadas en las distintas máquinas virtuales. [3]

C. Vyatta

Es una organización que provee software base para routers, firewall y VPN que trabajan con protocolo IPv4 e IPv6. El sistema está basado en Debian, que es una distribución de Linux con aplicaciones de red como Quagga, Open VPN entre otras. La intención de la organización es desarrollar software que pueda reemplazar sistemas operativos Cisco, con un gran énfasis en el costo y la flexibilidad por el hecho de ser una fuente libre. Los sistemas que provee la organización son basados en Linux y corren muy establemente en arquitecturas con hardware x86 o bien en máquinas virtuales Xen o VMware. Vyatta también provee una guía de reemplazo Cisco que puede ser descargada de su página web, misma que muestra varios de los productos cisco y la solución comparable con Vyatta/x86. [4]

III. Topología de Red, Servicios y Funcionalidades a Implementar

A. Estrategia de Diseño de la Red Corporativa

La estrategia que se usó para el diseño de la red corporativa persigue las siguientes características:

- Ancho de banda compartido para la mayoría de usuarios.
- Un switch central como backbone.
- Nivel de tolerancia a fallos intermedio.
- Mínima administración.
- Crecimiento de la red.

B. Servicios dentro de la Red Corporativa

Esta red corporativa se diseñara con los siguientes requerimientos típicos:

- Conectividad a 50 usuarios a la red.
- Conectividad para 10 impresoras.
- Servicio de base de datos y transferencia de archivos.
- Servicio de email dentro de la compañía.
- Conexión a internet.
- Servicio web.
- Seguridad de red.

C. Conectividad dentro de la Red Corporativa

El diseño de la conectividad es relativamente simple, es básicamente un switchbackbone de acceso compartido con el escritorio. El objetivo es un diseño bajo en costo y que se adapte a expansiones futuras. [5]

El cableado típicamente será de categoría 5 UTP, concentrado en un cuarto de computadores o zona desmilitarizada, donde también se alojaran los servidores. Las impresoras normalmente estarán colocadas cerca de los usuarios de las mismas.

Existirán dos grupos de usuarios los de poder y los de no poder. El grupo de poder tenderá a realizar bastantes impresiones, descargar grandes archivos del servidor o guardarlos en el mismo, usan tarjetas de red en sus PCs de 10/100 Mbps. El grupo de no poder realiza tareas como contestar llamadas telefónicas o asistir en tareas administrativas, usan la red más que nada para leer correo electrónico y algún tipo simple de procesamiento de palabras.

La red física que se implementó para poder perseguir los objetivos de este proyecto es la de la Figura 1 y la red lógica está distribuida tal como la Figura 2.

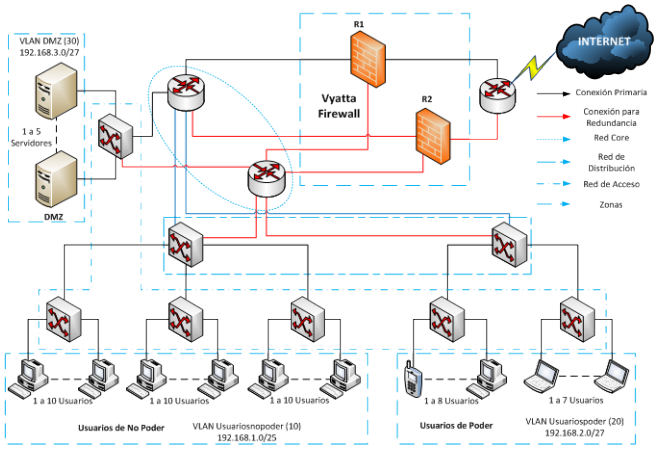

Fig. 1 Topología de la red física

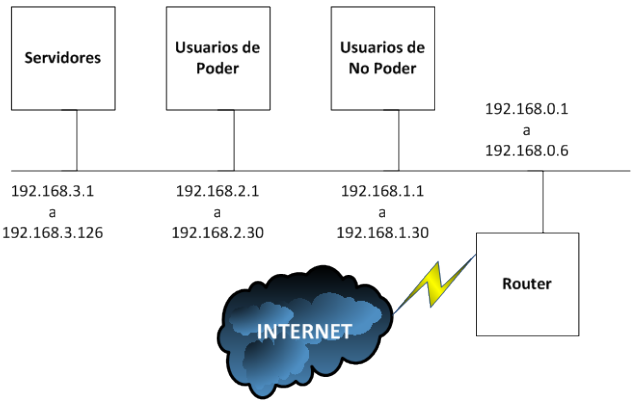

Fig. 2 Topología de la red lógica

IV. Tabulación, Analisis y Conclusiones de los DatosObtenidos en las Pruebas Realizadas en la Red Corporativa

A. DHCP y DNS

En el caso de las pruebas que se efectuaron para DHCP y DNS sólo se puede concluir que el servicio está funcionando adecuadamente y que los tiempos de respuesta son rápidos o bien están dentro de un rango aceptable.

B. Calidad de Servicio

Mediante la configuración que se propuso para las pruebas de calidad de servicio, el sistema Vyatta tenía que dividir el ancho de banda total en diferentes porcentajes para cada una de las zonas, el 15% del total para la zona de poder y el 80% para la zona DMZ, se debe aclarar que esta división es algo desproporcionada para un ambiente corporativo pero tan sólo ha sido tomada en cuenta para obtener resultados más visibles en las pruebas.

Por otra parte el ancho de banda total que se tomó en consideración para salida al internet es de 100Mbps, con esto podemos calcular los valores medios de ancho de banda para cada zona, en consecuencia, la zona de poder tendrá un ancho de banda aproximadamente de 80Mbps y la zona de no poder un ancho de banda de 15Mbps, también se debe tomar en consideración que idealmente el ancho de banda total será de 100Mbps pero existen pérdidas debido a equipos intermedios, cables de transmisión, conectores, etc, por lo que el ancho de banda real será menor, los anchos de banda quedarán repartidos en 80Mbps y 15Mbps.

Resumiendo los resultados obtenidos en las pruebas de calidad de servicio se obtuvo la Tabla I.

TABLA I

RESUMEN DE PRUEBAS DE CALIDAD DE SERVICIO EN UNA RED CON ANCHO DE BANDA DE 100Mbps

	Zona de Poder			Zona de no Poder		
	Teórico	Experimental	Error Porcentual	Teórico	Experimental	Error Porcentual
TCP Descarga de Datos Media	80	33,6	58	15	6,35	57,67

Teniendo en cuenta que el ancho de banda medio de la red es de 60Mbps y por tanto el ancho de banda para la zona DMZ sería de 48Mbps y de 9Mbps para la zona de poder, entonces se recalculan estos errores y se obtiene la Tabla II.

TABLA II

RESUMEN DE PRUEBAS DE CALIDAD DE SERVICIO EN UNA RED CON ANCHO DE BANDA DE 60Mbs

	Zona de Poder			Zona de no Poder		
	Teórico	Experimental	Error Porcentual	Teórico	Experimental	Error Porcentual
TCP Descarga de Datos Media	48	33,6	30	9	6,35	29,44

Del análisis de estos resultados se puede concluir que la calidad de servicio implementado mediante división del ancho de banda por zonas es adecuada, pero no tan precisa como se esperaba debido a los errores mayores al 10%.

C. Desempeño de La Red

Las primeras pruebas que se ejecutaron para probar el desempeño de la red están basadas en una comparación entre una conexión intranet y una conexión internet, El resumen de los datos obtenidos en estas pruebas se presentan en la Tabla III.

TABLA III

TABULACIÓN DE DATOS DE LAS PRUEBAS REALIZADAS CON CONEXIONES HACIA INTRANET E INTERNET

Conexiones Desde Zona de Poder			
Hacia el Sistema Vyatta		Hacia www.google.com	
Ancho de Banda (Mbps)	RTT (mseg)	Ancho de Banda (Mbps)	RTT (mseg)
46,5	0,78	0,2047	129

Lógicamente la velocidad de conectividad o el ancho de banda interno es mucho más rápido que una conexión hacia un servidor en el internet, esta prueba tan sólo nos da una idea del verdadero ancho de banda que se está manejando dentro y fuera de la red.

En la Tabla IV se encuentran tabulados los datos obtenidos en las pruebas de desempeño de la red local, en el instante que los clientes de la zona de poder y de la zona de no poder se conectaron hacia el servidor de la zona DMZ.

TABLA IV

TABULACIÓN DE DATOS DE LAS PRUEBAS REALIZADAS CON 4SERVICIOS EN LA ZONA DMZ Y CON CONEXIONES DESDE LA ZONA DE PODER Y NO PODER

	Conexiones Hacia DMZ					
	Zona de Poder			Zona de no Poder		
	TCP	UDP	UDP perdido	TCP	UDP	UDP perdido
	Puerto 20 (Mejor Esfuerzo)			Puerto 3650 (AudioVideo)		
Subida (Mbps)	44,12	64,05	1,40%	35,27	63,03	1,10%
Bajada (Mbps)	38,11	73,11	45,80%	37,76	0	100%
	Puerto 80 (Mejor Esfuerzo)			Puerto 3651 (Voz)		
Subida (Mbps)	37,39	62,58	0,20%	45,48	73,07	0,60%
Bajada (Mbps)	46,08	58,97	7,30%	52,75	57,37	10,30%

Es necesario recalcar que en esta prueba las conexiones fueron simultaneas y debido a esto el ancho de banda fue dividido, por tal razón la diferencia del ancho de banda real entre esta prueba al de las siguientes es bastante grande en el caso del tráfico TCP ya que este siendo un protocolo controlado necesita inyectar más paquetes a la red para dicho control, la diferencia que se puede apreciar entre los datos obtenidos en la Tabla *.* y la Tabla *.* en el caso de TCP es de casi el doble, también hay que considerar que el tipo de paquetes TCP que se estaban manejando son BestEffort, esto quiere decir que no se está usando algún tipo de calidad de servicio, también implica que no existe una preasignación de recursos, ni plazos conocidos, ni garantía de recepción correcta de la información, al momento de enviar paquetes TCP que implican calidad de servicio como en la conexión entre la zona de no poder y la zona DMZ en las que se envían paquetes de audiovideo y de voz, el ancho de banda usado por estos clientes disminuye en relación a los que no usan calidad de servicio, estos datos se pueden apreciar relacionando los resultados tabulados en la Tabla V y los de la Tabla VI.

Como conclusión se puede notar claramente que la interferencia en ancho de banda que Vyatta produce al intercomunicar las distintas zonas de nuestra topología proyecto es mínima.

En la Tabla V se presenta la tabulación de los datos obtenidos en las pruebas cuando sólo existía conexión desde la zona de poder hacia la zona DMZ, y en la Tabla VI están los datos obtenidos cuando sólo existía conexiones desde la zona de no poder hacia la zona DMZ.

TABLA V

TABULACIÓN DE DATOS DE LAS PRUEBAS REALIZADAS CON 2CONEXIONES DESDE LA ZONA DE PODER HACIA LA ZONA DMZ

	Zona de Poder		
	TCP	UDP	UDP perdido
	Puerto 20 (Mejor Esfuerzo)		
Subida (Mbps)	80,61	87,94	0,70%
Bajada (Mbps)	68,93	78,62	11,00%
	Puerto 80 (Mejor Esfuerzo)		
Subida (Mbps)	60,36	84,81	0,60%
Bajada (Mbps)	80,15	78,09	10,10%

TABLA VI

TABULACIÓN DE DATOS DE LAS PRUEBAS REALIZADAS CON 2CONEXIONES DESDE LA ZONA DE NO PODER HACIA LA ZONA DMZ

	Zona de no Poder		
	TCP	UDP	UDP perdido
	Puerto 3650 (AudioVideo)		
Subida (Mbps)	41,97	66,05	0,00%
Bajada (Mbps)	47,84	0	100%
	Puerto 3651 (Voz)		
Subida (Mbps)	47,73	73,72	0,30%
Bajada (Mbps)	56,7	60,84	32,20%

D. Redundancia y Alta Disponibilidad

Lamentablemente no se pudo probar la sincronización del sistema debido a que este proyecto sólo utiliza la versión de distribución libre, la sincronización sólo puede ser implementada comprando alguno de los paquetes que ofrece la compañía Vyatta.

El sistema de redundancia funcionó eficazmente, mediante las pruebas realizadas se pudo ver en las distintas capturas de paquetes el funcionamiento del protocolo VRRP, mismo que se está difundiendo en la red durante espacios de tiempo, este paquete lleva consigo información de la prioridad del sistema en este caso el sistema master tiene una prioridad de 150 y el de respaldo una prioridad de 100, los paquetes capturados demuestran que en el momento en que el sistema de respaldo deja de percibir los paquetes VRRP del sistema master, este sistema de respaldo se pone al mando de la red, es posible detectar este funcionamiento viendo que justo en el momento en que el sistema de respaldo se alza como primario aparecen paquetes VRRP difundiéndose por la red, obviamente detallando su prioridad.

Los tiempos que se necesita para levantar al sistema redundante cuando el master deja de funcionar son detallados en la Tabla VII, estos valores han sido tabulados de las pruebas respectivas a redundancia y alta disponibilidad del capítulo iv. Dichos tiempos son relativamente pequeños por tanto el sistema se vuelve estable rápidamente.

TABLA VII

TIEMPOS DE LEVANTAMIENTO DEL SISTEMA DE REDUNDANCIA

	Tiempo de Levantamiento del Sistema Prioritario	
	Slave como Primario	Master
Ping al Sistema Vyatta (mseg)	0,652	1,342
Ping a Dirección de Internet 8.8.8.8 (mseg)	97,13	306,392

V RECOMENDACIONES

Es favorable analizar de manera adecuada toda la topología de red física como lógica que se desea implementar antes de empezar con la configuración del sistema Vyatta, así se podrá obtener resultados robustos y velozmente.

Se debe tener muy en cuenta que si se desea implementar Vyatta dentro de una máquina virtual, entonces se debe escoger de manera adecuada el servidor donde esta será instalada, Vyatta presenta distribuciones que son más funcionales con máquinas virtuales de primer nivel como VMwareESXi, XenServer, etc. El problema se presenta cuando estas máquinas virtuales deben ser instaladas en el servidor ya que no todos los procesadores son compatibles con ellas, así como la tarjeta madre del servidor o las tarjetas de red, debido a esto entonces es necesario hacer un estudio antes de instalar la máquina virtual y Vyatta sobre ella.

Dentro de la página de VMware (www.vmware.com) existe una sección donde se detalla los distintos procesadores, tarjetas madre, tarjetas de red, etc, compatibles con VMwareESXi.

Hay que tomar muy en cuenta, que si se desea instalar este sistema dentro de una red corporativa, debe existir una persona que este encargada de su instalación y mantenimiento, en caso de que se desee obviar personal entonces se puede comprar las licencias que son distribuidas por la organización Vyatta, estas incluyen soporte, almacenamiento virtual extendido, clases de entrenamiento en línea, soporte telefónico y acuerdos del nivel de servicio, todas estas características de la licencia varían de acuerdo al tipo de plan contratado.

Existe también la posibilidad de que dentro de nuestro entorno corporativo de alta disponibilidad y tolerante a fallos, sean necesarias características en el sistema Vyatta como la sincronización de los distintos sistemas levantados o bien un entorno gráfico para un manejo más amigable y rápido del sistema, en este caso será necesario adquirir una licencia ya que con el programa de uso libre no están incorporadas estas características.

REFERENCIAS

- [1] (2012) Wikipedia sitio web. [Online]. Disponible: http://es.wikipedia.org/wiki/Alta_disponibilidad
- [2] (2012) Omicrono sitio web. [Online]. Disponible: http://www.omicrono.com/2011/11/las-mejores-herramientas-de-virtualizacion-vmware-virtualbox-y-virtualpc/
- [3] Recursos InformáticosWindows Server 2008 – Administración y Explotación, Autor Philippe FREDDI, Editorial ENI
- [4] (2012) Openredessitio web. [Online]. Disponible: http://www.openredes.com/wp-content/uploads/2011/10/Evento-Vyatta.pdf, página 3.
- [5] IBM, High Availability Solution for IBM FileNet P8 Systems, ibm.com/redbooks, Agosto 2009, 4 de Mayo de 2012