ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

INFORME DE MATERIA DE GRADUACIÓN

"MONITOREO Y ADMINITRACION DE MAQUINAS VIRTUALES A TRAVES DE ENLACES WAN"

Previa a la obtención del Título de:

LICENCIADO EN REDES Y SISTEMAS OPERATIVOS

Presentada por

GALO ERNESTO NARVAEZ ZAMBRANO

JOSE LUIS ZAMBRANO PINTO

Guayaquil - Ecuador

2012

TRIBUNAL DE SUSTENTACIÓN

_____

Rayner Stalyn Durango Espinoza

PROFESOR DE LA MATERIA DE GRADUACIÓN

_____

Guiseppe Blacio Abad

PROFESOR DELEGADO POR EL DECANO DE LA FACULTAD

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Trabajo de Grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral"

_____

Galo Ernesto Narváez Zambrano

_____

Jose Luis Zambrano Pinto

RESUMEN

La presente investigación, consiste en la implementación de un Sistemas de monitoreo y administración de máquinas virtuales a través de enlaces WAN, que una vez realizada, permitió demostrar que es posible administrar y monitorear un sistema virtualizado con alta disponibilidad, mediante el uso de varias herramientas propias del sistema Operativo.

Estas herramientas nos permitirán generar indicadores de rendimiento con los cuales analizaremos el comportamiento de nuestra plataforma y los diferentes servicios que brinda estando estos dentro de equipos virtualizados.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

INTRODUCCIÓN

Toda empresa privada tiene un fin lucrativo por lo que es importante implementar herramientas de bajo costo que le permitan cumplir con sus estándares de calidad.

Cuando se habla de una empresa, se toman en cuenta productos tangibles e intangibles cuya calidad podrá ser medida y valorada por la satisfacción del cliente.

Debido a estos factores nace la necesidad de crecimiento continuo de las organizaciones lo que conlleva también a la adquisición constante de hardware para sus servidores de producción, por este motivo se ha planteado una solución de “VIRTUALIZACIÓN” el cual permite a las organizaciones la escalabilidad en el tiempo y las necesidad de adquirir un nuevo hardware cada vez que se requiera asignar mayor cantidad de recursos a un servidor.

Siendo Windows Server 2008 una herramienta propietaria de Microsoft, se puede realizar la implementación de un módulo de “VIRTUALIZACIÓN” denominado “HYPER-V” el cual se encuentra disponible en el “WEBSITE” de Microsoft, para cumplir así con las necesidades de la empresa a un bajo costo para la misma.

CAPÍTULO 1

1 ANTECEDENTES Y JUSTIFICACIÓN

1.1 ANTECEDENTES

Actualmente, la decisión de un cliente no solo se basa en la publicidad que una empresa le dé a su producto o servicio, sino también en cómo esta empresa brinda soluciones en tiempo real a través de las diferentes tecnologías de comunicación que juegan un papel muy importante en el mundo competitivo de hoy.

Es por esta razón que la "VIRTUALIZACIÓN" otorga una solución de servidores, el cual mediante un esquema adecuado de contingencia pueden brindar una funcionalidad que esté disponible 24x7, con un tiempo de respuesta óptimo. Beneficiando no solo al usuario final, sino también a la empresa que tendrá la oportunidad de poseer un servicio con alta disponibilidad.

En el transcurso de los últimos años, se han desarrollado herramientas o tecnologías que ayudan al mejor desempeño de una infraestructura basada en compartir recursos de hardware a varios sistemas operativos "GUEST" alojados dentro de un mismo sistema operativo principal ("HOST") para ello debe existir una comunicación previa entre ambos, y esta comunicación se rige a través de ciertos parámetros que, bajo su cumplimiento, permiten dicha

comunicación. Esta premisa originó la idea del proyecto "Administración y monitoreo de servidores virtualizados a través de enlaces “WAN” es decir que desde cualquier lugar de internet puedan estos servidores ser gestionados por el personal de “IT”.

La integración de estas tecnologías permite que la solución sea modular, al poder aumentar o disminuir las características en función a los requerimientos de la empresa. Este proyecto se basa en satisfacer todos estos puntos dando como resultado una solución escalable, flexible y a bajo costo.

1.2 JUSTIFICACIÓN

Debido a la demanda de las empresas por adquirir una solución de “VIRTUALIZACIÓN” con características de alto rendimiento y teniendo en mente permitir la versatilidad para implementar diferentes sistemas operativos siendo usuario final el más beneficiado por dicha solución, nace la necesidad de desarrollar un ambiente de alta disponibilidad que también permita ajustarse al continuo crecimiento de la empresa.

El proceso de elección del “SOFTWARE” de “VIRTUALIZACIÓN” adecuado para nuestro proyecto de "Administración y monitoreo de servidores virtualizados a través de enlaces WAN” se basó en el siguiente análisis considerando ventajas de cada una de ellas.

“HYPER-V” proporciona capacidades de migración como la migración en vivo que se incluye en “WINDOWS SERVER 2008 R2” sin costo adicional. Con

“VMWARE”, “VMOTION” de “VMWARE”, tanto en la “FUNDATIÓN” y de las ediciones “STANDARD”, hay un cargo adicional al agregar estas capacidades de migración además el licenciamiento de “VMWARE” y “XEN SERVER” es por procesador algo que no ocurre con “HYPER V”

La siguiente tabla compara las principales características de “VMWARE ENTERPRISE” con “MICROSOFT WINDOWS SERVER 2008 HYPER-V (R2)” y Sistema de Gestión de Centro de características básicas.

Característica	VMware VI Empresa	Microsoft WS08 Hyper-V R2/SMSE
Hipervisor bare-metal	ESX / ESXi	Hyper-V
Centralizado de gestión de hipervisor	Centro Virtual	SMSE (VMM)
VMware y la gestión de Microsoft	Ninguno	SMSE (VMM)
VM copia de seguridad	VCB (proxy solamente)	SMSE (DPM)
Alta disponibilidad de la VM / conmutación por error	Centro Virtual	WS08 Clustering
VM migración	VMotion	Migración en vivo
Storage VMotion	Sí	Todavía no
SO invitado parches / gestión	Sí	SMSE (SCCM)
Fin-a-extremo SO de monitoreo	Ninguno	SMSE (Ops Mgr)
Anfitrión / optimización de máquinas virtuales de nivel	DRS	SMSE (PRO)
Aplicación / servicio de vigilancia	Ninguno	SMSE (PRO)
Gestión física y virtual integrada	Ninguno	SMSE

El enfoque adoptado por “XEN SERVER”, que utiliza en sus productos es tener una capa de virtualización extremadamente delgada entre el hardware físico y sistema operativo “GUEST”, y hacer lo mínimo necesario para permitir que los “HOST” que se ejecute con seguridad juntos en un sistema. El Rendimiento sigue siendo un elemento diferenciador en particular cuando se desea la consolidación extrema, o cuando las aplicaciones son particularmente exigentes.

Esta tecnología permite que sistemas operativos sin modificar actúen como hosts dentro de las máquinas virtuales de “XEN SERVER”, siempre y cuando el servidor físico soporte las extensiones “VT” de “INTEL” o “PACIFIC” de “AMD” debido a ello nos exige usar un modelo especifico de hardware

Con “MICROSOFT”, la virtualización con “HYPER-V” fue construido en “WINDOWS SERVER 2008”. Para grandes plataformas de “MICROSOFT”, esto significa una mayor integración con su infraestructura existente y las herramientas de gestión. Dado que la tecnología “HYPER-V” es parte de “WINDOWS SERVER 2008”, al estar basado en este sistema Operativo puede ejecutar muy bien cualquier configuración de “HARDWARE”, ya que cualquier configuración de “HARDWARE” que está diseñado para soportar

Windows. Sólo puede ejecutar “VMWARE” y “XEN SERVER” en docenas o tal vez un menor número de configuraciones de servidor que puede ejecutar “WINDOWS”. Esto significa que la tecnología “HYPER-V” se puede ejecutar en cientos y cientos, de configuraciones por ello podríamos decir que “XEN SERVER” Y “ESX VMWARE” son productos más limitados en este ámbito.

MICROSOFT, acaba de actualizar el número de núcleos que se pueden ejecutar con HYPER-V por la liberación de soporte para el nuevo procesador Intel de 6 núcleos de AMD, lo que significa que ahora se ejecutan hasta 24 NÚCLEOS sin problema alguno y sin licenciamiento adicional.

1.3 DESCRIPCIÓN DEL PROYECTO

1.3.1 OBJETIVO GENERAL

Implementar un entorno de servidores virtualizados que a través de una correcta gestión se brinde un servicio óptimo mediante una administración y monitoreo de los equipos por medio de un enlace “WAN” por medio de una conexión tipo “VPN”.

1.3.2 OBJETIVOS ESPECÍFICOS

- Implementar servidores virtualizados bajo “HYPER V”

- Monitorear y administrar las diferentes plataformas virtualizadas a través de un enlace “WAN”
- Analizar y medir el rendimiento de los servidores por medio de indicadores de monitoreo propietarias o de terceros.

El proyecto consiste en implementar una solución de “VIRTUALIZACIÓN”, mediante el uso de “HYPER V” herramienta de “VIRTUALIZACIÓN” Microsoft. Se usará un equipo que va a cumplir las Servidor de “VIRTUALIZACIÓN” sistema operativo “HOST” para que este administre e interactúe a con los sistemas operativos “GUEST” y posterior a ello a través de una enlace “WAN” “VPN” podamos desde cualquier parte administrar nuestro equipos virtuales de manera remota.

Gracias a este diseño nos aseguramos de brindar una alta administración y monitoreo remoto de la nuestros servidores virtualizados.

La conexión con la “WAN” se valdrá de un servidor “VPN” mediante el cual garantizaremos una conexión segura en todo momento al establecer el enlace para administrar nuestros recursos y se puede llevar un control más eficiente del servicio brindado.

1.4 METODOLOGÍA

Se utilizarán tres equipos físicos, uno será el servidor de “VIRTUALIZACIÓN” en el cual estará instalado Windows server 2008 de 64bits, los otros dos serán un “ROUTER” cisco 1811.

El cual será nuestro servidor “VPN” y por ultimo un equipo portátil en el cual será el cliente que se conectara a la “VPN” y con el cual podremos administrar y monitorear nuestros servidores. El diseño se muestra en al siguiente gráfica

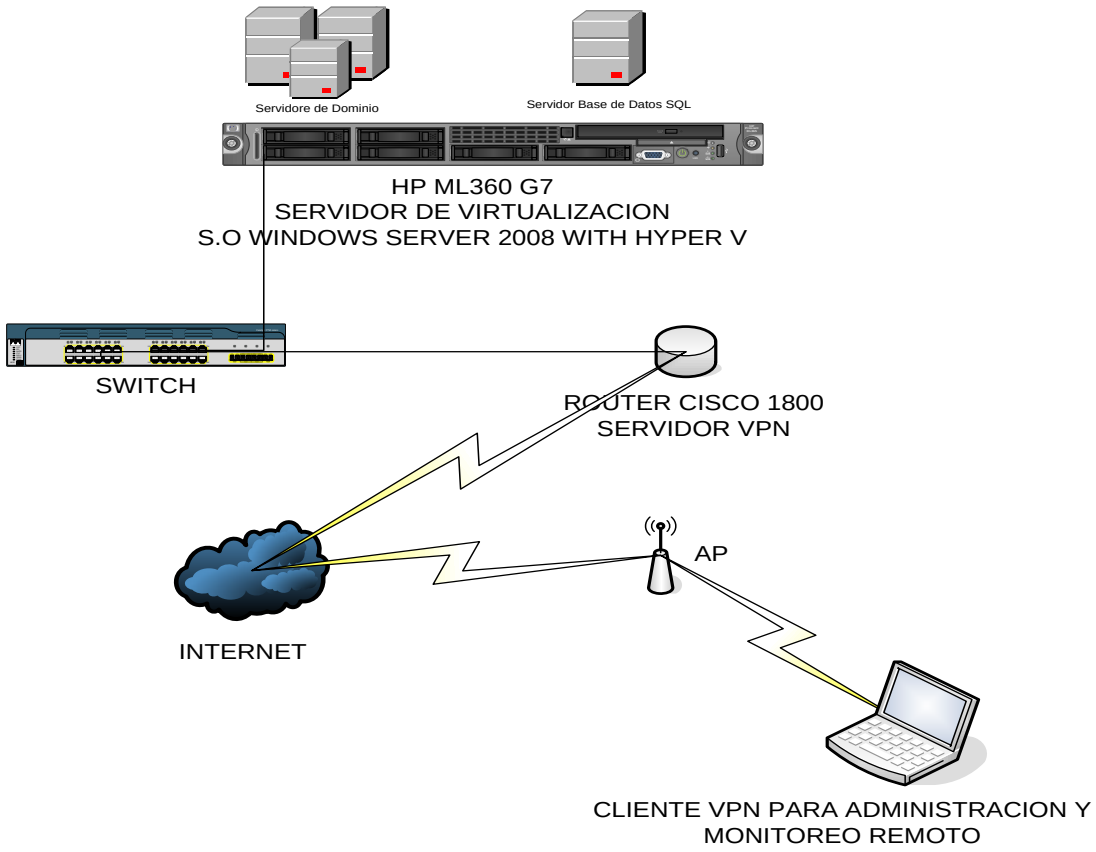


FIG 1 DISENO DE PROYECTO

CAPÍTULO 2

2 HERRAMIENTAS

2.1 VIRTUALIZACION Y HYPER V

2.1.1 INTRODUCCION.

2.1.1.1 MODELO VIRTUALIZACION

En Informática, “VIRTUALIZACIÓN” se refiere a la abstracción de los recursos de una computadora, llamada “HYPERVISOR” o “VMM” (“VIRTUAL MACHINE MONITOR”) que crea una capa de abstracción entre el hardware de la máquina física (“HOST”) y el sistema operativo de la “VM” (“VIRTUAL MACHINE”, “GUEST”), siendo un medio para crear una versión virtual de un dispositivo o recurso, como un servidor, un dispositivo de almacenamiento, una red o incluso un sistema operativo, donde se divide el recurso en uno o más entornos de ejecución.

Esta capa de software (“VMM”) maneja, gestiona y arbitra los cuatro recursos principales de una computadora (“CPU”, Memoria, Red, Almacenamiento) y así podrá repartir dinámicamente dichos recursos entre todas las máquinas

virtuales definidas en el computador central. De modo que nos permite tener varios ordenadores virtuales ejecutándose sobre el mismo ordenador físico.
Tal término es antiguo; se viene usando desde 1960, y ha sido aplicado a diferentes aspectos y ámbitos de la informática, desde sistemas computacionales completos, hasta capacidades o componentes individuales. Lo más importante en este tema de “VIRTUALIZACIÓN” es la de ocultar detalles técnicos a través de la encapsulación.

La “VIRTUALIZACIÓN” se encarga de crear una interfaz externa que esconde una implementación subyacente mediante la combinación de recursos en localizaciones físicas diferentes, o por medio de la simplificación del sistema de control. Un avanzado desarrollo de nuevas plataformas y tecnologías de “VIRTUALIZACIÓN” han hecho que se vuelva a prestar atención a este importante concepto. De modo similar al uso de términos como “abstracción” y “orientación a objetos”, “VIRTUALIZACIÓN” es usado en muchos contextos diferentes.

La máquina virtual en general es un sistema operativo completo que corre como si estuviera instalado en una plataforma de hardware autónoma. Típicamente muchas máquinas virtuales son simuladas en un computador central. Para que el sistema operativo “GUEST” funcione, la simulación debe ser lo suficientemente grande (siempre dependiendo del tipo de “VIRTUALIZACIÓN”).

FIG. 2 MODELO DE VIRTUALIZACION

2.1.1.2 ¿QUÉ ES “VIRTUALIZACIÓN”?

Se debe partir por la definición de virtual, que es lo virtual, según como se define “que tiene existencia aparente y no real” en su definición general aportada por la real academia española de la lengua además define en su terminología informática como “Representación de escenas o imágenes de objetos producida por un sistema informático, que da la sensación de su existencia real”.

Se puede definir como el procedimiento capaz de realizar una administración entre el hardware de un equipo y su sistema operativo mediante la creación de una versión virtual de lo que se está virtualizando (ya sea un disco, memoria, aplicación o un sistema operativo completo).

Una definición de “VIRTUALIZACIÓN” que se puede hacer referencia es una que se generaliza en la red en donde se describe a la “VIRTUALIZACIÓN” como el procedimiento de simular un sistema operativo dentro de otro haciendo

alusión por cierto a la “VIRTUALIZACIÓN” de sistemas operativos dejando fuera a otros tipos de “VIRTUALIZACIÓN” que se tratara más adelante por ejemplo de nivel 1 o tipo 1.

Las máquinas virtuales que emulan un sistema operativo completo crean memorias ‘’RAM”, discos duros procesadores, aplicaciones, de manera virtual permitiendo su traslado almacenamiento y restauración de manera más rápida que con sistemas físicos de trabajo.

2.1.1.3 ¿CÓMO FUNCIONA LA “VIRTUALIZACIÓN”?

Windows Server 2008 “HYPER-V” es la funcionalidad de “VIRTUALIZACIÓN” basada en el “HYPERVISOR”, incluida como un rol de servidor específico de Windows Server 2008. Contiene todo lo necesario para la puesta en servicio de escenarios de “VIRTUALIZACIÓN”. “HYPER-V” permite reducir costes, mejorar el nivel de utilización de los servidores y crear una infraestructura de “IT” más dinámica. El aumento de la flexibilidad que proporciona “HYPER-V” se debe a sus capacidades de plataforma dinámica, fiable y escalable combinadas con un conjunto exclusivo de herramientas de gestión que permiten administrar tanto los recursos físicos como los virtuales, lo que facilita la creación de un “DATACENTER ‘ ágil y dinámico y el avance hacia un modelo de sistemas dinámicos auto gestionados.

Aparte de “HYPER-V”, Microsoft también presenta el Microsoft “HYPER-V” Server. Microsoft “HYPER-V” Server es una solución de “VIRTUALIZACIÓN”

simplificada, fiable, económica y optimizada que permite reducir costes, mejorar el nivel de utilización de los servidores y aprovisionar rápidamente nuevos servidores. Microsoft “HYPER-V” Server se conecta con gran facilidad a las infraestructuras de IT de los clientes, aprovechando las actuales herramientas de gestión y el nivel de conocimientos de los profesionales de “IT” con el máximo nivel de soporte por parte de Microsoft y sus Partners.

2.1.2 VENTAJAS DE LA “VIRTUALIZACIÓN”

El modelo de “VIRTUALIZACIÓN” se utiliza por las siguientes razones:

- ✓ Rápida incorporación de nuevos recursos para los servidores virtualizados.
- ✓ Reducción de los costes de espacio y consumo necesario de forma proporcional al índice de consolidación logrado
- ✓ Administración global centralizada y simplificada.
- ✓ Nos permite gestionar nuestro “CPD” (Centro de Procesamiento de datos) como un pool de recursos o agrupación de toda la capacidad de procesamiento, memoria, red y almacenamiento disponible en nuestra infraestructura
- ✓ Mejora en los procesos de clonación y copia de sistemas: Mayor facilidad para la creación de entornos de test que permiten poner en marcha nuevas aplicaciones sin impactar a la producción, agilizando el proceso de las pruebas.
- ✓ Aislamiento: un fallo general de sistema de una máquina virtual no afecta al resto de máquinas virtuales.

- ✓ No sólo aporta el beneficio directo en la reducción del hardware necesario, sino también los costes asociados.
- ✓ Reduce los tiempos de parada.
- ✓ Migración en caliente de máquinas virtuales (sin pérdida de servicio) de un servidor físico a otro, eliminando la necesidad de paradas planificadas por mantenimiento de los servidores físicos.
- ✓ Balanceo dinámico de máquinas virtuales entre los servidores físicos que componen el pool de recursos, garantizando que cada máquina virtual ejecute en el servidor físico más adecuado y proporcionando un consumo de recursos homogéneo y óptimo en toda la infraestructura.
- ✓ Alto grado de satisfacción general.

2.1.2.1 MAQUINAS VIRTUALES

Las máquinas virtuales son una de las opciones de “VIRTUALIZACIÓN” existentes Una definición que se acerca bastante es la de “GOLDBERG” que la define como “un duplicado de hardware y software del sistema de computación real en el cual un subconjunto de instrucciones del procesador se ejecuta sobre el procesador anfitrión en modo nativo”.

Una característica esencial de las máquinas virtuales es que los procesos que ejecutan están limitados por los recursos y abstracciones proporcionados por ellas. Estos procesos no pueden escaparse de esta "computadora virtual".

2.1.2.2 EL VMM:

El “VIRTUAL MACHINE MANAGER” es la principal herramienta al momento de trabajar con una máquina virtual es el encargado de conectar el hardware con la máquina virtual.

Un “MMV” tiene tres características principales

1 Proporciona un ambiente de ejecución idéntico al de la máquina real.
2 El “MMV” debe tener acceso a los recursos, y posiblemente control, de los recursos del sistema real.
3 Un “MMV” es eficiente debido a que un gran porcentaje del conjunto de instrucciones del procesador virtual se ejecutan directamente en el procesador real, sin intervención del mismo.

El monitor de máquina virtual o “HYPERVISOR” puede ejecutarse directamente sobre el hardware o a través de un sistema operativo anfitrión, si se ejecuta directamente sobre el sistema operativo significa que estamos hablando de un monitor de máquina virtual del tipo I y si se ejecuta en un sistema operativo anfitrión, que hospeda al “HYPERVISOR” se habla de un monitor de máquina virtual del tipo II.

El monitor de máquina virtual es el encargado de realizar la gestión de recursos entre el hardware y el sistema operativo pudiendo trabajar en un sistema anfitrión (por ejemplo un Windows, Ubuntu.) o también con un sistema anfitrión que hace un nivel virtual y se hace cargo de este, este tipo de

“VIRTUALIZACIÓN” se llama ”PARAVIRTUALIZACIÓN”, permite al ““HYPERVISOR” ” gestionar directamente los recursos de hardware virtuales.

Existen 4 niveles de administración en la “CPU”, donde el ““HYPERVISOR” ” accede con un nivel de ejecución ring 0 permitiéndole así una comunicación directa con el hardware además de un nivel superior de ejecución sobre las máquinas virtuales hospedadas las cuales se ejecutan en un nivel ring 1

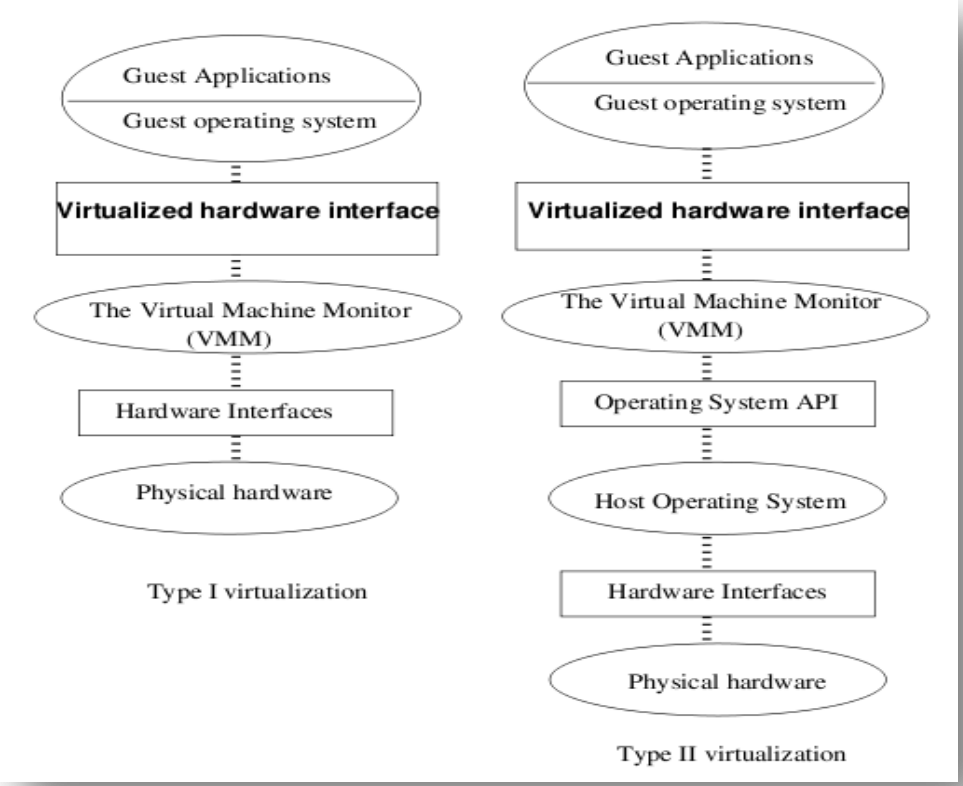


FIG. 3CAPAS DE LA VIRTUALIZACION

2.1.3 TIPO DE VIRTUALIZACION.

Es posible diferenciar los tipos de “VIRTUALIZACIÓN” además en 4 categorías donde, sobre la base de que se pueden clasificar en tipo I y II dependiendo si está corriendo el “HYPERVISOR” como huésped sobre otro sistema operativo o no se puede clasificar en “PARAVIRTUALIZACION”, full “VIRTUALIZACIÓN”, “VIRTUALIZACIÓN” de sistema operativo y “VIRTUALIZACIÓN” con asistencia de hardware o “VIRTUALIZACIÓN” nativa.

2.1.3.1 FULL “VIRTUALIZACIÓN”

Full “VIRTUALIZACIÓN” es la que permite a nuestro entorno virtualizado un acceso a cada uno de los dispositivos a través de una “VIRTUALIZACIÓN” de un sistema operativo “HOST” permitiendo así tener acceso a cada uno de los dispositivos virtualizados a través de conversiones binarias.

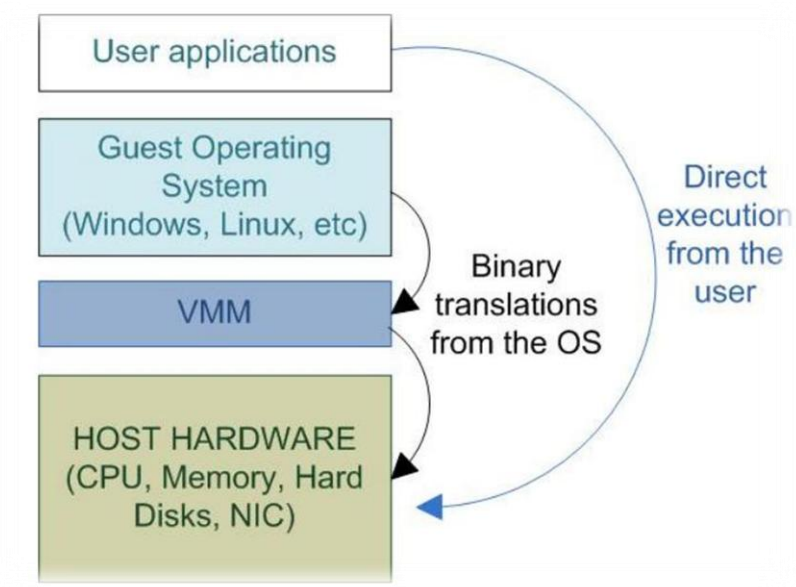


FIG. 4 METODOLOGIA 1

2.1.3.2 “VIRTUALIZACIÓN” CON ASISTENCIA DE HARDWARE

La “VIRTUALIZACIÓN” con asistencia de hardware o “VIRTUALIZACIÓN” nativa, requiere para su funcionamiento y en “VIRTUALIZACIÓN” de algunos dispositivos el uso de recursos del hardware o del procesador que vienen en las nuevas arquitecturas de diseño de hardware de AMD (AMD V) e Intel (Intel VT). Esta técnica puede ser utilizada junto con “PARAVIRTUALIZACION” o full “VIRTUALIZACIÓN” para obtener mejores resultados de rendimiento.

2.1.3.3 “VIRTUALIZACIÓN” DE SISTEMA OPERATIVO.

La “VIRTUALIZACIÓN” de sistema operativo corresponde a una “VIRTUALIZACIÓN” tipo I donde el sistema operativo levanta mediante software una máquina virtual sobre ella, este tipo de “VIRTUALIZACIÓN” es posible usarlo de manera nivel usuario pero tiene ciertos inconvenientes de uso de CPU

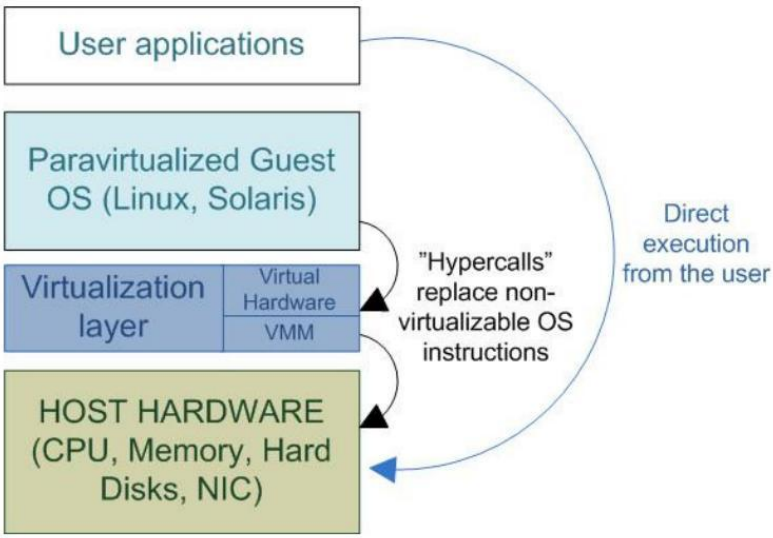


FIG. 5 METODOLOGIA 2

2.1.4 PARA"VIRTUALIZACIÓN"

La "PARAVIRTUALIZACION" permite al hardware hacer llamadas al hardware llamadas Hypercalls, en la "PARAVIRTUALIZACION" se simula un hardware virtual permitiendo menos modificaciones a nivel de "KERNEL" en el sistema operativo siendo todo administrado por el ""HYPERVISOR" " permitiendo así una mayor facilidad y compatibilidad de trabajo

2.1.4.1 CLASIFICANDO LA "VIRTUALIZACIÓN".

La "VIRTUALIZACIÓN" se puede clasificar según distintos tipos de vista, se clasificara para ser más específicos y para que se tenga en claro bajo que ámbitos está presente la "VIRTUALIZACIÓN", entonces bajo este criterio se le clasificare en:

- ✓ “VIRTUALIZACIÓN” de hardware.

- ✓ “VIRTUALIZACIÓN” de sistema operativo.

2.1.4.1.1 “VIRTUALIZACIÓN” DE HARDWARE:

La “VIRTUALIZACIÓN” de hardware corresponde a administrar la parte física de un servidor o equipo que contiene a la aplicación que esta virtualizando y ser capaz de generar todos estos dispositivos físicos (discos, memoria, procesador, etc.) a un entorno virtualizado, pudiendo así admitir por ejemplo varios equipos “HOST” ,la única implicancia de este tipo de “VIRTUALIZACIÓN” es que la memoria asignada a los equipos host es asignada de forma real así por ejemplo no se puede asignar más memoria a los equipos host de la que tiene el equipo físico.

2.1.4.1.2 “VIRTUALIZACIÓN” DE SISTEMAS OPERATIVOS:

Este tipo de “VIRTUALIZACIÓN” va de la mano con la “VIRTUALIZACIÓN” por hardware ya que el sistema operativo que se virtualiza se encuentra instalado sobre una plataformas virtualizadas de hardware, en el se emulan sistemas operativos ya sea corriendo sobre el “HYPERVISOR” o sobre un sistema operativo anfitrión.

Este tipo de “VIRTUALIZACIÓN” es muy ocupada en ambientes de desarrollo de software por ejemplo para realizar pruebas de compatibilidad de la

aplicación que se esté desarrollando pudiendo así el programador testear en distintos ambientes (Linux, Windows, Mac) un mismo programa logrando así obtener una amplia compatibilidad de lo contrario para realizar estas pruebas el programador debería cambiar de escritorio y contar con otros equipos con los otros sistemas operativos a testear.

2.2 VPN (VIRTUAL PRIVATE NETWORK)

2.2.1 INTRODUCCION VPN

Una “RED PRIVADA VIRTUAL” (“VPN”) es una red privada construida dentro de una infraestructura de red pública, así como lo es el Internet. Las empresas pueden usar redes privadas virtuales para conectar en forma segura oficinas y usuarios remotos a través de accesos a Internet económicos proporcionados por terceros, abaratando costos con la adquisición de enlaces “WAN”.

Las redes privadas virtuales proporcionan el mayor nivel posible de seguridad mediante seguridad “IP” (“IPSEC”) cifrada o túneles “VPN” de “SECURE SOCKETS LAYER” (“SSL”) y tecnologías de autenticación. Estas tecnologías protegen los datos que pasan por la red privada virtual contra accesos no autorizados. Las empresas pueden aprovechar la infraestructura estilo Internet de la red privada virtual, cuya sencillez de abastecimiento permite agregar rápidamente nuevos sitios o usuarios. También pueden aumentar

drásticamente el alcance de la red privada virtual sin expandir significativamente la infraestructura.

De esta forma podemos estar conectados a un bajo costo, con niveles elevados de seguridad, realizando tareas como si estuviéramos en su misma red local

2.2.2 ¿QUÉ ES UNA VPN?

Una “RED PRIVADA VIRTUAL” (“VIRTUAL PRIVATE NETWORK”) es una red privada que se extiende, mediante un proceso de encapsulación y en algún caso de cifrado, desde los paquetes de datos a diferentes puntos remotos, mediante el uso de infraestructuras públicas de transporte. Los paquetes de datos de la red privada viajan por un túnel definido en la red pública.

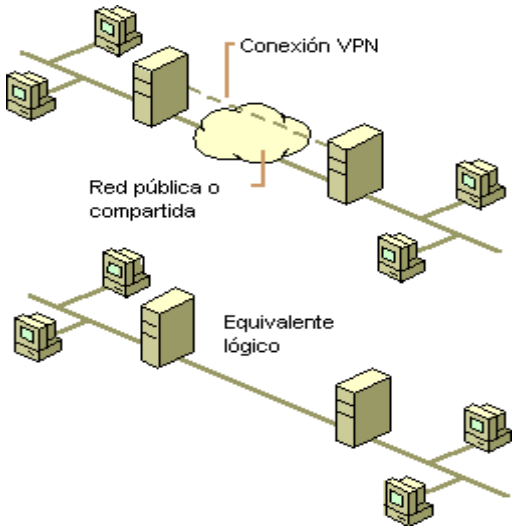


FIG. 6 EJEMPLO VPN

En el caso de acceso remoto, la “VPN” permite al usuario acceder a su red corporativa, asignando a su ordenador remoto las direcciones y privilegios de esta, aunque la conexión la haya realizado mediante un acceso público a Internet:

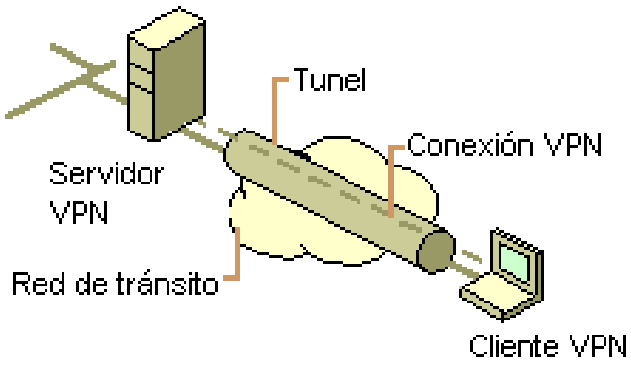


FIG. 7 TUNEL VPN

En ocasiones, puede ser interesante que la comunicación que viaja por el túnel establecido en la red pública vaya cifrada para permitir una confidencialidad mayor.

2.2.3 VENTAJAS DE UNA VPN

Una “RED PRIVADA VIRTUAL” VPN bien diseñada, puede dar muchos beneficios a una compañía. Algunas ventajas son:

- ✓ Extensión de conectividad a nivel geográfico
- ✓ Mejoras de seguridad
- ✓ Reduce costes al ser instalado frente a las redes “WAN” más utilizadas
- ✓ Mejora la productividad
- ✓ Simplifica la topología de red
- ✓ Proporciona oportunidades de comunicación adicionales

Las funciones que una red “VPN” debe incorporar son seguridad, fiabilidad, escalabilidad, gestión de red y políticas de gestión.

2.2.4 PROTOCOLOS DE TÚNEL

Los principales protocolos de túnel son:

- ✓ “PPTP” (Protocolo de túnel punto a punto) es un protocolo de capa 2 desarrollado por Microsoft, 3Com, Ascend, US Robotics y ECI Telematics.

- ✓ “L2F” (Reenvío de capa dos) es un protocolo de capa 2 desarrollado por Cisco, Northern Telecom y Shiva. Actualmente es casi obsoleto.
- ✓ “L2TP” (Protocolo de túnel de capa dos), el resultado del trabajo del “IETF” (“RFC” 2661), incluye todas las características de “PPTP” y “L2F2. Es un protocolo de capa 2 basado en “PPP”.
- ✓ “IPSEC” es un protocolo de capa 3 creado por el IETF que puede enviar datos cifrados para redes “IP”.

2.2.4.1 PROTOCOLO PPTP

El principio del “PPTP” (Protocolo de túnel punto a punto) consiste en crear tramas con el protocolo “PPP” y encapsularlas mediante un datagrama de “IP”.

Por lo tanto, con este tipo de conexión, los equipos remotos en dos redes de área local se conectan con una conexión de igual a igual (con un sistema de autenticación/cifrado) y el paquete se envía dentro de un datagrama de “IP”.

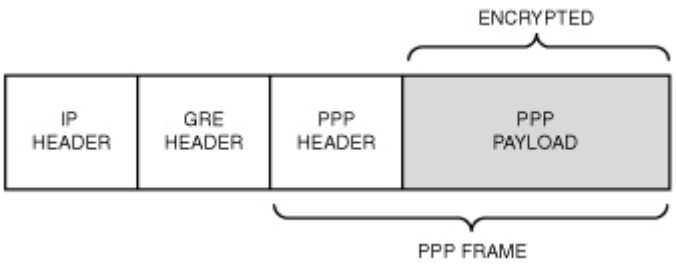


FIG. 8 ESTRUCTURA PAQUETE PPTP

De esta manera, los datos de la red de área local (así como las direcciones de los equipos que se encuentran en el encabezado del mensaje) se encapsulan

dentro de un mensaje “PPP”, que a su vez está encapsulado dentro de un mensaje “IP”.

2.2.4.2 PROTOCOLO L2TP

“L2TP” (Layer 2 Tunneling Protocol) fue diseñado por un grupo de trabajo de “IETF” como el heredero aparente de los protocolos “PPTP” y “L2F”, creado para corregir las deficiencias de estos protocolos y establecerse como un estándar aprobado por el “IETF” (“RFC” 2661). “L2TP” utiliza “PPP” para proporcionar acceso telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado. “L2TP” define su propio protocolo de establecimiento de túneles, basado en “L2F”. El transporte de “L2TP2 está definido para una gran variedad de tipos de paquete, incluyendo “X.25”, “FRAME RELAY” y “ATM”.

Al utilizar “PPP” para el establecimiento telefónico de enlaces, “L2TP” incluye los mecanismos de autenticación de “PPP”, “PAP” y “CHAP”. De forma similar a “PPTP”, soporta la utilización de estos protocolos de autenticación, como “RADIUS”.

- ✓ A pesar de que “L2TP” ofrece un acceso económico, con soporte multiprotocolo y acceso a redes de área local remotas, no presenta unas características criptográficas especialmente robustas. Por ejemplo:
- ✓ Sólo se realiza la operación de autenticación entre los puntos finales del túnel, pero no para cada uno de los paquetes que viajan por él. Esto puede dar lugar a suplantaciones de identidad en algún punto interior al túnel.

- ✓ Sin comprobación de la integridad de cada paquete, sería posible realizar un ataque de denegación del servicio por medio de mensajes falsos de control que den por acabado el túnel “L2TP” o la conexión “PPP” subyacente.

- ✓ “L2TP” no cifra en principio el tráfico de datos de usuario, lo cual puede dar problemas cuando sea importante mantener la confidencialidad de los datos.

- ✓ A pesar de que la información contenida en los paquetes “PPP” puede ser cifrada, este protocolo no dispone de mecanismos para generación automática de claves, o refresco automático de claves. Esto puede hacer que alguien que escuche en la red y descubra una única clave tenga acceso a todos los datos transmitidos.

.“L2TP” es en realidad una variación de un protocolo de encapsulamiento “IP”. Un túnel “L2TP” se crea encapsulando una trama “L2TP” en un paquete “UDP”, el cual es encapsulado a su vez en un paquete IP, cuyas direcciones de origen y destino definen los extremos del túnel. Siendo el protocolo de encapsulamiento más externo IP, los protocolos “IPSEC” pueden ser utilizados sobre este paquete, protegiendo así la información que se transporta por el túnel.

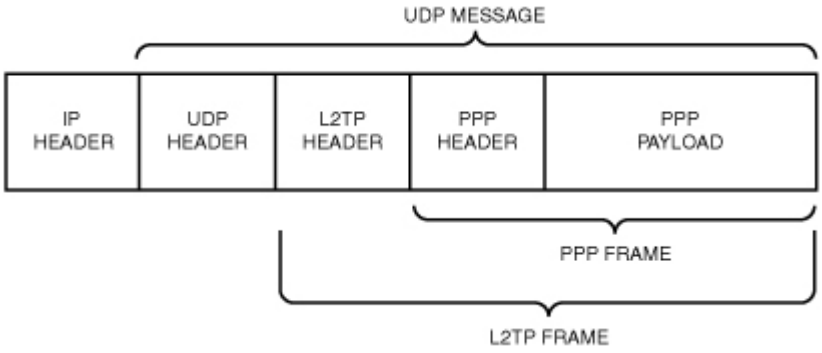


FIG. 9 STRUCTURE OF THE L2TP PACKET.

2.2.4.3 PROTOCOLO IPSEC

"IPSEC" es un protocolo definido por el "IETF" que se usa para transferir datos de manera segura en la capa de red. En realidad es un protocolo que mejora la seguridad del protocolo "IP" para garantizar la privacidad, integridad y autenticación de los datos enviados.

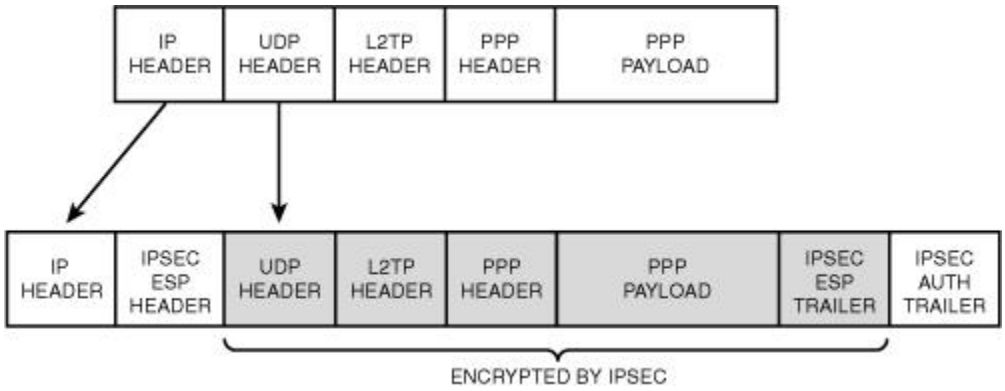


FIG. 10 STRUCTURE AND ARCHITECTURE OF THE IPSEC PACKET.

"IPSEC" se basa en tres módulos:

Encabezado de autenticación IP ("AH"), que incluye integridad, autenticación y protección contra ataques de replay a los paquetes.

Carga útil de seguridad encapsulada ("ESP"), que define el cifrado del paquete. "ESP" brinda privacidad, integridad, autenticación y protección contra ataques de replay.

Asociación de seguridad (SA) que define configuraciones de seguridad e intercambio clave. Las SA incluyen toda la información acerca de cómo procesar paquetes "IP" (los protocolos "AH" y/o "ESP", el modo de transporte o túnel, los algoritmos de seguridad utilizados por los protocolos, las claves utilizadas, etc.). El intercambio clave se realiza manualmente o con el protocolo de intercambio "IKE" (en la mayoría de los casos), lo que permite que ambas partes se escuchen entre sí.

2.2.5 TIPOS DE VPN

Básicamente existen tres arquitecturas de conexión “VPN”:

2.2.5.1 VPN DE ACCESO REMOTO

Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura “DIAL-UP” (módems y líneas telefónicas).

2.2.5.2 VPN PUNTO A PUNTO

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor “VPN”, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel “VPN”. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales (realizados comúnmente mediante conexiones de cable físicas entre los nodos), sobre todo en las comunicaciones internacionales. Es más común el siguiente punto, también llamado tecnología de túnel o tunneling.

2.2.5.3 **TUNNELING**

La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo un “PDU” determinada dentro de otra “PDU” con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la “PDU” encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser “SSH”.

El uso de esta técnica persigue diferentes objetivos, dependiendo del problema que se esté tratando, como por ejemplo la comunicación de islas en escenarios multicast, la redirección de tráfico, etc.

Uno de los ejemplos más claros de utilización de esta técnica consiste en la redirección de tráfico en escenarios “IP” Móvil. En escenarios de “IP” móvil, cuando un nodo-móvil no se encuentra en su red base, necesita que su home-agent realice ciertas funciones en su puesto, entre las que se encuentra la de capturar el tráfico dirigido al nodo-móvil y redirigirlo hacia él. Esa redirección del tráfico se realiza usando un mecanismo de tunneling, ya que es necesario que los paquetes conserven su estructura y contenido originales (dirección IP de origen y destino, puertos, etc.) cuando sean recibidos por el nodo-móvil.

2.2.5.4 VPN OVER LAN

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (“LAN”) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (“WIFI”).

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo “VPN”, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de recursos humanos habilitado pueda acceder a la información.

Otro ejemplo es la conexión a redes “WIFI” haciendo uso de túneles cifrados “IPSEC” o “SSL” que además de pasar por los métodos de autenticación tradicionales (“WEP”, “WPA”, direcciones “MAC”, etc.) agregan las credenciales de seguridad del túnel “VPN” creado en la “LAN” interna o externa.

2.3 SOFTWARE

2.3.1 CISCO VPN CLIENT.

FIG. 11 CLIENTE VPN

Cisco “VPN” Client le permite establecer túneles cifrados “VPN” de alta conectividad, remota y segura para sus empleados móviles o teleworkers. Es Simple de implementar y utilizar, nuestra seguridad IP (“IPSEC”) basada en “VPN” Client es compatible con todos los productos de “VPN” de Cisco. Cisco “VPN” Client pueden ser pre configurados para los despliegues en masa, y los inicios de sesión inicial requieren poca intervención del usuario.

2.3.1.1 SOPORTE VPN CLIENTE Y COMPATIBILIDAD.

El Cisco “VPN” Client es compatible con:

- ✓ Windows XP, Vista, 7 (x86/32-bt solamente)
- ✓ Windows x64 (64 bits) requiere AnyConnect Cisco VPN Client Linux (Intel)
- ✓ Mac OS X 10.4 y 10.5
- ✓ Solaris UltraSparc (32 y 64 bits)

El cliente “VPN” de Cisco se incluye con el “SA 5500 Series (excepto ASA 5505) y trabaja con los siguientes productos:

- ✓ Catalyst 6500 Series Series/7600 IPsec VPN Services Module y SPA “VPN” de Cisco IOS Software 12.2SX.
- ✓ Concentrador “VPN2 3000 Series Software Version 3.0 y superiores.
- ✓ Cisco IOS Software Release 12.2 (8) T y superiores.
- ✓ PIX Security Appliance Software versión 6.0 y superiores.
- ✓ ASA 5500 Series Software versión 7.0 o superior.

CAPÍTULO 3

3 IMPLEMENTACION

3.1 INTRODUCCION VIRTUALIZACION HYPER V

Al implementar el proyecto Monitoreo de Servidores virtualizados por a través de enlaces “WAN” mediante el uso de “HYPER-V”, demostraremos las bondades, capacidades y flexibilidad de este software, permitiéndonos cumplir con características propias de un sistema que cumple con los requerimientos de una infraestructura estable proveyendo, escalabilidad y confiabilidad.

Mediante la administración de recursos se brindara una solución al alcance de una pequeña o media empresa, con ahorros significativos, prescindiendo de la adquisición del Hardware cada ver que se requiera de una actualización del mismo, que en si conlleva grandes gastos.

Podremos acceder desde una conexión a internet tradicional para monitorear el los recurso y el rendimiento de nuestros servidores virtualizados adicionalmente esta conexión se realizara mediante un túnel de datos “VPN”.

3.1.1 HARDWARE

Para esta implementación en la parte del hardware se ha considerado la escalabilidad en el tiempo, para esto se ha utilizado equipos que cumplan con características de rendimiento óptimas. “HYPER-V” de Microsoft, por ser en si una plataforma que funciona sobre un sistema operativo Windows Server 2008, es implementado con equipos de características robustas ya que dentro de esta plataforma se virtualizarán servidores los cuales pueden crecer en su momento dado.

3.1.2 SERVIDORES

Servidor HP ProLiant DL360.

Para nuestra implementación utilizaremos HP ProLiant DL360 G7 que ha sido optimizado para instalaciones con limitaciones de espacio y combina potencia informática concentrada en espacio 1U, HP Insight Control y tolerancia a fallos esencial. Los últimos procesadores Intel® Xeon® Serie 5600 (de 6 y 4 núcleos), con elección de DDR3 DIMM registrada o sin búfer, Smart Array integrada que admite hasta ocho unidades SAS/SATA/SSD y tecnología PCI Express Gen2 doble, proporcionan un sistema de alto rendimiento, ideal para toda la gama de aplicaciones de escalabilidad horizontal.

3.1.3 EQUIPO DE CONEXION ATRAVES DE UN ENLACE WAN

Router Cisco 1811

Para nuestra implementación utilizaremos un Router cisco serie 1800 y de modelo especifico 1811 por su desempeño, capacidad de ancho de banda y sobre todo características adecuadas para poder implementar nuestra VPN.

3.2 INSTALACIÓN CONSOLA HYPER V

“HYPER-V” requiere hardware específico. Para identificar sistemas que admitan la arquitectura x64 y “HYPER-V”

Para instalar y usar el rol “HYPER-V” , se necesita lo siguiente:

Un procesador basado en x64. “HYPER-V” está disponible en las versiones basadas en x64 de Windows Server 2008, concretamente, las versiones basadas en x64 de Windows Server 2008 Standard, Windows Server 2008 Enterprise y Windows Server 2008 Datacenter.

“VIRTUALIZACIÓN” asistida por hardware. Está disponible en procesadores que incluyen una opción de “VIRTUALIZACIÓN”; concretamente, Intel Virtualization Technology (Intel VT) o AMD Virtualization (AMD-V).

La Prevención de ejecución de datos (DEP) implementada por hardware debe estar disponible y habilitada. Concretamente, debe habilitar el bit XD de Intel (bit ejecutar deshabilitado) o el bit NX de AMD (bit no ejecutar).

3.2.1 CONSIDERACIONES ADICIONALES

La configuración de la “VIRTUALIZACIÓN” asistida por hardware y la DEP implementada por hardware están disponibles en el “BIOS”. Sin embargo, los nombres de las opciones de configuración pueden diferir de los nombres identificados anteriormente. Para saber si un modelo de procesador específico admite “HYPER-V” , se debe consultar con el fabricante del equipo.

Si modifica la configuración para la “VIRTUALIZACIÓN” asistida por hardware o para la DEP implementada por hardware, es posible que necesite apagar el equipo y encenderlo nuevamente. Es posible que al reiniciar el equipo no se apliquen los cambios de configuración.

Además para protección del sistema Operativo se requiere q nuestro servidor posea un mínimo de 2 particiones en la cual en una se instalara sistema operativo y en la otra se alojaran las máquinas virtuales

Partición	Tamaño Mínimo	Tipo de Sistema de Archivos
Disco 1 Partición 1	100 Gb	NTFS
Disco 1 Partición 2	400 GB	NFTS

3.3 PROCESO DE INSTALACION

3.3.1 ACTIVACIÓN DEL ROL DE “HYPER-V”

El proceso de activación del l rol de “HYPER-V” en Windows 2008 R2 se realiza desde la consola de administración de servidores, se deberán de desplegar los roles disponibles, y seleccionar posteriormente el rol de “HYPER-V”.

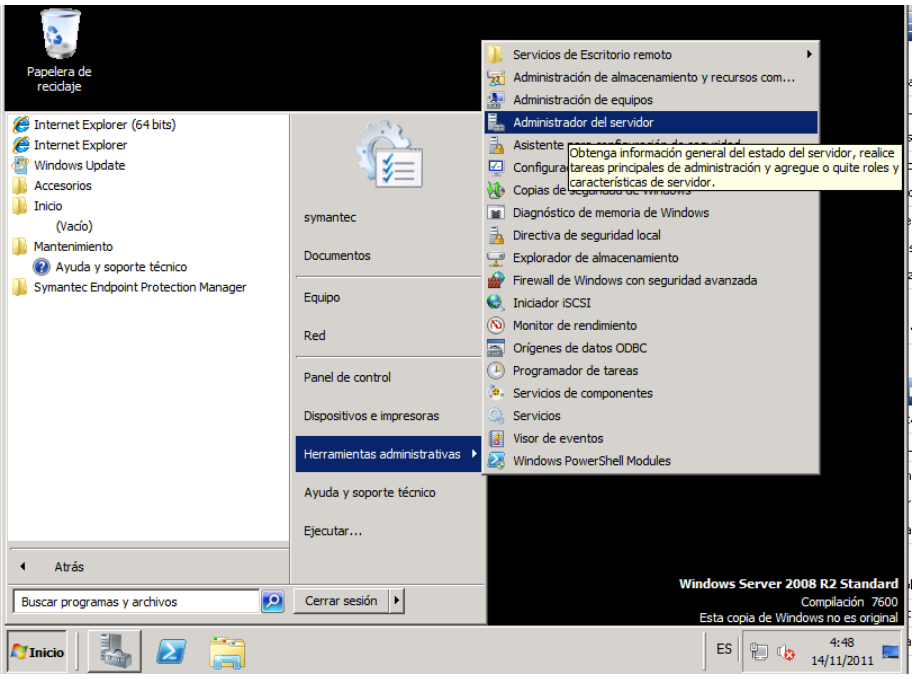


FIG. 12 WINDOWS SERVER 2008 AGREGAR UN ROL DE HYPER

Seleccionamos roles para agregar el nuevo servicio requerido

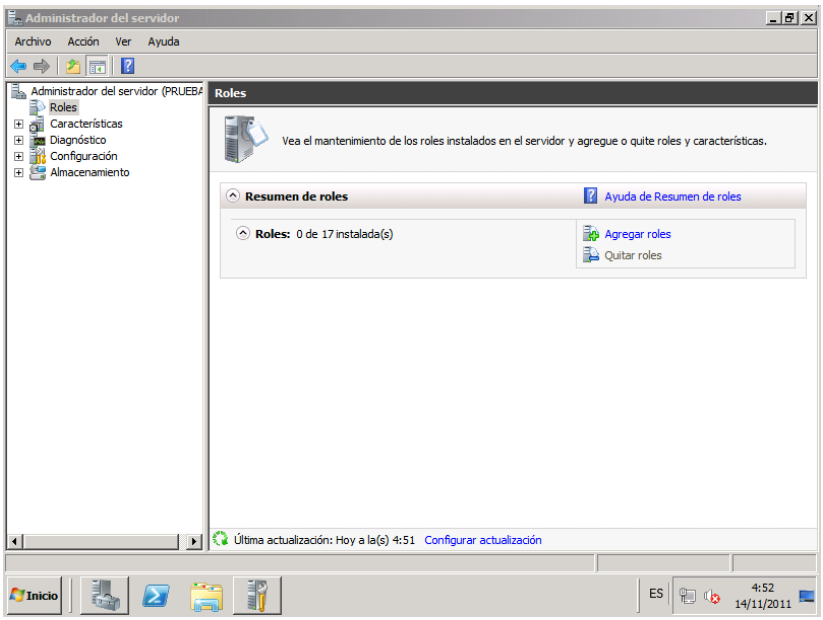


FIG. 13 WINDOWS SERVER 2008 AGREGAR UN ROL DE HYPER V

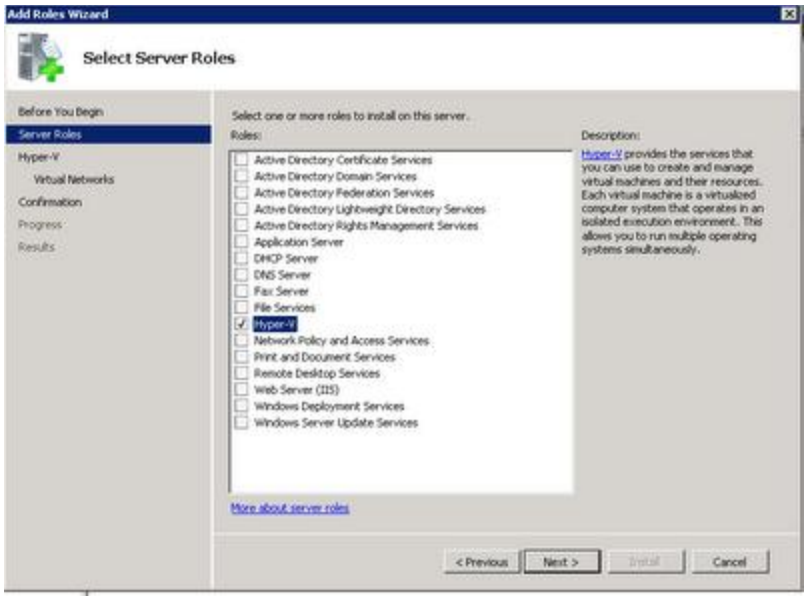


FIG. 14 WINDOWS SERVER 2008 AGREGAR UN ROL DE HYPER V

Una vez, seleccionado el rol, la configuración automática, procede con la selección la interface de red que será utilizada para realizar la gestión del equipo, se recomienda que esta interface no sea utilizada como virtual switch

para mejorar el rendimiento de la red en los servidores virtuales, se recomienda que esta interface sea utilizada solamente para realizar la administración del equipo.

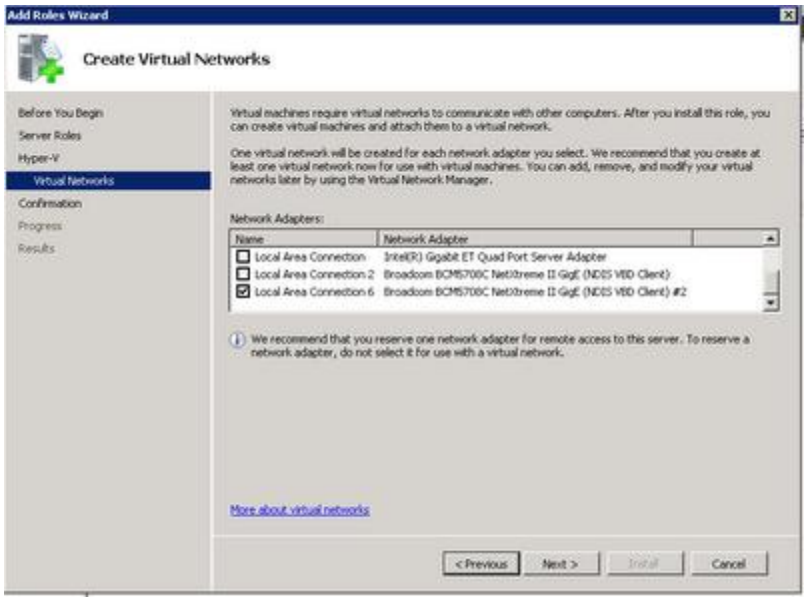


FIG. 15 WINDOWS SERVER 2008 AGREGAR UN ROL HYPER V.

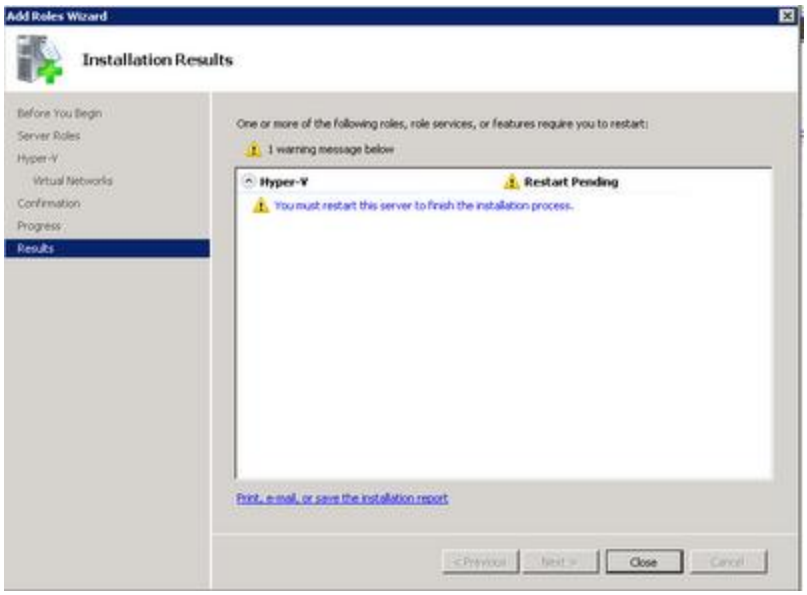


FIG. 16 WINDOWS SERVER 2008 AGREGAR UN ROL HYPER V.

El proceso continuara, sin embargo, es necesario reiniciar el sistema para poder cargar la consola de administración de “HYPER-V”.

Una vez instalado, ”HYPER-V” puede administrarse desde la Consola de Administración de Servidores, de la misma manera que los otros roles de Windows Server 2008. Seleccione el "HYPER-V” Manager" desde la carpeta de Herramientas Administrativas en el menú Inicio para abrir la consola de gestión de la “VIRTUALIZACIÓN”. Con esta consola se puede administrar un sistema local o conectarse con otros servidores “HYPER-V” para administrarlos en remoto.

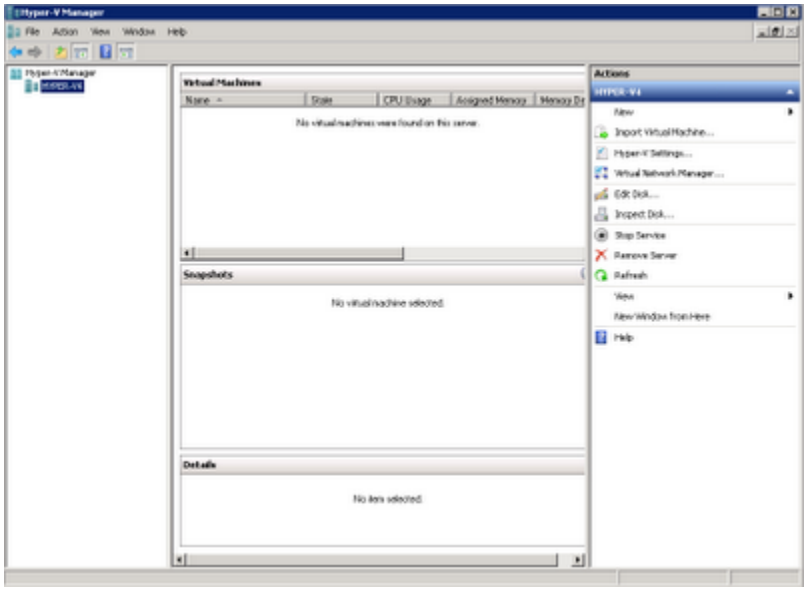


FIG. 17 CONSOLA DE HYPER V

3.4 SERVIDOR PARA CONEXIÓN VPN

Como se indicó anteriormente para realizar la conexión a través de un enlace “WAN” para administrar nuestro servidor se requiere la instalación y configuración de un servidor Cisco 1811 así como también de un software cliente “VPN” el cual se estará en computador de administrador para se pueda realizarse la conexión de una manera segura.

3.4.1 CONFIGURACION ROUTER CISCO.

A continuación un breve manual de la configuración básica de un Router Cisco. Se deben tener como premisa que toda la configuración es realizada en “configuración global” excepto aquellos puntos en los cuales el prompt indique que nos encontramos dentro de una interface, lo cual es indicado en cada caso.

3.4.1.1 COLOCACIÓN DE HOSTNAME, DOMINIO Y DNS

El hostname del router, debe ser un nombre representativo

```
Router(config)#hostname CISCO

CISCO(config)# ip domain-name my_empresa.com

CISCO(config)# ip name-server 200.105.239.3
```

CISCO(config)# ip name-server 200.205.225.2

3.4.1.2 ELIMINACIÓN DE SERVICIOS QUE VIENEN POR DEFAULT

Existen servicios que viene por default en los routes Cisco , como el http, el dhcp, y debemos deshabilitarlos a menos que se desee una configuración especial con estos servicios.

CISCO(config)#no service config

CISCO(config)#no ip http server

CISCO(config)#no ip http authentication local

CISCO(config)#no ip http secure-server

CISCO(config)#no ip http timeout-policy idle 600 life 86400 requests 10000

CISCO(config)#no service dhcp

CISCO(config)#no ip dhcp excluded-address 10.10.10.1

CISCO(config)#no ip dhcp pool sdm-pool

CISCO(config)#no ip http access-class 23

CISCO(config)#no username cisco

CISCO(config)#no banner exec

3.4.1.3 CONFIGURACIÓN DE COMANDOS VARIOS

Desactivación de CDP

CISCO(config)#no cdp run

Permite poner indicadores de tiempo en debugs

CISCO(config)#service timestamps debug uptime

Permite poner indicadores de tiempo en logs

CISCO(config)#service timestamps log uptime:

Permite poner indicadores de fecha en los logs

CISCO(config)#service timestamps log datetime

Para evitar la presencia de los logs en la consola

CISCO(config)#no logging console

Para activar el log en el buffer del sistema

CISCO(config)# logging buffered 4096 debugging

Para permitir el uso de subredes 0

CISCO(config)#ip subnet-zero

Para indicar al router que si no encuentra una ruta en la tabla, se vaya por la ruta por defecto.

CISCO(config)#ip classless

El siguiente comando habilita CEF en el router (Cisco Express Forwarding) CEF es uno de los métodos de Interrupt Context Switching. Tiene la ventaja de switchear los paquetes más rápidamente y a su vez representa una carga menos pesada para la CPU del equipo. Dada la capacidad de la CPU de los ciertos routers CISCO, es muy importante tener este comando habilitado. De lo contrario nos exponemos a saturación de la CPU.

CISCO(config)#ip cef

3.4.1.4 CREACIÓN DE USUARIOS

Se crean los usuarios monitoreo, administrador.

ISCO(config)#username monitoreo privilege 5 secret m1m0n1t0r

CISCO(config)#username administrador privilege 15 secret adm1n1strat0r

CISCO(config)#enable secret clave_secreta

Para permitir el acceso solo a usuarios locales a través de consola y de acceso remoto

CISCO(config)#line con 0

CISCO(config-line)#Login local

CISCO(config-line)#exit

CISCO(config)#line vty 0 4

CISCO(config-line)#login local

CISCO(config-line)#exit

3.4.1.5 CONFIGURACIÓN DE IP'S

Entrar en modo de configuración global

CISCO# config term

Entrar a la interface

CISCO(config)# int f0

Configurar la ip y la mascara

CISCO(config-if)# ip address 200.105.245.46 255.255.255.248

Colocar la descripción de la interface

CISCO(config-if)#description WAN

Para evitar el redireccionamiento del paquete por la misma interface

CISCO(config-if)#no ip redirects

Levantamos la interface.

CISCO(config-if)#no shutdown

Para deshabilitar que el router actúe como proxy

CISCO(config-if)#no ip proxy-arp

Salir

CISCO(config-if)#exit

Adaptar lo mismo para la eth1 considerando las siguientes interfaces:

CISCO(config)# int vlan1

CISCO(config-if)# ip address 192.168.1.107 255.255.255.0

3.4.1.6 CONFIGURACIÓN DEL GATEWAY

Domo default usaremos la IP asignada por el proveedor de internet

CISCO(config)# ip route 0.0.0.0 0.0.0.0 200.105.245.41

3.4.1.7 LISTAS DE ACCESO

En la access-list 1 se incluirán las IPs de monitoreo, desde las cuales se permitirá el acceso a equipos.

CISCO(config)#access-list 1 remark ACCESOS

CISCO(config)#access-list 1 permit 200.105.245.40 0.0.0.7

CISCO(config)#access-list 1 permit 192.168.1.0 0.0.0.255

Luego permitir únicamente el acceso de los usuarios permitidos:

```
CISCO(config)#line vty 0 4

CISCO(config-line)#login local

CISCO(config-line)# access-class 1 in

CISCO(config-line)#exec-timeout 30

CISCO(config-line)#exit
```

CAPÍTULO 4

4 FUNCIONAMIENTO Y PRUEBAS

4.1 CONFIGURACIÓN HYPER V

4.1.1 CREACIÓN DE UNA MAQUINA VIRTUAL, EN “HYPER-V”

Con la consola “HYPER-V” manager puede, de una manera muy sencilla, crear nuevas máquinas virtuales, modificar la configuración del host y las máquinas virtuales, detener y arrancar máquinas virtuales, obtener instantáneas, entre otras características. Todo ello utilizando la interfaz de Windows, basada en asistentes y muy conocida por los administradores.

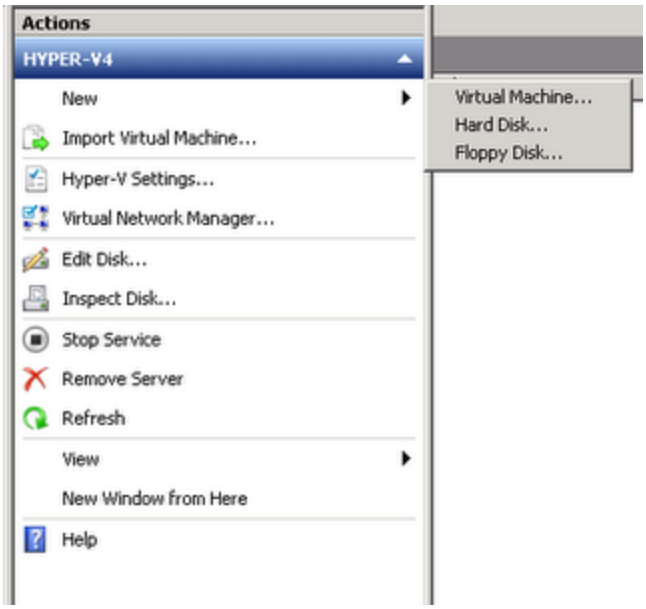


FIG. 18 CREANDO MAQUINAS VIRTUALES

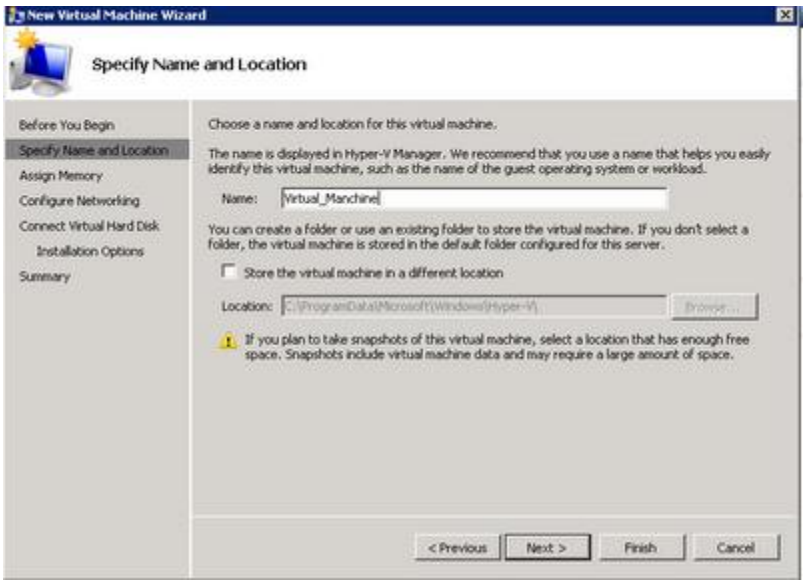


FIG. 19 CREANDO MAQUINAS VIRTUALES

Una vez seleccionado el nombre que tendrá la máquina virtual, se procede a la asignación de memoria, para el equipo virtual, este y otras configuraciones pueden ser modificadas posteriormente.

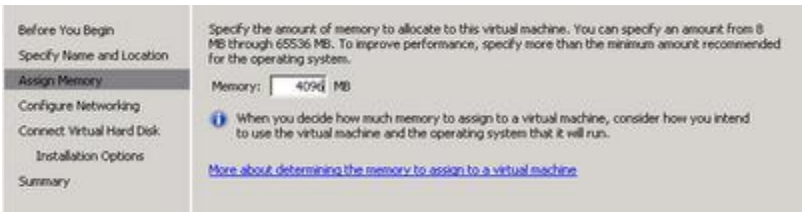


FIG. 20 CREANDO MAQUINAS VIRTUALES

La configuración o asignación de las tarjetas de red. Esto, es importante recordar que puede realizarse posteriormente.

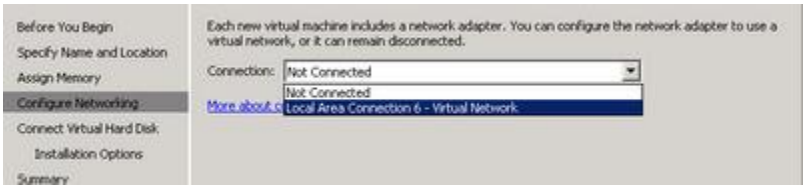


FIG. 21 CREANDO MAQUINAS VIRTUALES

La siguiente imagen muestra el proceso de asignación de un medio de almacenamiento, en entornos Enterprise se recomienda utilizar algún sistema de almacenamiento externo, para brindar más seguridad e independencia de la información.

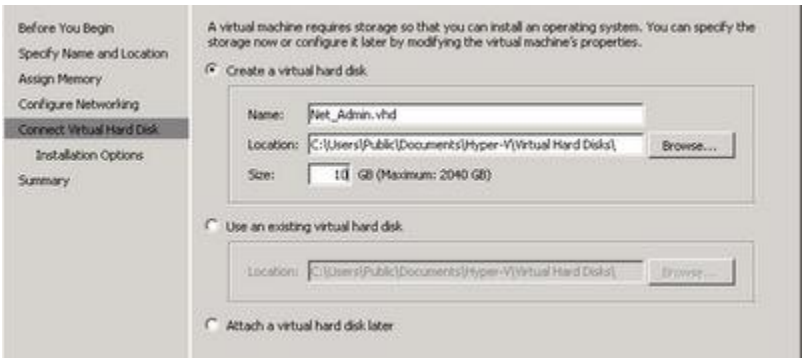


FIG. 22 CREANDO MAQUINAS VIRTUALES

Esta es la manera en que aparecerán las máquinas virtuales en la consola “HYPER-V”, como puede verse, el proceso de instalación, configuración y administración de “HYPER-V” es muy sencillo, y no requiere de mucho esfuerzo para implementarse. Sin embargo se recomienda tener mucho cuidado al realizar un sistema de “VIRTUALIZACIÓN” complejo, con el fin de evitar fallas en este tipo de entorno.

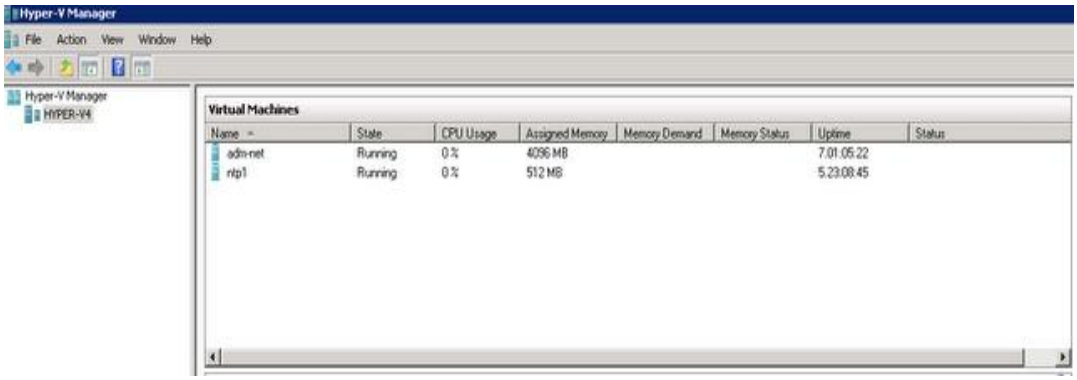


FIG. 23 CREANDO MAQUINAS VIRTUALES

4.2 CONFIGURACIÓN SERVIDOR Y CLIENTE VPN

4.2.1 CONFIGURACION DE LA VPN

Habilitaremos la autenticación, autorización para poder hacer logon.

CISCO(config)# aaa new model

CISCO(config)# aaa authentication login AAA-VPN local

CISCO(config)# aaa authorization network AAA-VPN local

Definiremos el pool que usara nuestra LAN al conectarse a la VPN

CISCO(config)# ip local pool VPNLANPOOL 10.9.0.1 10.9.0.254

Configuraremos el cifrado de nuestro grupo VPN.

CISCO(config)# crypto isakmp client configuration group vpnall

CISCO(config-isakmp-group)# key blindhog1@

CISCO(config-isakmp-group)# dns 200.105.239.3

CISCO(config-isakmp-group)# pool VPNLANPOOL

CISCO(config-isakmp)#crypto isakmp policy 1

CISCO(config-isakmp)#authentication pre-share

CISCO(config-isakmp)#encryption 3des

CISCO(config-isakmp)#hash sha

CISCO(config-isakmp)# group 2

CISCO(config-isakmp)#crypto ipsec transform 3des-sha esp-3des esp-sha-hmac

CISCO(config-isakmp)#crypto dynamic-map dynmap 10

CISCO(config-isakmp)# set transform-set 3des-sha

CISCO(config)#crypto map vpn 10 ipsec-isakmp dynamic dynmap

CISCO(config)#crypto map vpn client configuration address respond

```
CISCO(config)#crypto map vpn client authentication list AAA-VPN

CISCO(config)#crypto map vpn isakmp authorization list AAA-VPN
```

Configuraremos un loopback para que el tráfico que venga de la VPN siga cifrado y no se una fácilmente con el tráfico de la LAN.

```
CISCO(config)# interface Loopback0

CISCO(config-if)#ip address 10.1.1.1 255.255.255.0

 CISCO(config-if)# ip nat inside

 CISCO(config-if)# ip virtual-reassembly
```

Permitimos por ACL la red que va a ser nateada

```
CISCO(config)# access-list 101 permit ip 10.9.0.0 0.0.0.255 any

CISCO(config)# ip access-list extended ACL-OUTSIDE-PBR

CISCO(config)# permit ip 10.9.0.0 0.0.0.255 any
```

Creamos una route-map para que no se una el tráfico con el de lan fácilmente en el momento del cifrado.

```
CISCO(config)# route-map RM-OUTSIDE-PBR permit 10

 CISCO(config)# match ip address ACL-OUTSIDE-PBR
```

CISCO(config)# set ip next-hop 10.1.1.2

Configuraremos en nuestra interface WAN para que pueda salir todo el trafico (nateo)

CISCO(config)# interface fa0

CISCO(config-if)# ip nat outside

CISCO(config-if)# crypto map vpn

CISCO(config-if)# ip policy route-map RM-OUTSIDE-PBR

Nateamos la red LAN que usaremos para la VPN

CISCO(config)# ip nat inside source list 101 interface FastEthernet0 overload.

4.2.2 CONFIGURACION VPN CLIENT.

Para garantizar la seguridad durante todo la conexión se realiza la instalación del software cliente en el equipo del administrador.

- Descargamos de la página oficial de cisco la última versión del software CISCO “VPN” CLIENT
  http://www.cisco.com/cisco/software/release.html?
- Procedemos a instalar el software cliente.

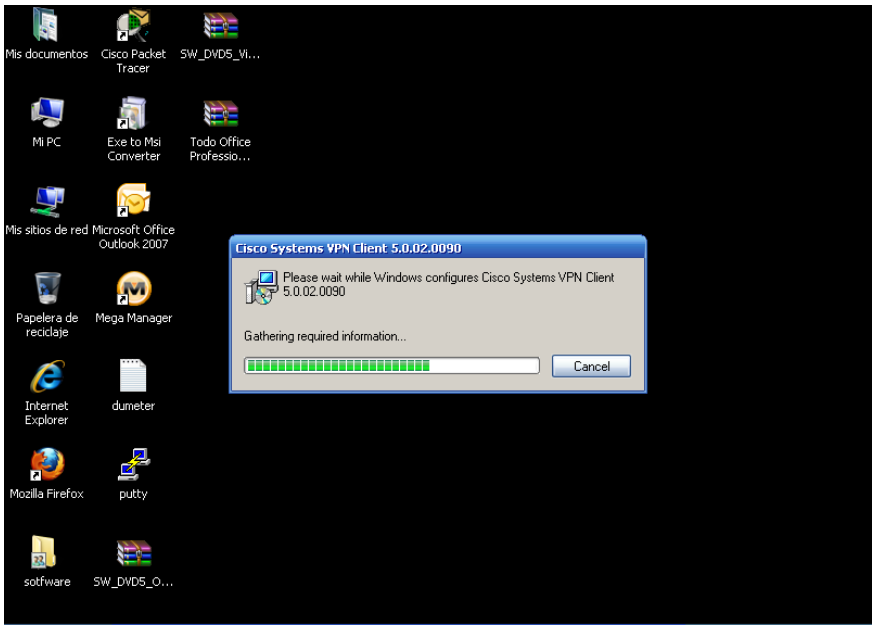


FIG. 24 INSTALACION CLIENTE VPN

Nos muestra la pantalla de bienvenida damos siguiente.

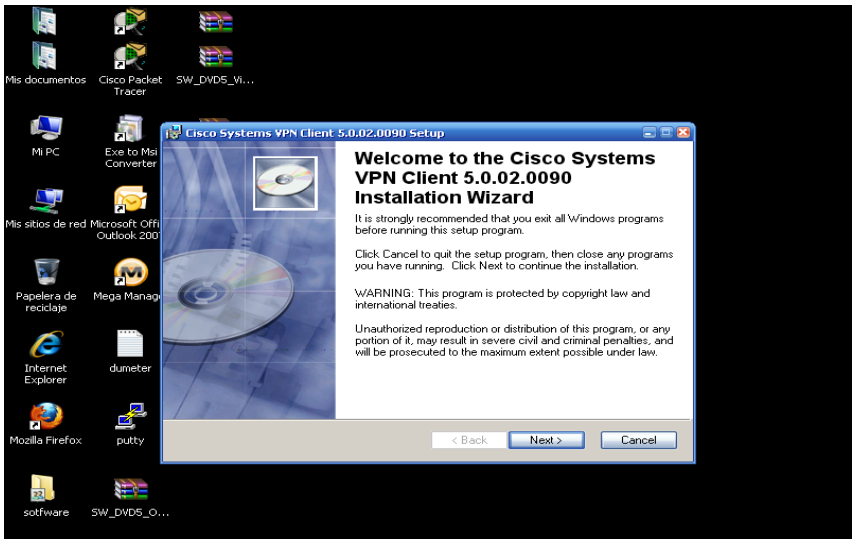


FIG. 25 INSTALACION CLIENTE VPN

- Procedemos a aceptar los términos de uso.

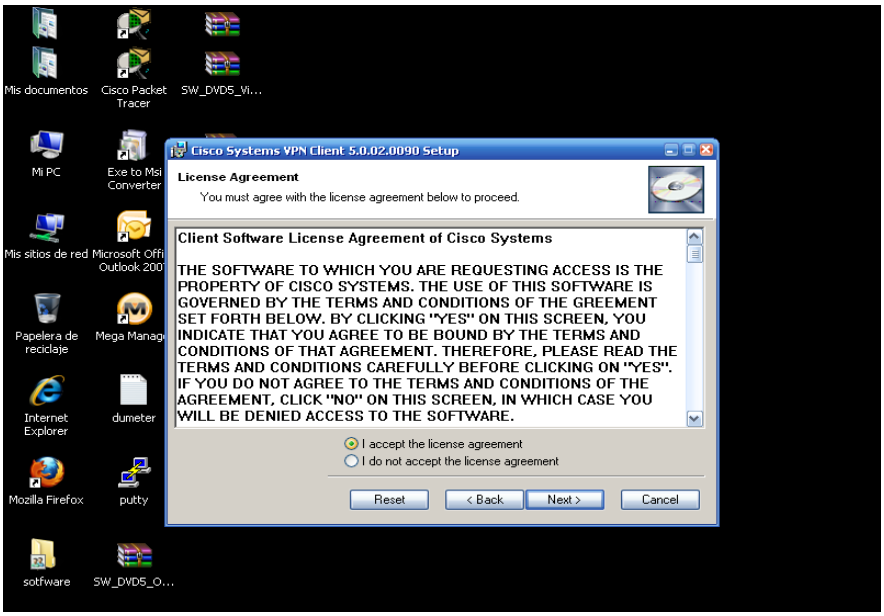


FIG. 26 INSTALACION CLIENTE VPN

Damos siguiente para confirmar la instalación.

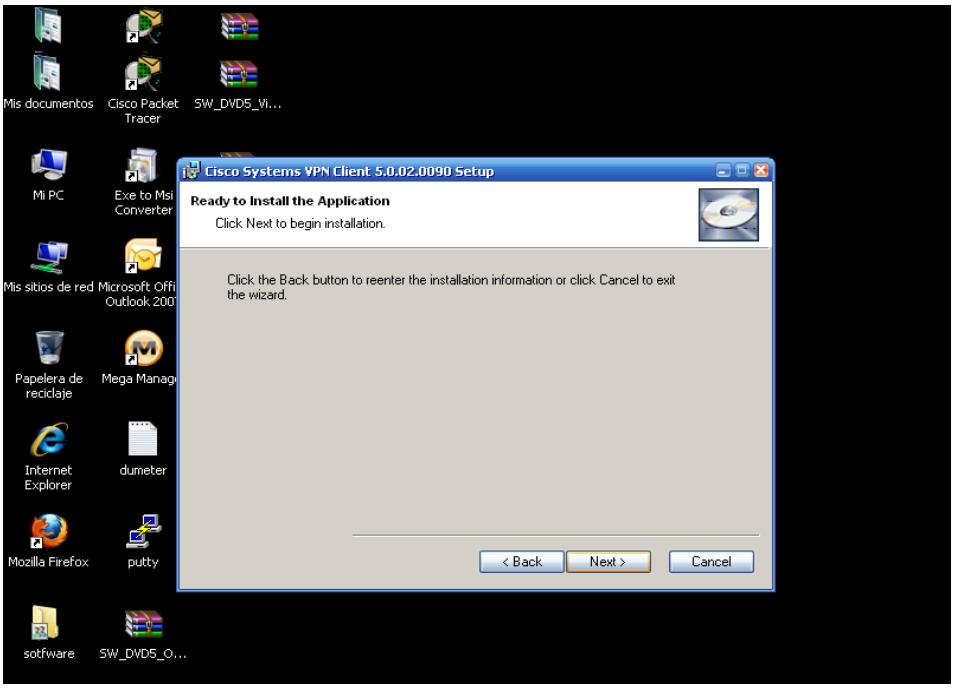


FIG. 27 INSTALACION CLIENTE VPN

Esperamos que se llene la barra de la instalación.

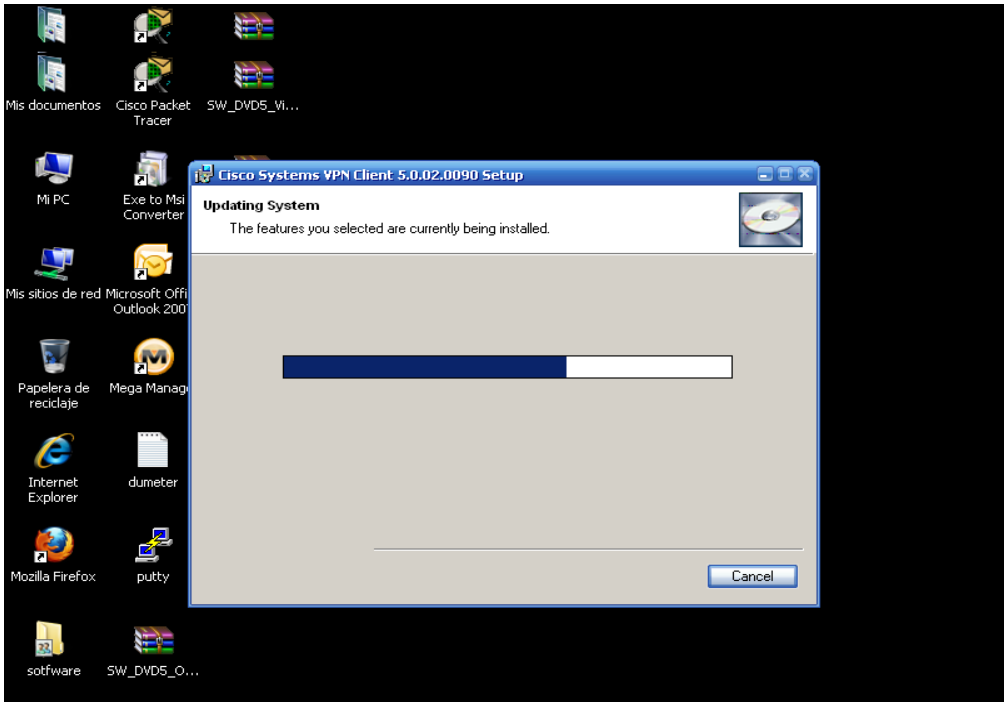


FIG. 28 INSTALACION CLIENTE VPN

Nos mostrara una leyenda que el software está instalado,

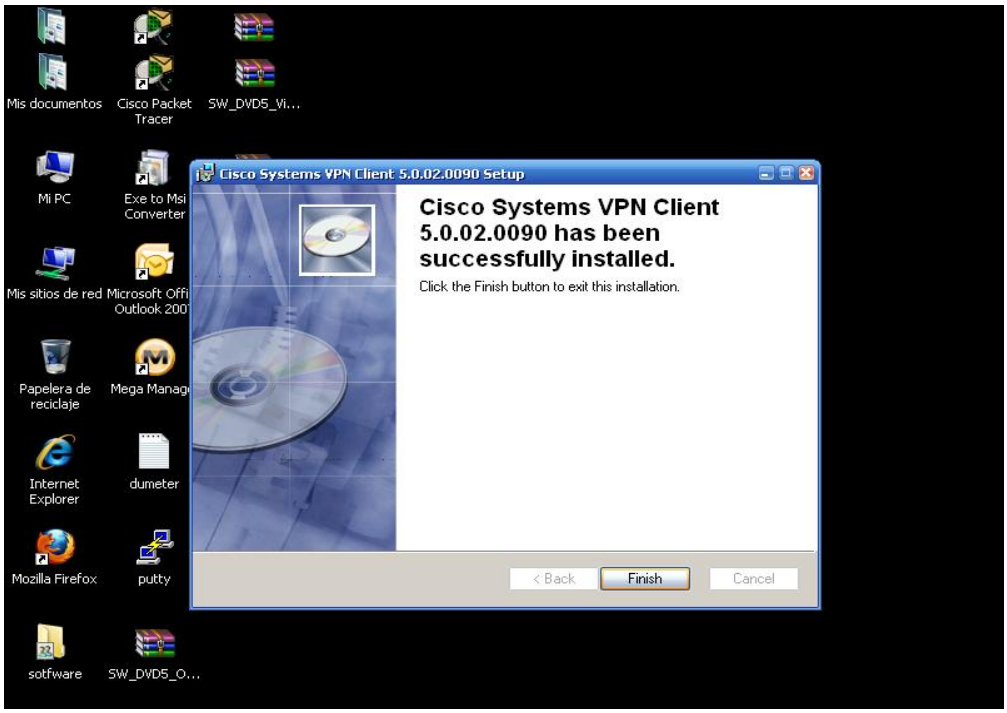


FIG. 29 INSTALACION CLIENTE VPN

Veremos en el escritorio el icono de un candado y en la barra de fecha y hora.

4.2.2.1 CONFIGURACION DE VPN.

Ubicamos el icono “VPN CLIENT” y le damos doble clic. (Fig. 34)

Damos clic en “NEW” para agregar nuestra “VPN”. (Fig. 35)

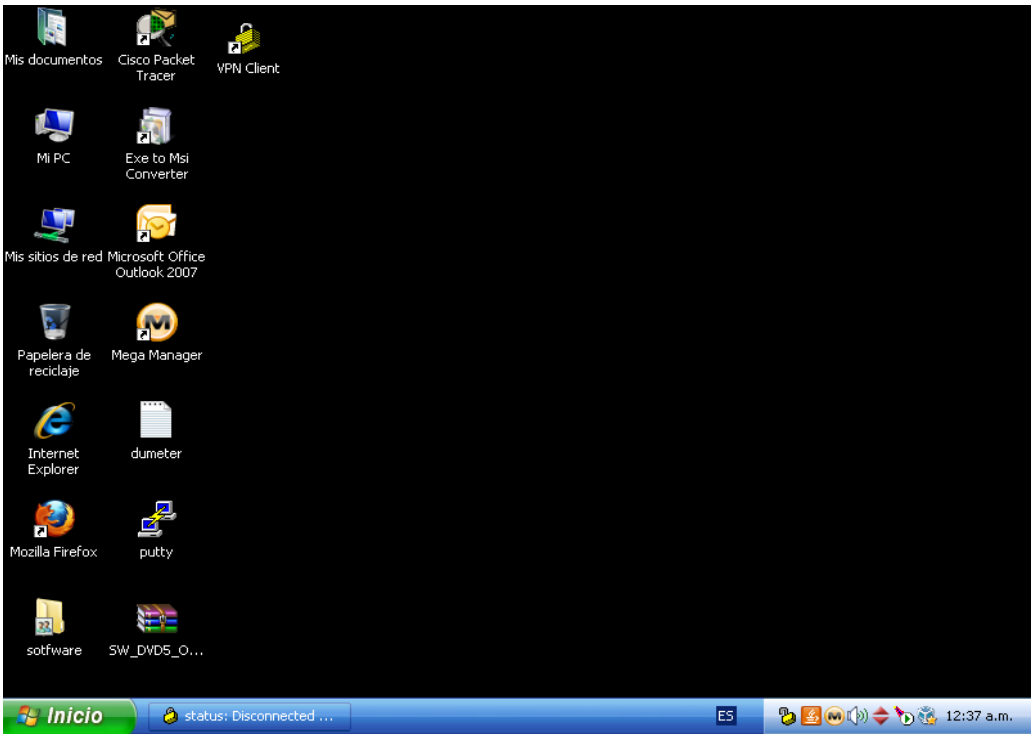


FIG. 30 CONFIGURACION VPN CLIENT.

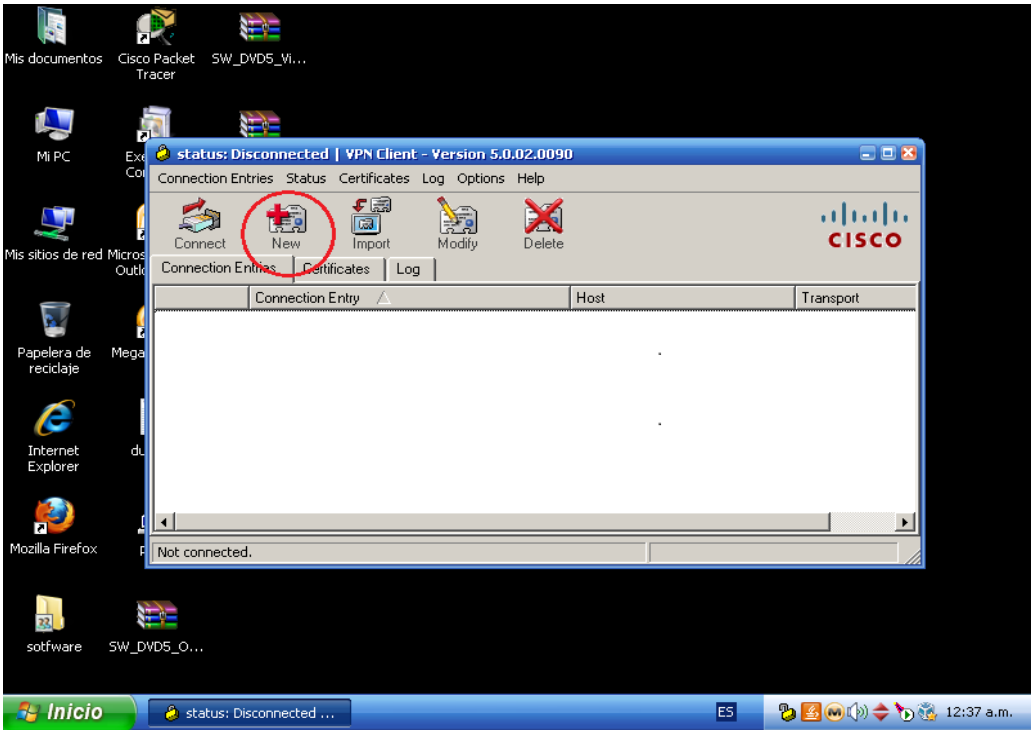


FIG. 31 CONFIGURACION VPN CLIENT.

Ingresamos un nombre, una descripción de la VPN, la IP publica, el nombre del Grupo de nuestra VPN, y la clave del grupo. Grabamos y nos daremos cuenta que en la parte inferior muestra un candado que está abierto.

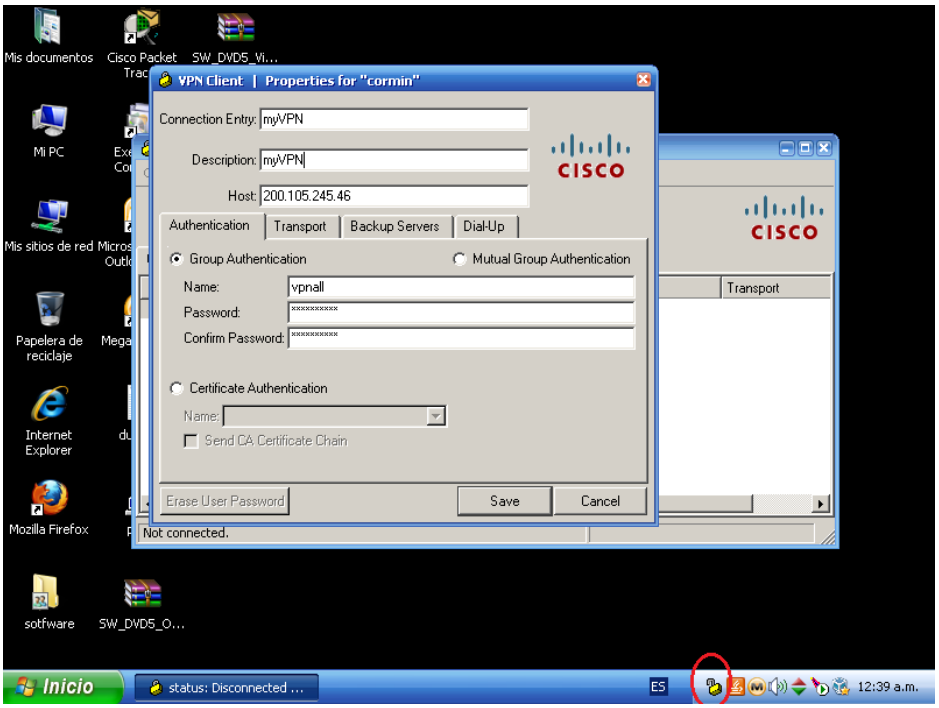


FIG. 32 CONFIGURACION VPN CLIENT.

Para conectarnos daremos un clic en “Connect” y nos mostrara una ventana para ingresar nuestro usuario creado. (Fig. 37)

Una vez aceptado nuestro usuario estaremos conectado a la VPN veremos los candados cerrados y un status connected. (Fig. 38)

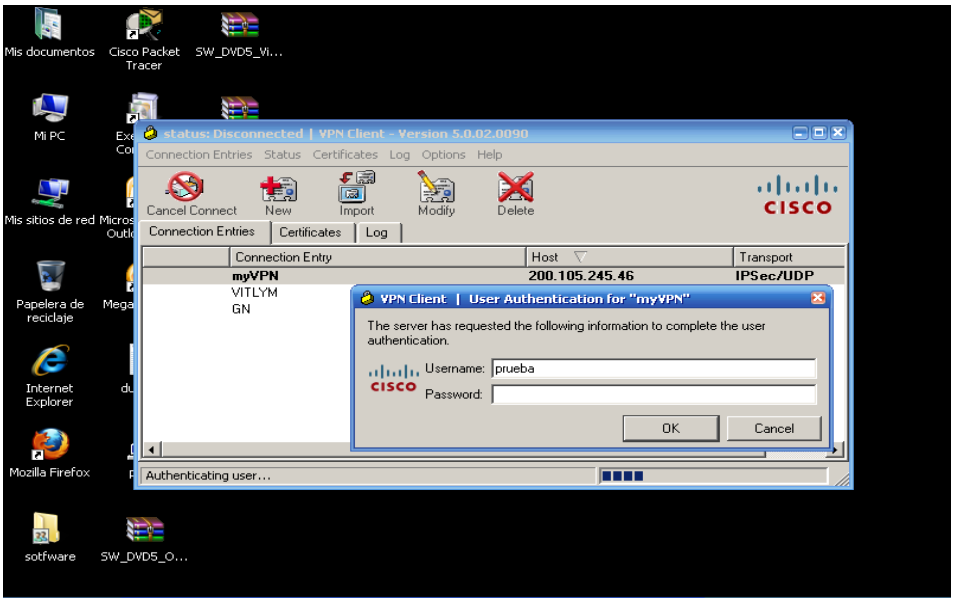


FIG. 33 CONFIGURACION VPN CLIENT.

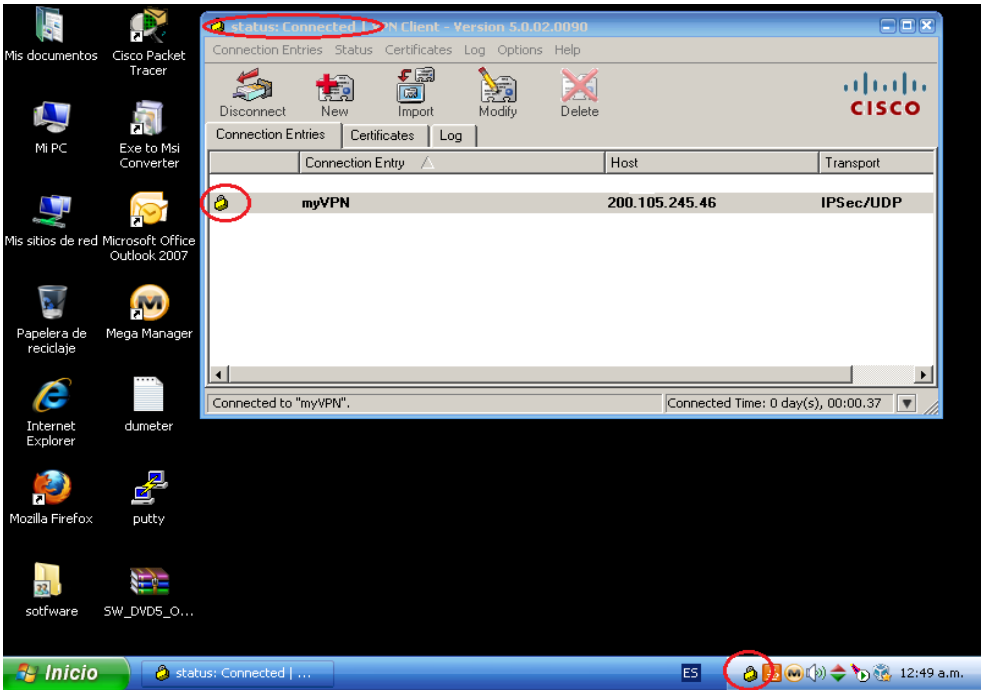


FIG. 37 CONFIGURACION VPN CLIENT.

4.3 PRUEBAS SERVIDOR HYPERV

Para realizar las pruebas respectivas de este rol se procedió a crear 3 máquinas virtuales para monitorear su respectivo funcionamiento

Nombre de maquina	Memoria RAM	Tamaño	Sistema Operativo	servicio
SRV-DC-COR	1GB	100 Gb	WINDOWS SERVER 2008	ACTIVE DIRECTORY
SRV-BD-COR	5GB	200 GB	WINDOWS SERVER 2008	BASE DATOS SQL 2008
SRV-DES-COR	2GB	50 GB	WINDOWS SERVER 2008	BASE DATOS SQL 2008

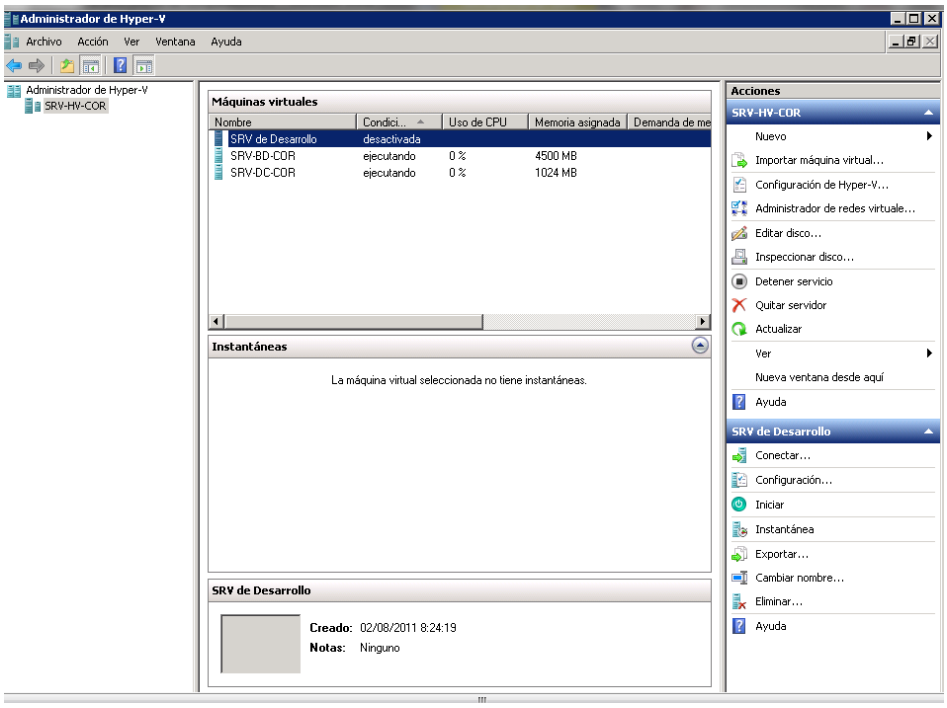


FIG 38 MEDICION DE RENDIMIENTO SERVIDOR HYPER V

Para monitorear el estatus de los servidores virtualizados se ha monitoreado desde 2 puntos de vista desde el equipo tiene la función de HOST Server monitoreando el rendimiento del mismo y de las máquinas virtuales para verificar el rendimiento de cada uno al estar virtualizado se han utilizado las herramientas propias del sistema operativo Windows server 2008

- Administrador de Tareas
- Monitor de rendimiento

El Administrador de tareas de Microsoft.- Es un programa pequeño que viene incorporado en Windows. Proporciona información sobre los programas y procesos que se ejecutan en el equipo. También proporciona los indicadores de rendimiento más utilizados por el equipo.

Con el Administrador de tareas podemos supervisar el rendimiento del ordenador, además podemos ver el estado de los programas que se ejecutan, y finalizar a los programas cuando no responde. Esta información la podemos obtener en modos de gráficos o tablas con los valores que necesitamos.

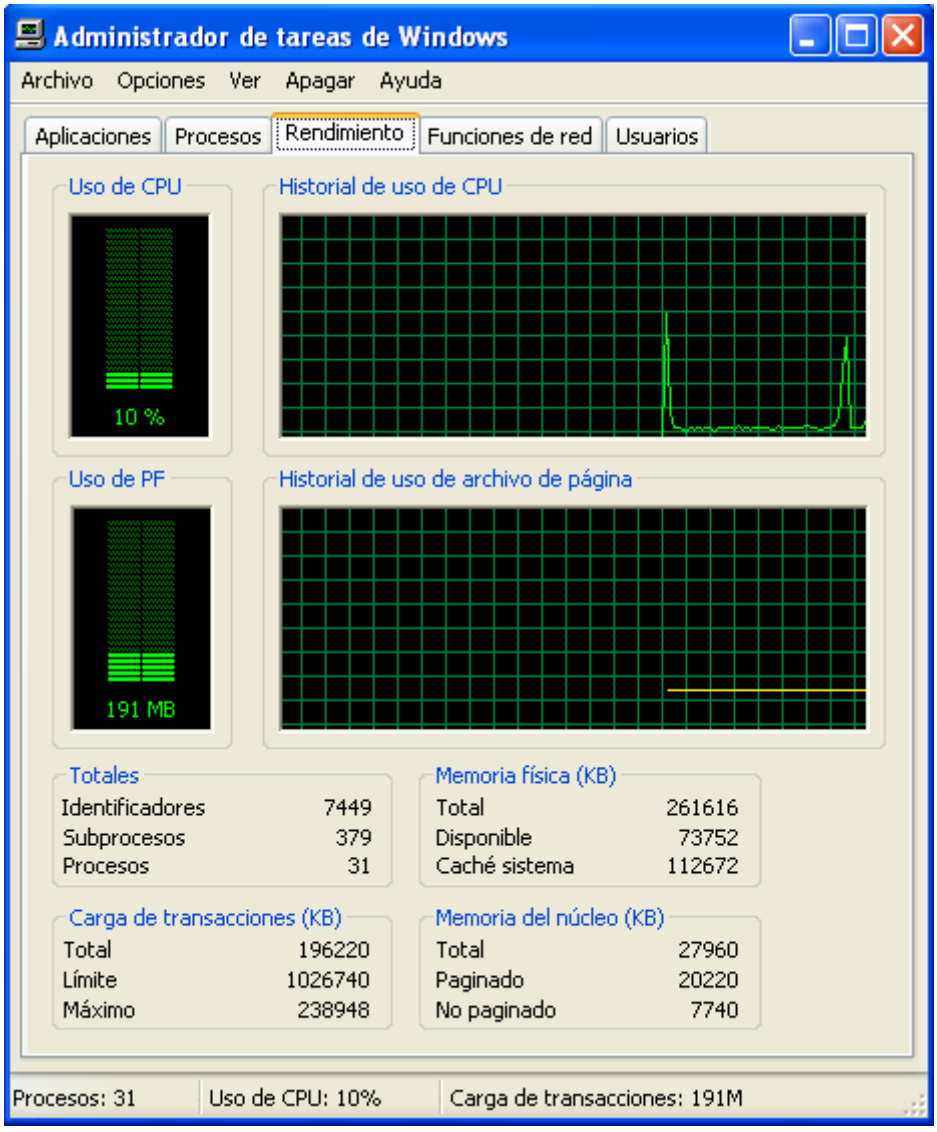


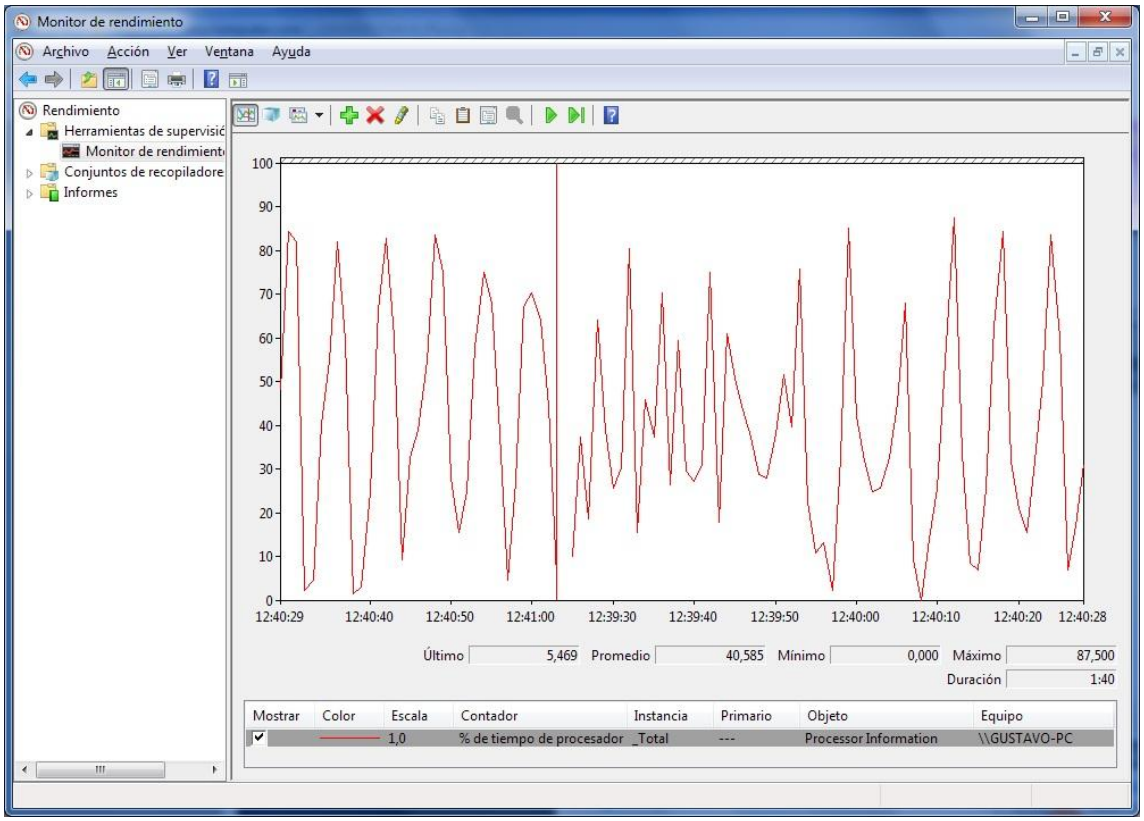
FIG. 39 ADMINISTRADOR DE TAREAS

El Monitor de rendimiento de Windows.- es un complemento de Microsoft Management Console (MMC) que proporciona herramientas para analizar el

rendimiento del sistema. Desde una sola consola puede supervisar el rendimiento de las aplicaciones y del hardware en tiempo real, personalizar los datos desea recopilar en los registros, definir umbrales para alertas y acciones automáticas, generar informes y ver datos de rendimientos pasados en una gran variedad de formas.

El Monitor de rendimiento de Windows combina la funcionalidad de herramientas independientes anteriores, incluidos Registros y alertas de rendimiento (PLA), Server Performance Advisor (SPA) y Monitor de sistema. Proporciona una interfaz gráfica para la personalización de conjuntos de recopiladores de datos y sesiones de seguimiento de eventos.

El Monitor de rendimiento de Windows realiza la recopilación de datos y el registro mediante conjuntos de recopiladores de datos.



4.3.1 MONITOREO HOST SERVER.

Como podemos apreciar en el resuenen de monitoreo nuestro equipo al tener que al gestionar 3 máquinas virtuales estamos usando una frecuencia máxima del 59% CPU y Memoria al 62% mientras que en disco y red no sobrepasa el 10%.

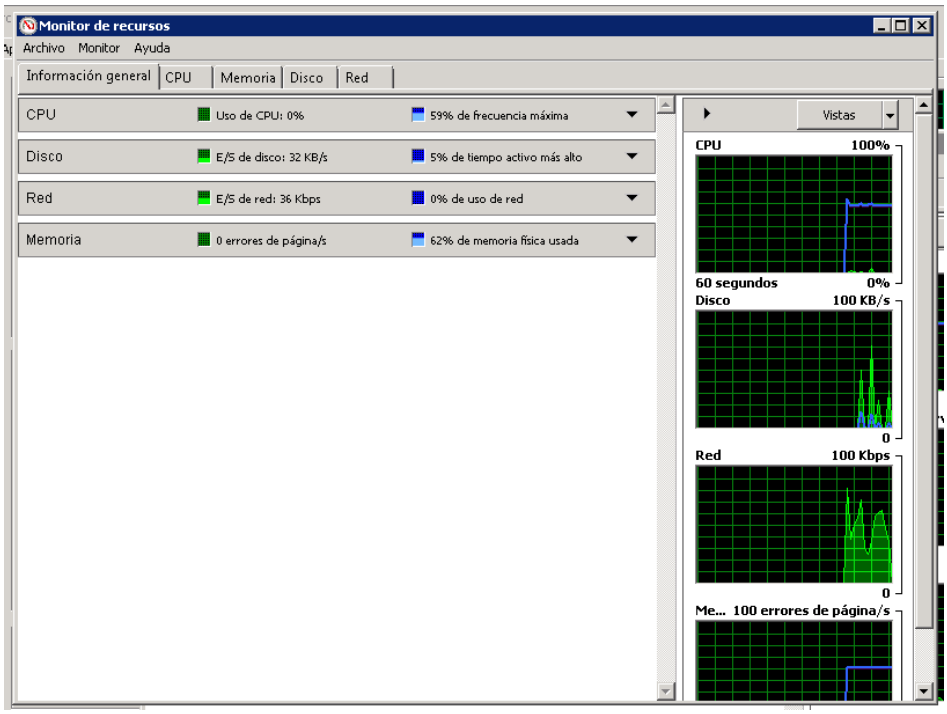


FIG. 34 MEDICION DE RENDIMIENTO SERVIDOR HYPER V

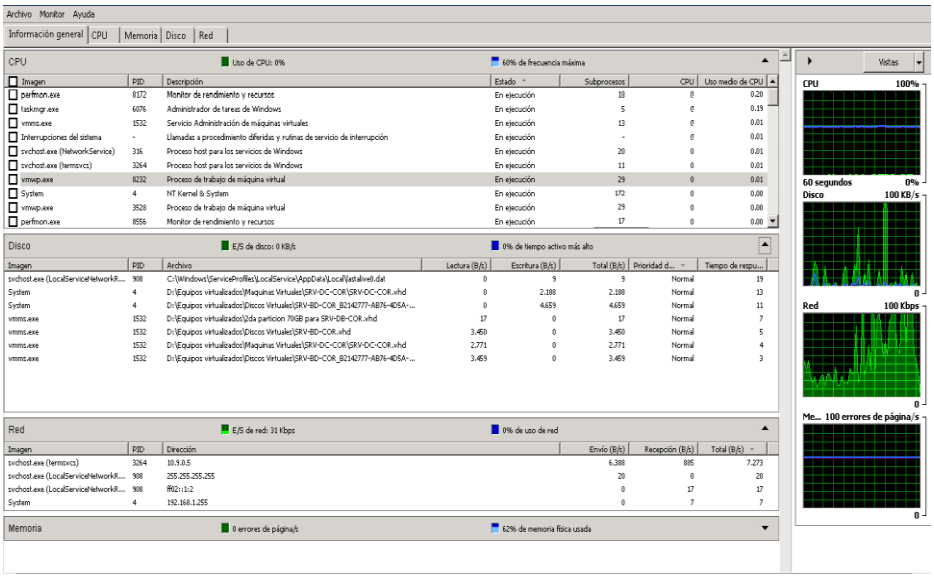


FIG. 35 MEDICION DE RENDIMIENTO SERVIDOR HYPER V

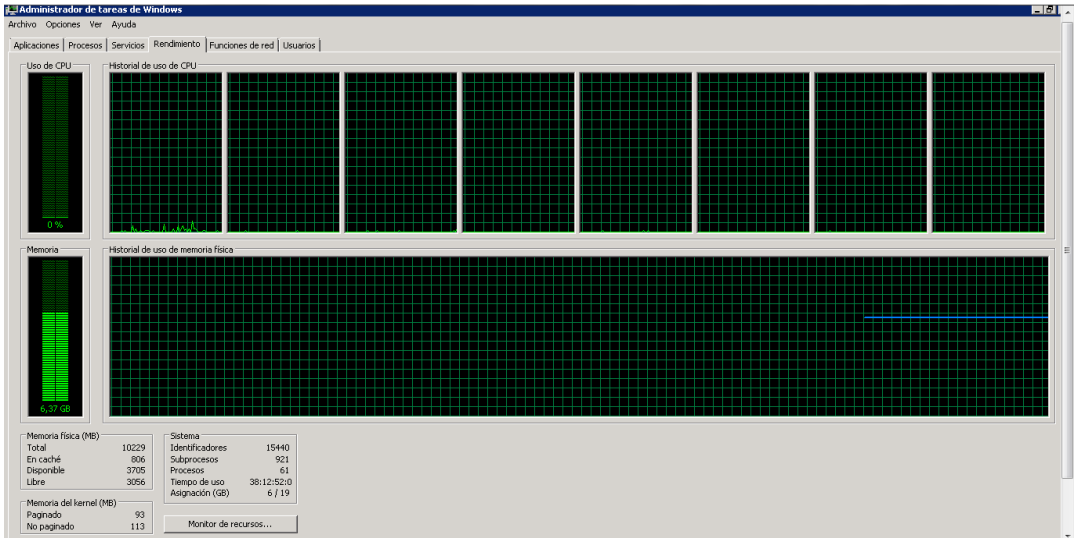


FIG. 36 MEDICION DE RENDIMIENTO SERVIDOR HYPER V

4.3.1.1 GRAFICA DE USO DEL CPU

En la siguiente grafica podemos visualizar el porcentaje de CPU usado por nuestro servidor virtualizado.

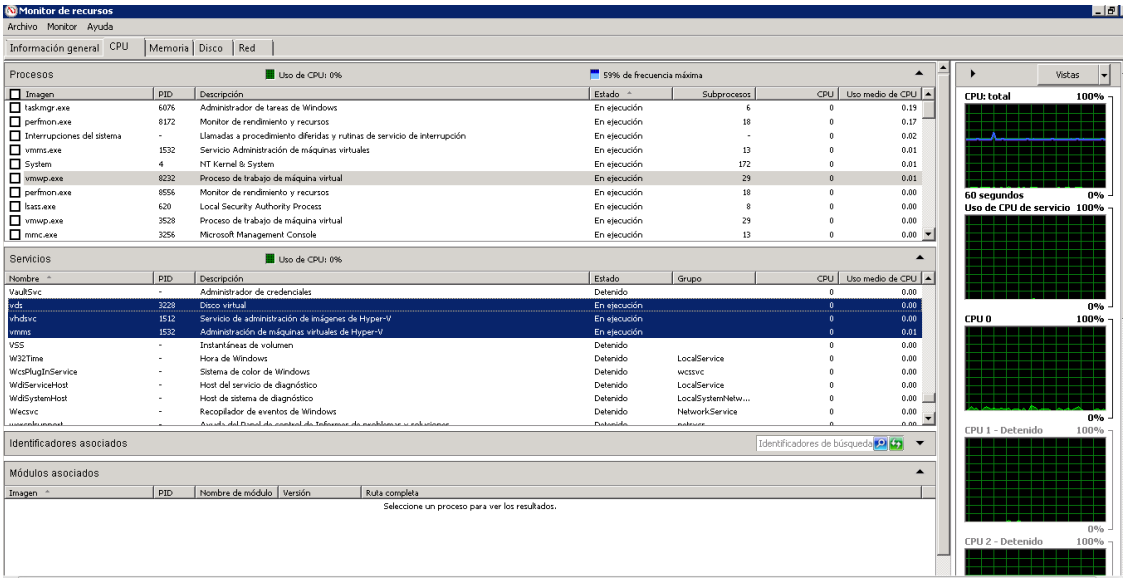


FIG 37 MEDICION DE RENDIMIENTO SERVIDOR HYPER V

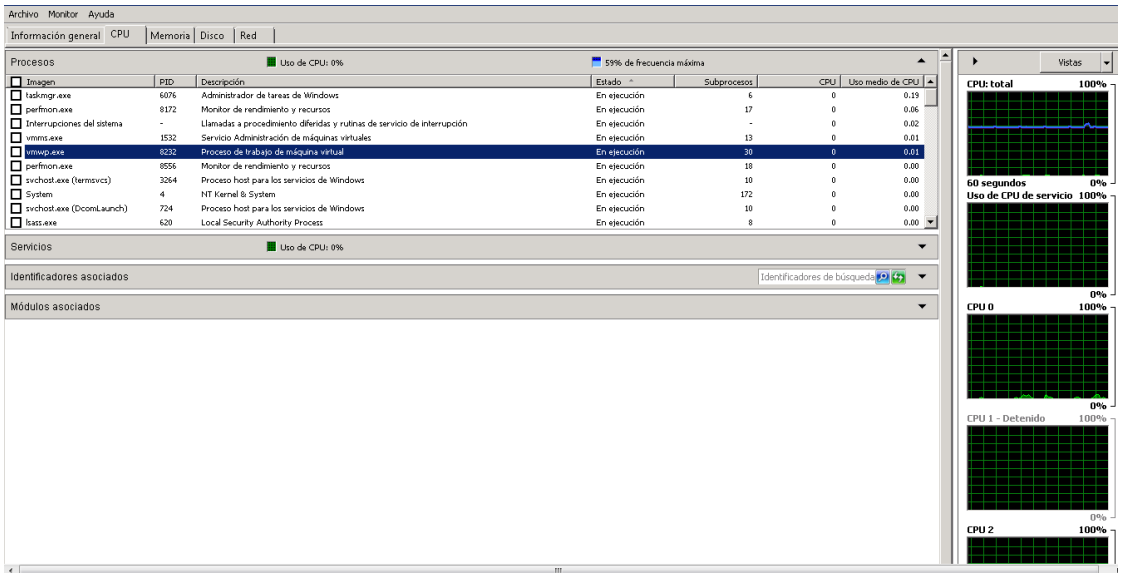


FIG. 38 MEDICION DE RENDIMIENTO SERVIDOR HYPER V

En la gráfica se muestra cuenta memoria RAM está manejando nuestro proceso de “VIRTUALIZACIÓN”

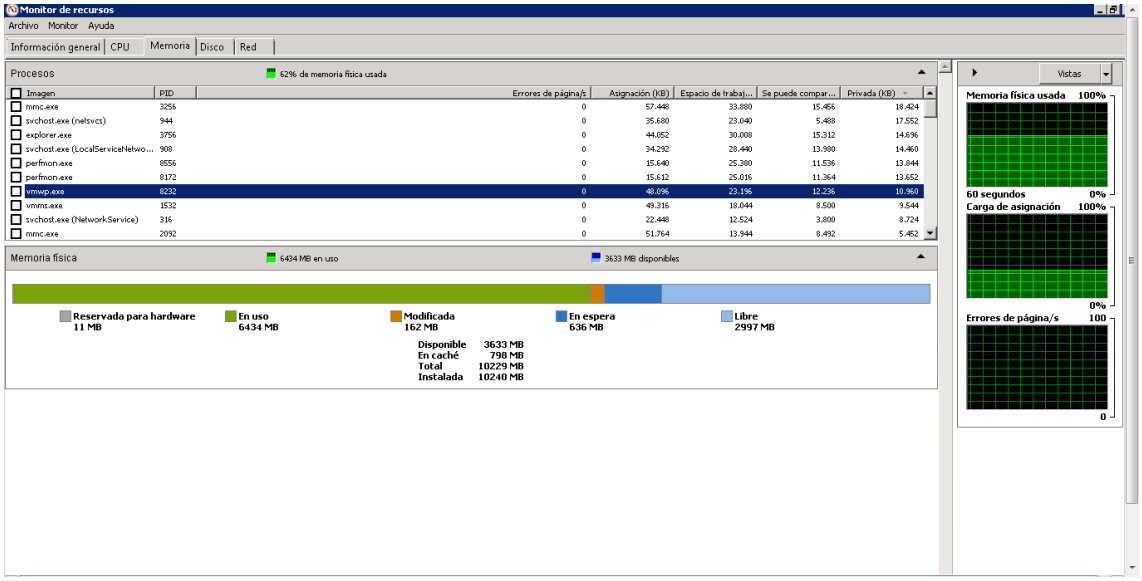


FIG. 39 MEDICION DE RENDIMIENTO SERVIDOR HYPER V

En esta grafica de indica cantidad de uso del disco duro a pasar de que nuestras máquinas virtuales se encuentran alojadas físicamente en una segunda partición primaria del disco duro el cual por contingencia se encuentra configurado en RAID 1.

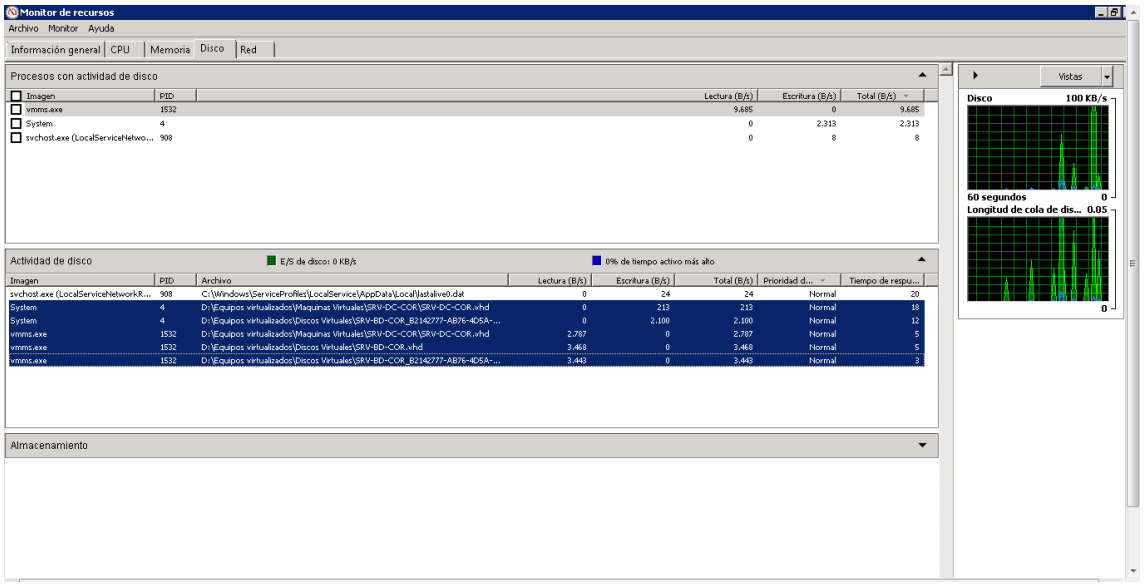


FIG 40 MEDICION DE RENDIMIENTO SERVIDOR HYPER V

Grafica de red uso máximo inferior al 10% esto varía de acuerdo a las conexiones concurrentes hacia nuestra base de datos.

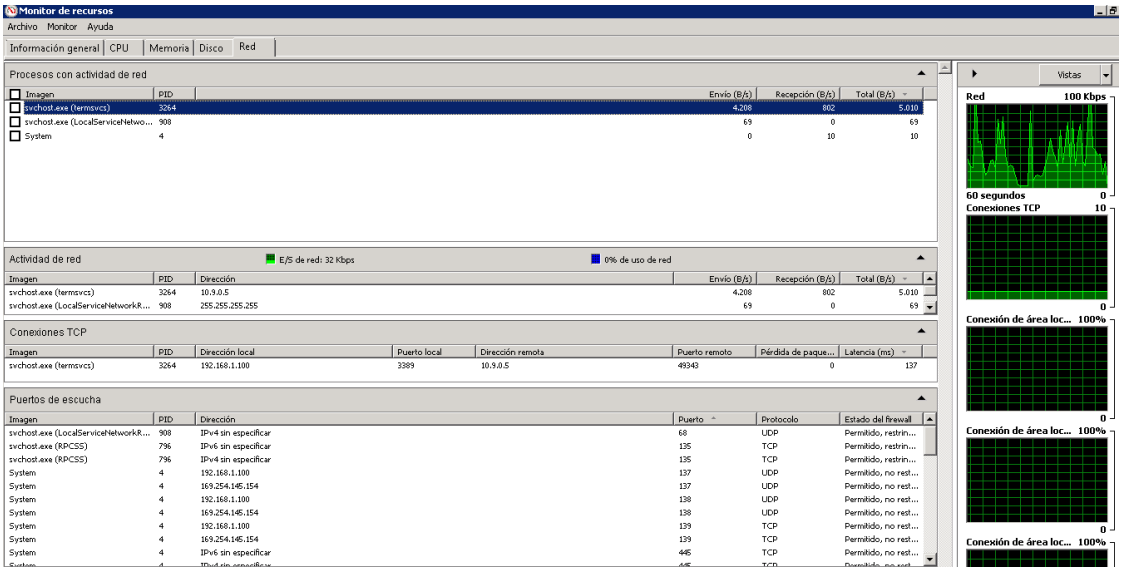


FIG. 41 MEDICION DE RENDIMIENTO SERVIDOR HYPER V

De igual manera toda esta información podemos corroborarla con la lectura de los lo del sistema operativo el cual nos dirá si éxito algún problema con el servicio de HYPER-V previamente instalado.

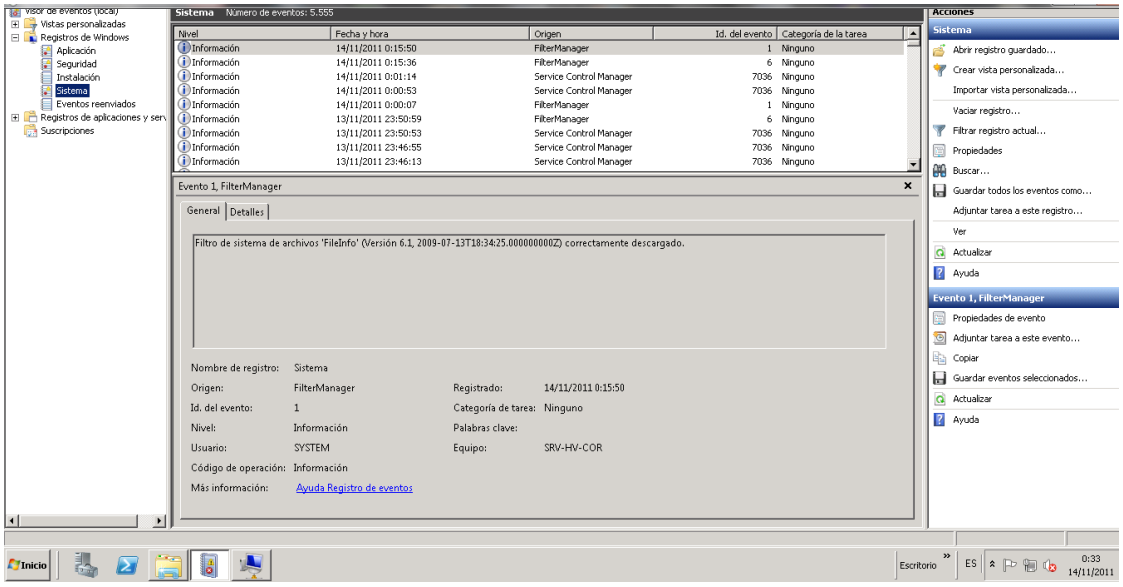


FIG. 42 MEDICION DE RENDIMIENTO SERVIDOR HYPER V

4.3.2 MONITOREO DE SERVIDOR VIRTUALIZADO SRV-DC-COR

En esta máquina virtual actualmente se encuentra levantado el servicio de Active Directory.

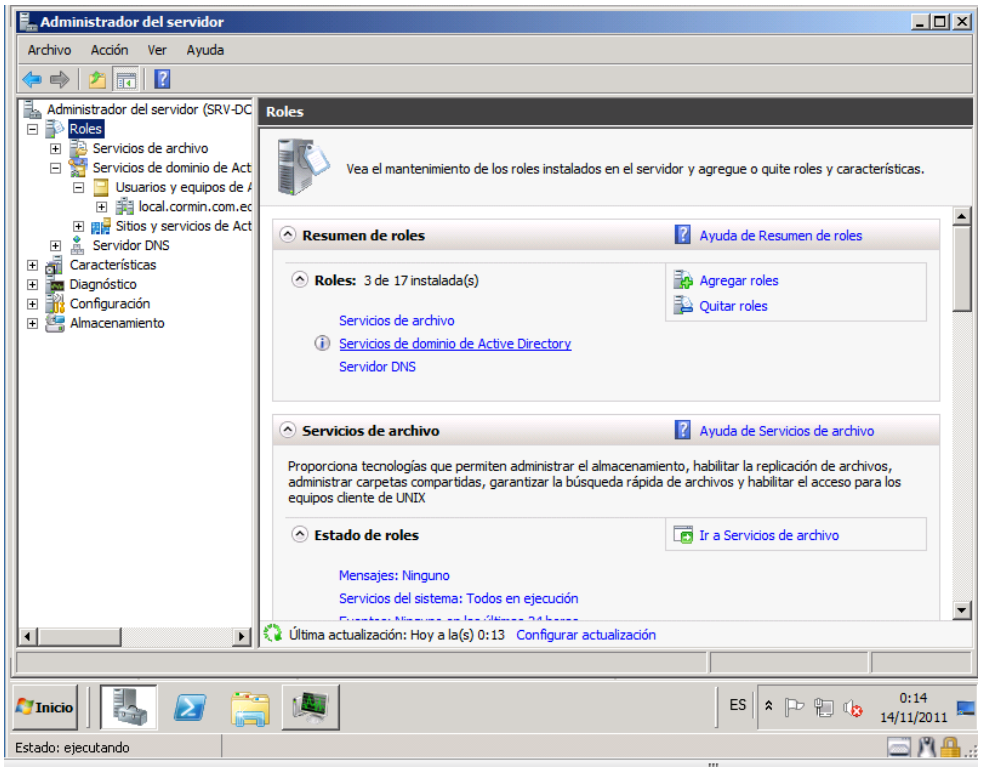


FIG. 43 MONITOREO DE RENDIMIENTO VM SRV-DC-COR

Administrador de Tareas de Windows.

Verificamos a pesar de estar virtualizado el servicio no se refleja mayor uso de recursos por parte de CPU únicamente se refleja un uso del 81% de la memoria física del equipo el cual para el servicio que se brinda actualmente es suficiente.

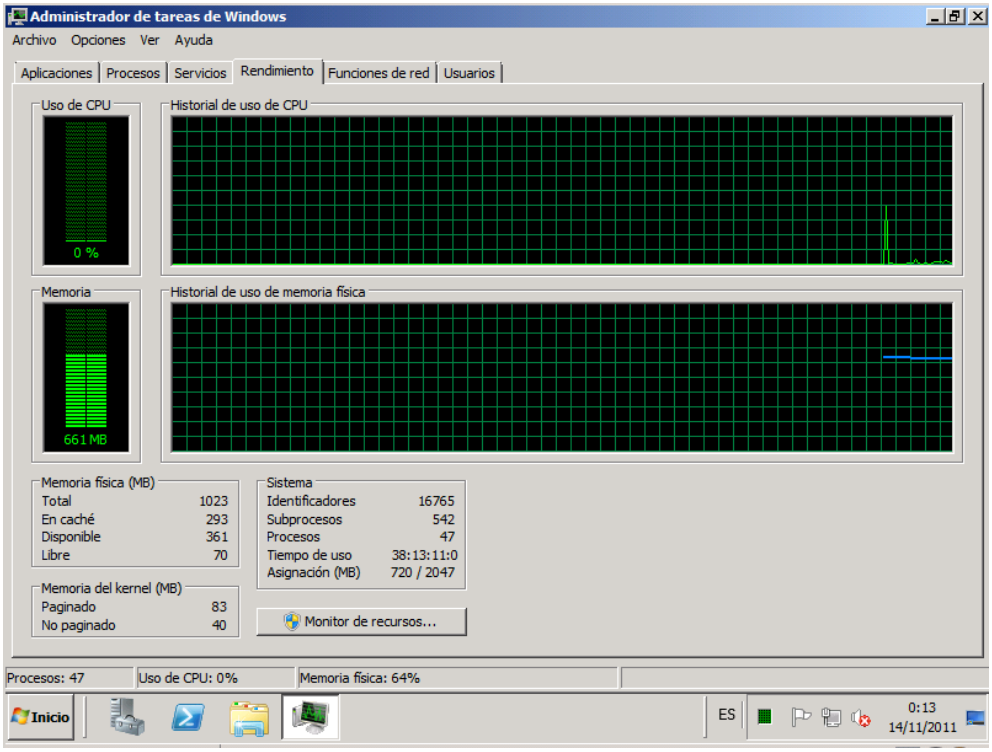


FIG.44 MONITOREO DE RENDIMIENTO VM SRV-DC-COR

En el Perfomance monitor podemos ver el uso del CPU en un maximo del 22%

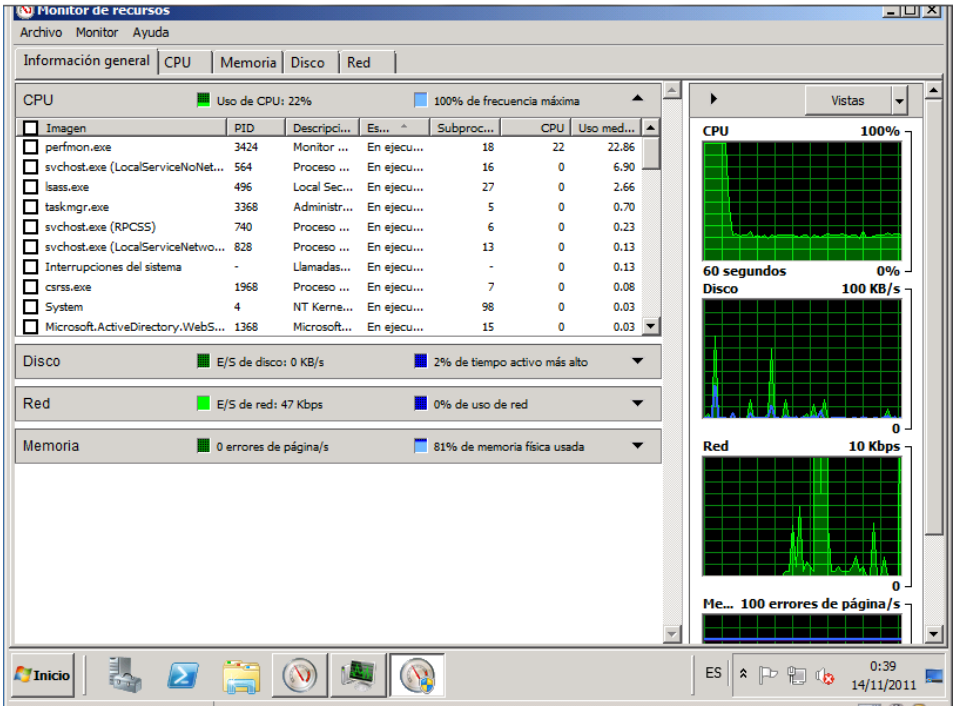


FIG. 45 MONITOREO DE RENDIMIENTO VM SRV-DC-COR

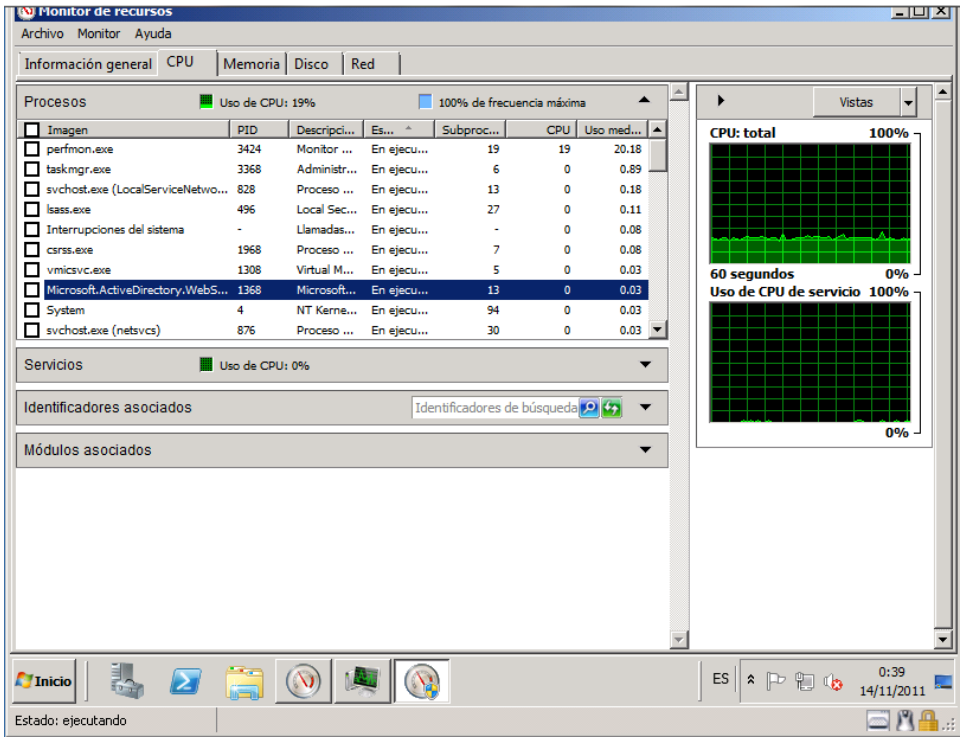


FIG. 46 MONITOREO DE RENDIMIENTO VM SRV-DC-COR

En el Perfomance monitor podemos ver el uso de la Memoria Fisica y disco.

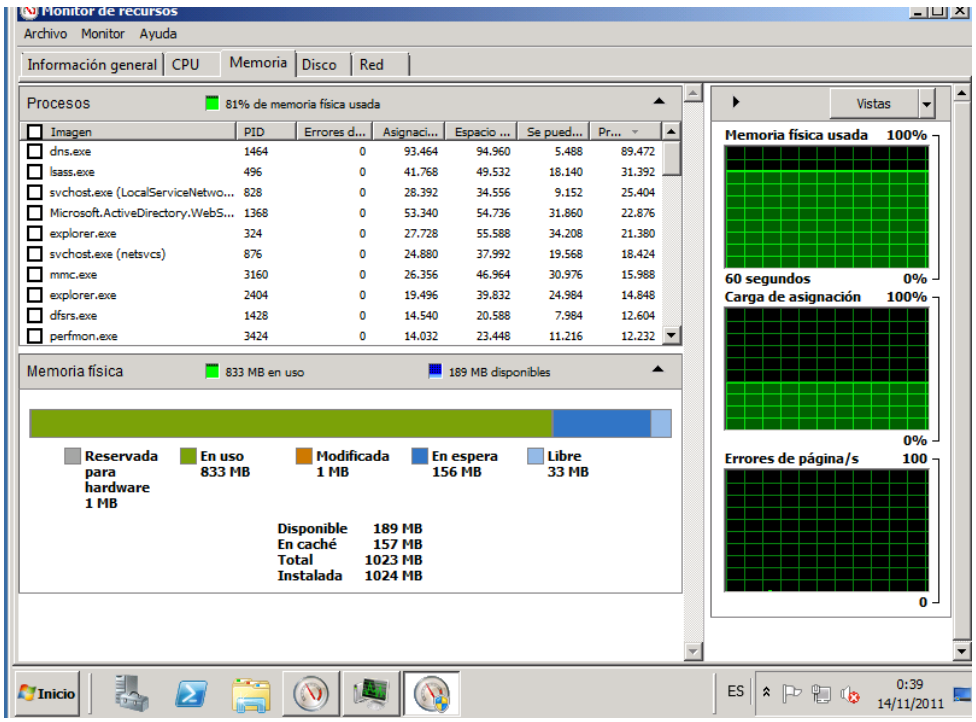


FIG. 47 MONITOREO DE RENDIMIENTO VM SRV-DC-COR

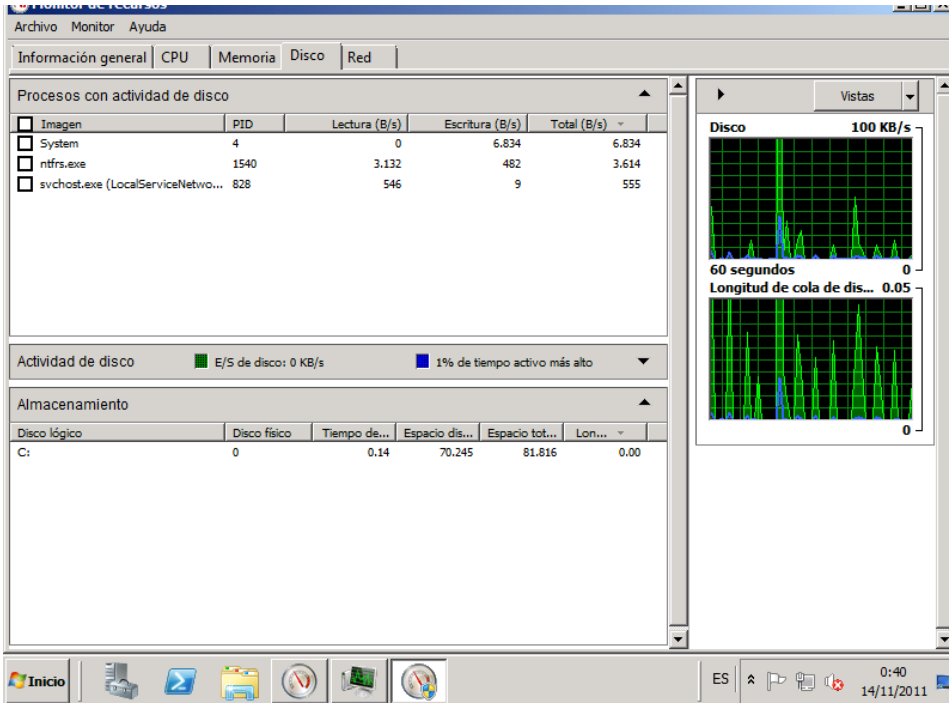


FIG. 48 MONITOREO DE RENDIMIENTO VM SRV-DC-COR

En el Perfomance monitor podemos ver el uso de la tarjeta de red.

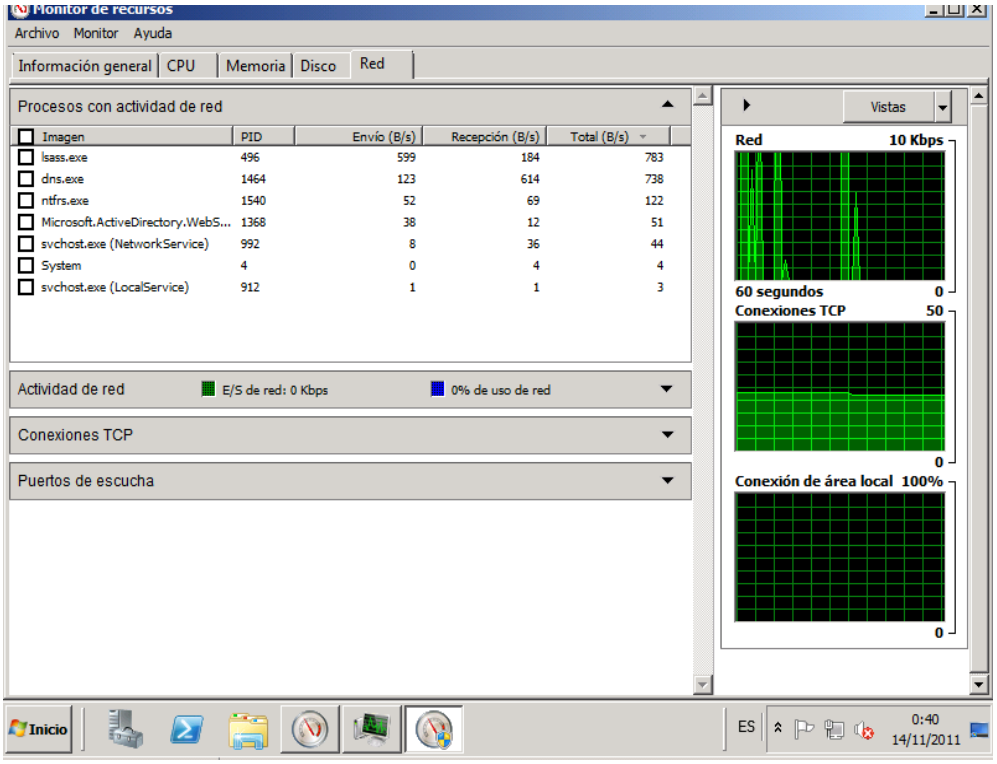


FIG. 49 MONITOREO DE RENDIMIENTO VM SRV-DC-COR

4.3.3 MONITOREO MAQUINA VIRTUAL SRV-DB-COR

Servicio instalado servidor de base de datos SQL

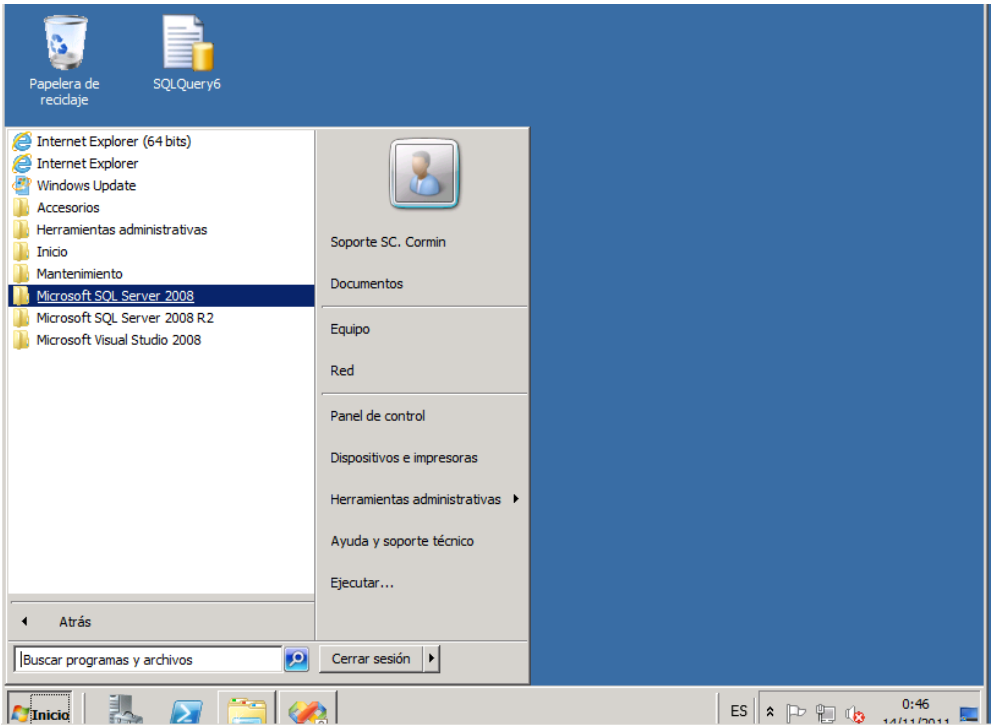


FIG. 50 MONITOREO DE RENDIMIENTO VM SRV-DB-COR

En la grafica podemos corroborar que el uso del cpu no supera el 10% no obstante la moria de 5gb esta siendo utilizada en un 94% esto debido a que el sql como tal esta reservando la mayor cantidad de memoria para que esta pueda ser utilizada en el momento que se requiera.

En el caso de necesitarse mas memoria ram se procedera a asgindar promeido de la consola de “HYPER-V”

En el Perfomance monitor podemos ver el uso del CPU

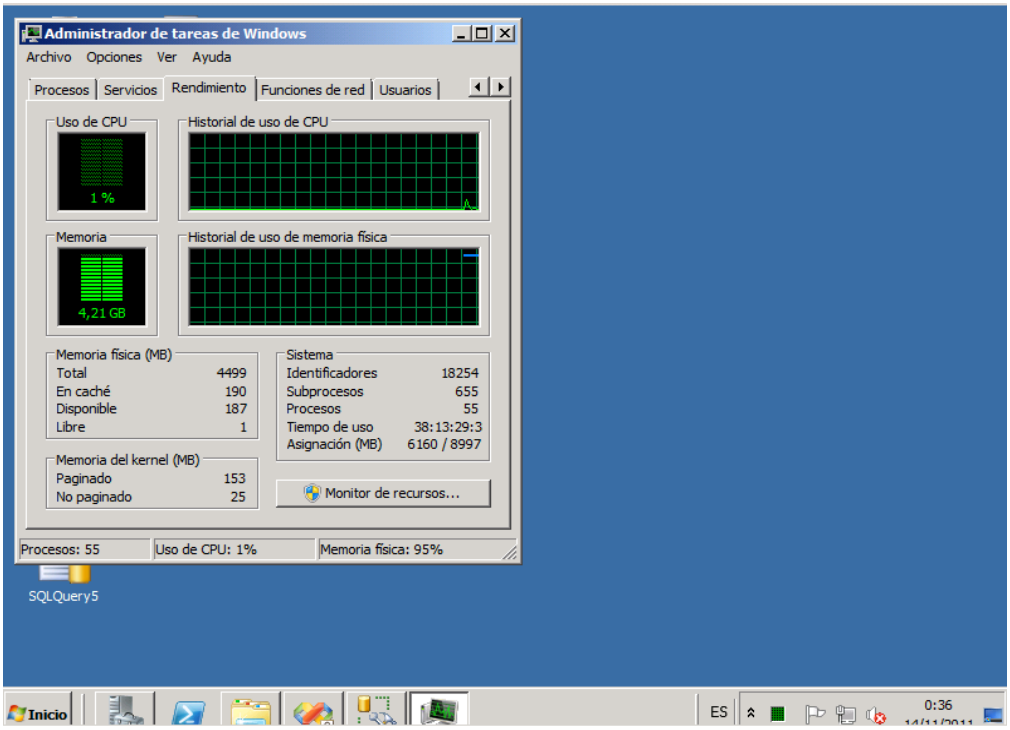


FIG. 51 MONITOREO DE RENDIMIENTO VM SRV-DB-COR

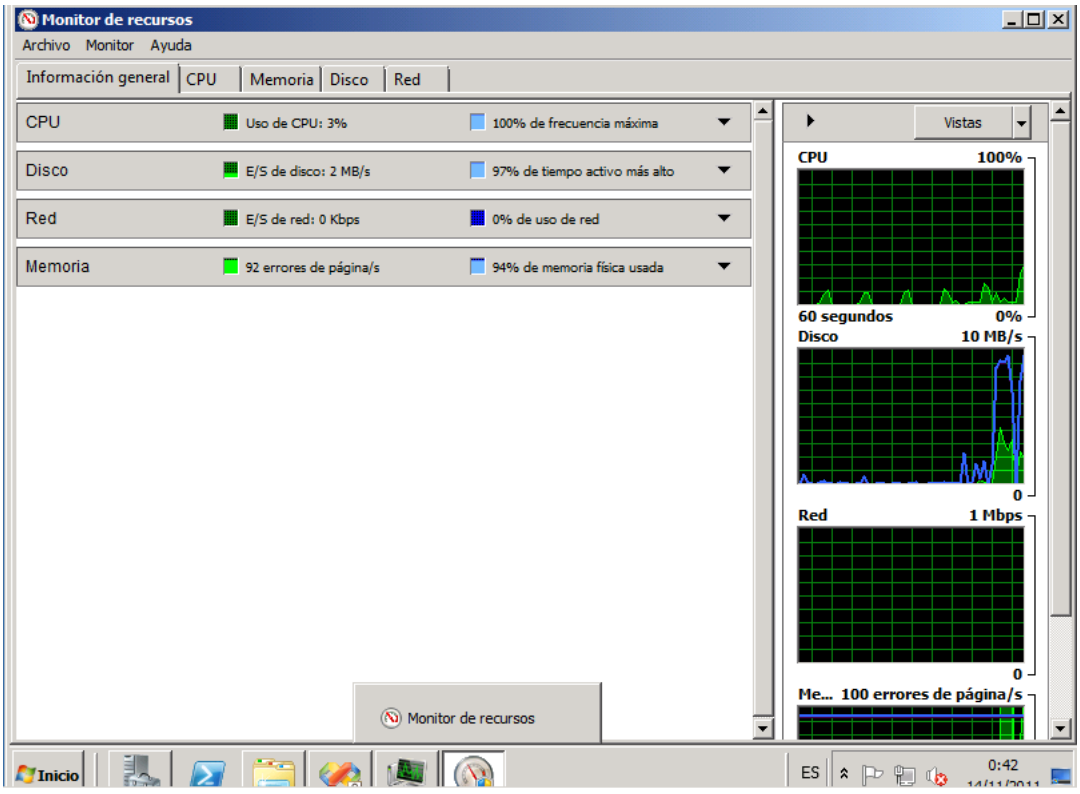


FIG. 52 MONITOREO DE RENDIMIENTO VM SRV-DB-COR

En el Perfomance monitor podemos ver el uso de la Memoria Fisica y disco.

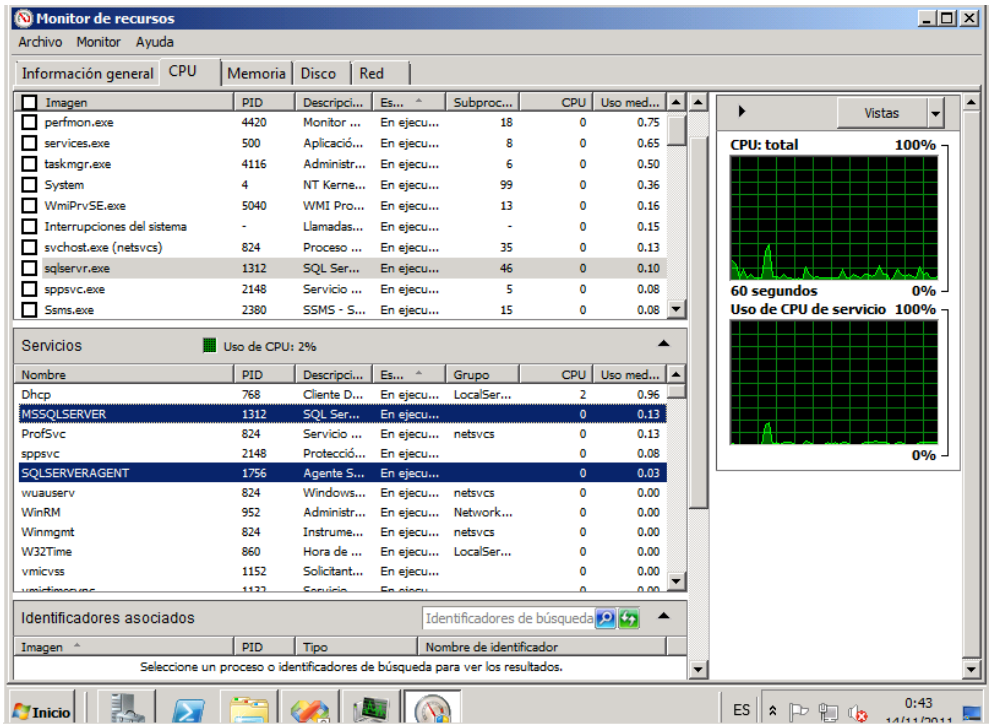


FIG.53 MONITOREO DE RENDIMIENTO VM SRV-DB-COR

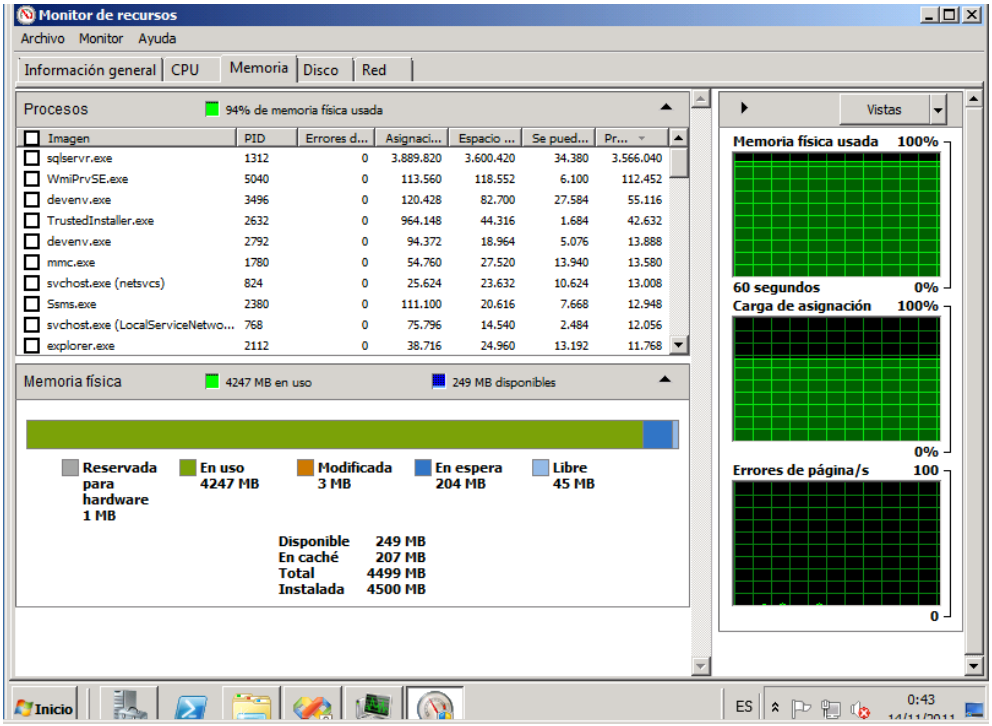


FIG. 54 MONITOREO DE RENDIMIENTO VM SRV-DB-COR

En el Perfomance monitor podemos ver el uso de recursos de red.

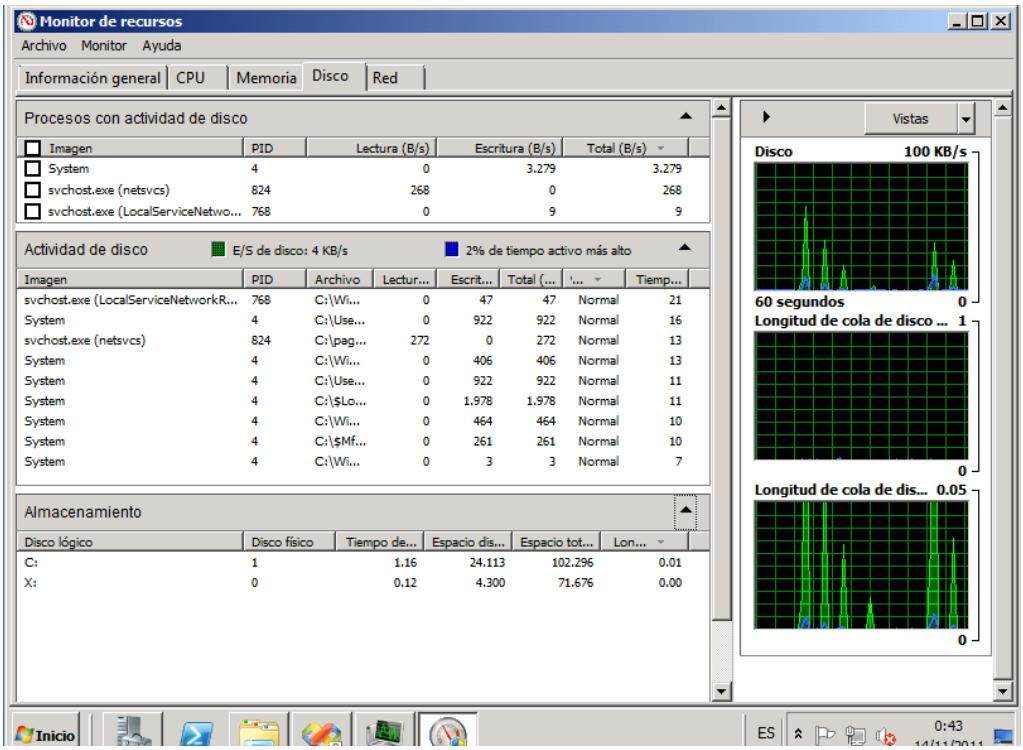


FIG. 55 MONITOREO DE RENDIMIENTO VM SRV-DB-COR

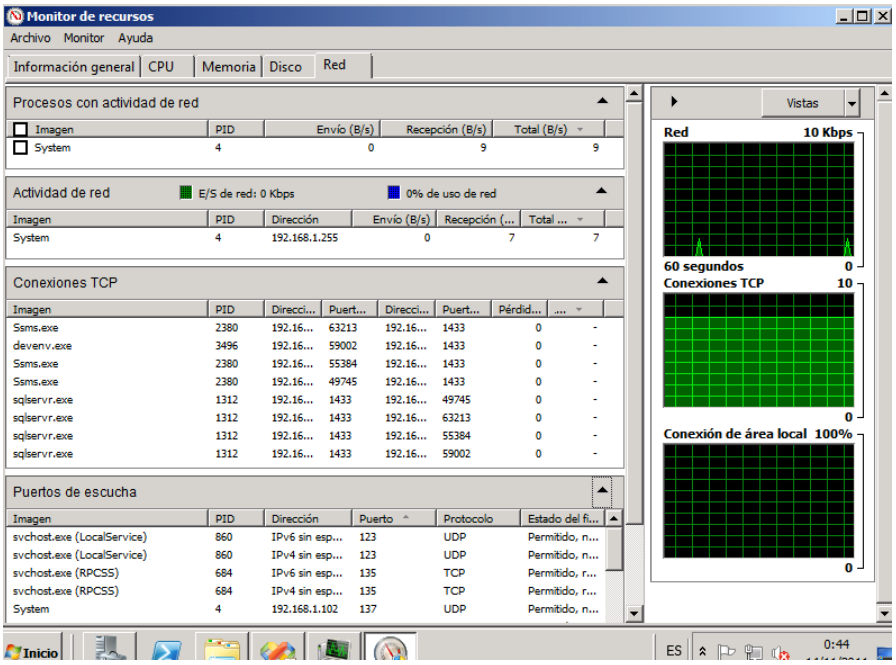


FIG.56 MONITOREO DE RENDIMIENTO VM SRV-DB-COR

4.4 MONITOREO DE ROUTER VPN

4.4.1 NETFLOW.

4.4.1.1 INTRODUCCION.

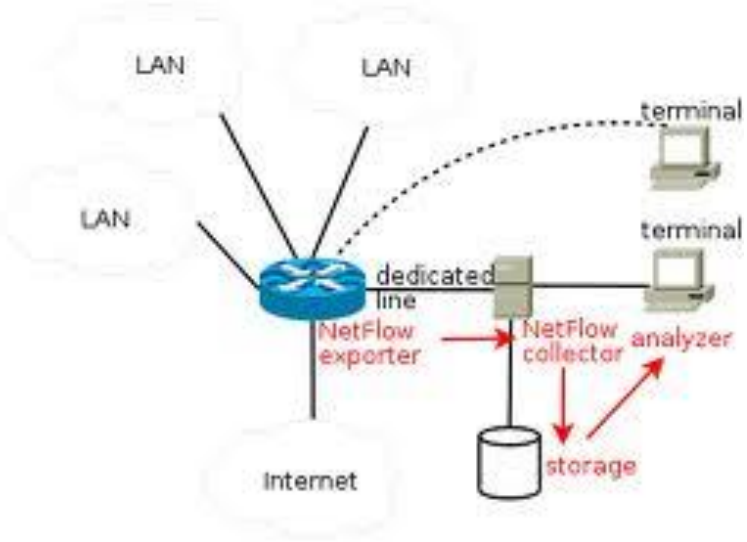


FIG.57 MONITOREO CONEXIÓN VPN

Se trata de un protocolo propietario de Cisco soportado en la actualidad por todas las líneas de switches y routers Cisco. Este protocolo permite a los dispositivos colectar información referida a todo tráfico que atraviesa los enlaces y enviar la información referida a ese tráfico utilizando “UDP” a un dispositivo que recibe la denominación de “NETFLOW” Collector.

La ventaja de “NETFLOW” respecto de “SNMP” es que este protocolo brinda, fundamentalmente, información y funcionalidades de management, mientras que a esa información “NETFLOW” le agrega la referida al tráfico que provoca el estado de utilización de cada dispositivo.

Entre las aplicaciones posibles de “NETFLOW” se pueden contar el monitoreo de la red, el monitoreo de aplicaciones específicas, el monitoreo de usuarios, el planeamiento de actualizaciones o modificaciones de la red, el análisis de seguridad, la implementación de sistemas de accounting y facturación, data warehousing y minig del tráfico de red, etc.

4.4.1.2 DESCRIPCION DE UN FLUJO (FLOW)

Cisco define un flujo de datos como una secuencia unidireccional de paquetes que comparten 5 elementos en común:

- Dirección IP de origen.
- Dirección IP destino.
- Número de puerto de origen.
- Número de puerto de destino.
- Protocolo.

Cisco llama a esta una "definición quíntuple de tráfico" en alusión a que se utilizan 5 elementos para la misma.

4.4.1.3 ¿QUÉ ES UN NETFLOW COLLECTOR?

Es de suponer que no sencillamente se desea coleccionar información, sino también (y por sobre todo) analizar los estadísticas y características de esta información de tráfico.

Para esto es que requerimos de un “NETFLOW” Collector. Se trata de un dispositivo (PC o servidor) ubicado en la red para recoger toda la información de “NETFLOW” que es enviada desde los dispositivos de infraestructura (routers y switches).

“NETFLOW” es un protocolo que genera y recoge esta información, pero también se necesita software que permita realizar la clasificación, almacenamiento y análisis de toda esta información de tráfico. Para esto hay en el mercado una amplia diversidad (por prestaciones y precio) de aplicaciones en el mercado que permiten trabajar sobre la información de “NETFLOW2:

- MARS - Cisco Security Monitoring, Analysis and Response System. Aplicativo de Cisco que a partir de la información obtenida por “NETFLOW” permite monitorear la red y generar respuesta a eventos de seguridad.
- Lista de aplicaciones desarrolladas por terceras partes, informada por Cisco.
- Lista de aplicaciones gratuitas, informada por Cisco.

4.4.1.4 MONITOREO CON NETFLOW

Mediante la herramienta de “NETFLOW” procederemos a registrar cual es el tipo de aplicaciones, protocolo, “IP” y puerto de origen y destino, la cantida de tráfico que vamos a necesitar para poder administrar nuestro servidor remotamente y poder dar el soporte.

Como habíamos mencionado en capítulos anteriores, nosotros para nuestra conexión “VPN” vamos a utilizar un Router Cisco 1811.

En esta grafica podemos ver que nuestro router en una prueba de administración de nuestra Máquina virtual puede llegar a consumir hasta un 4% de su “CPU”, ademas cabe recalcar que el router únicamente realiza la función de server “VPN”, por lo cual dicho consumo de “CPU”.

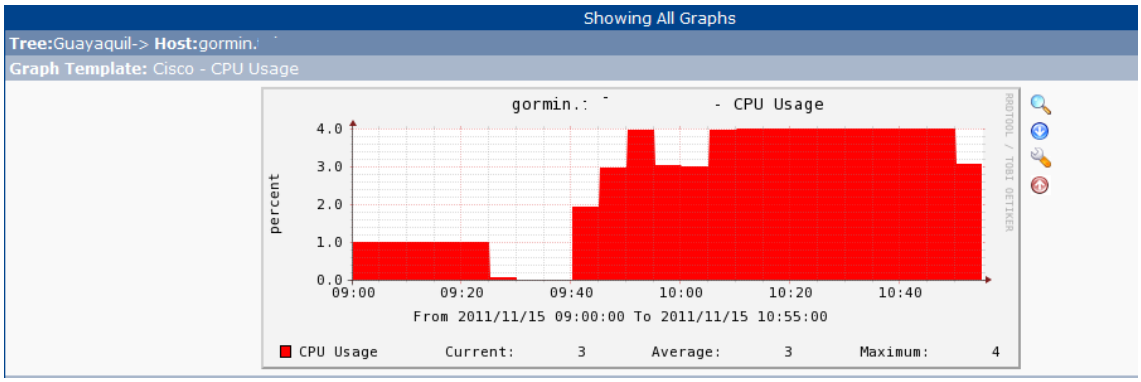


FIG. 58 MONITOREO CONEXIÓN VPN

En otra grafica podemos ver cuánto es al ancho de banda que está ocupando nuestro Router Cisco para la administración, teniendo un promedio de 177 Kb en tráfico de bajada y 63 Kb de subida.

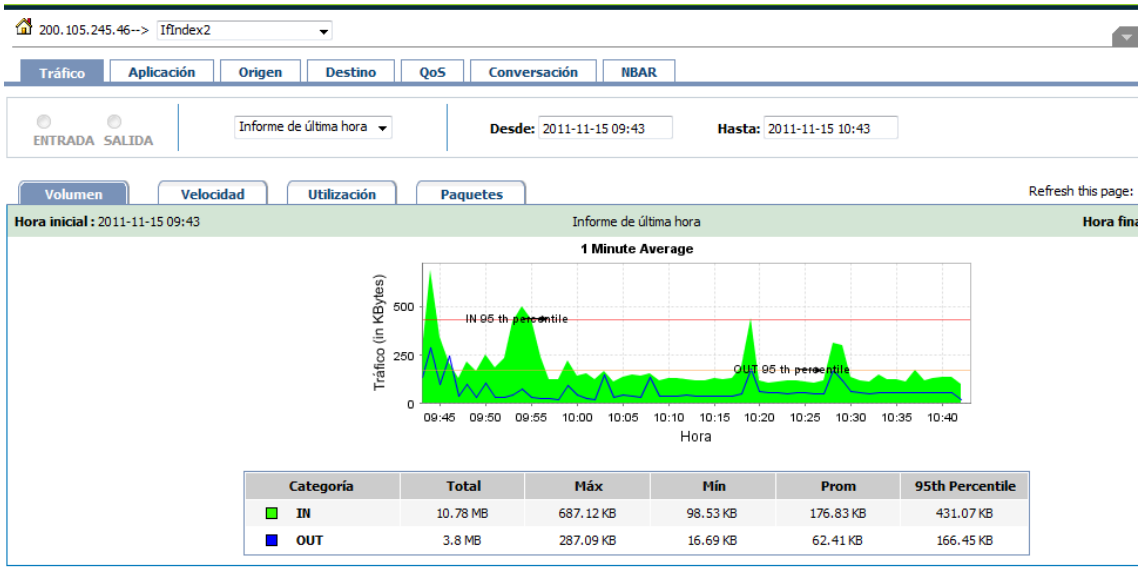


FIG. 59 MONITOREO CONEXIÓN VPN

Por lo cual se recomienda tener en el site remoto de donde uno se conecta un ancho de banda de bajada mínimo de 128 Kb, lo recomendable seria 256 Kb, pues como podemos ver tenemos picos que alanzan a veces hasta los 512, además de en nuestra matriz nuestro servidor debe tener acceso a internet mínimo de 128 Kb por usuario que se vaya a conectar, es decir si tenemos 3 administradores remotos y los 3 se conectan a las vez, el servidor debe tener como mínimo para estas 3 conexiones un mínimos de 384 Kb y un recomendable de 768 Kb, solo para administración por escritorio remoto.

En la siguiente grafica podemos ver los protocolos que se están utilizando, los que consumes mayor ancho de banda son los 3 primeros.

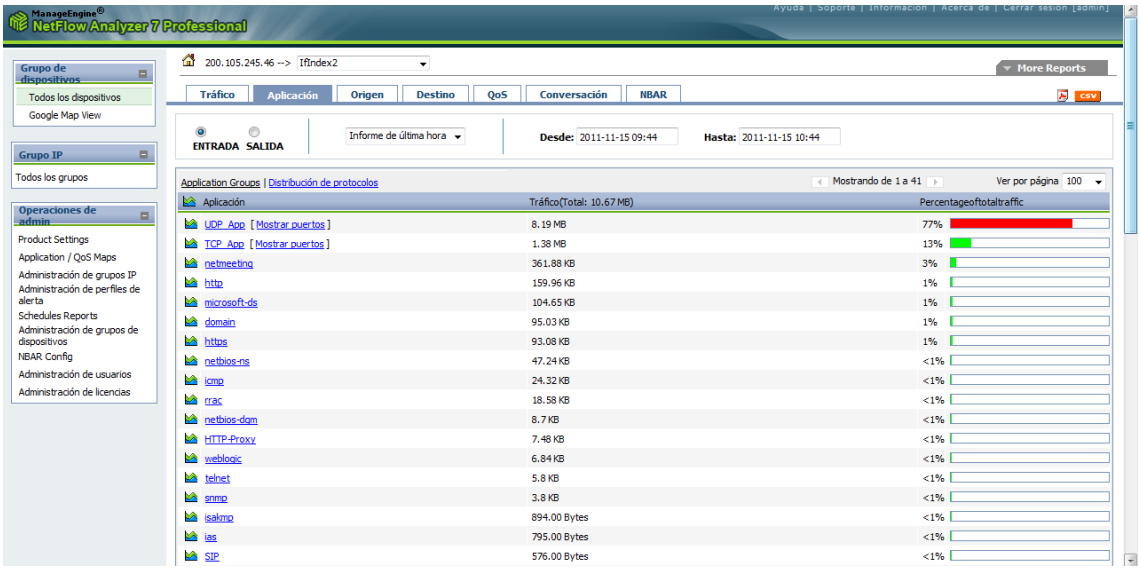


FIG. 60 MONITOREO CONEXIÓN VPN

“UDP” es el protocolo que mayor ancho de banda está consumiendo ya que mediante este levantamos la “VPN”, el siguiente es el protocolo “TCP”, seguido

del netmeeting, ya que mediante este podemos hacer un escritorio remoto con el servido virtualizado.

Además tenemos un gráfico de pastel en el cual podemos ver todos los protocolos que más se están usando, confirmando el análisis de la gráfica anterior.

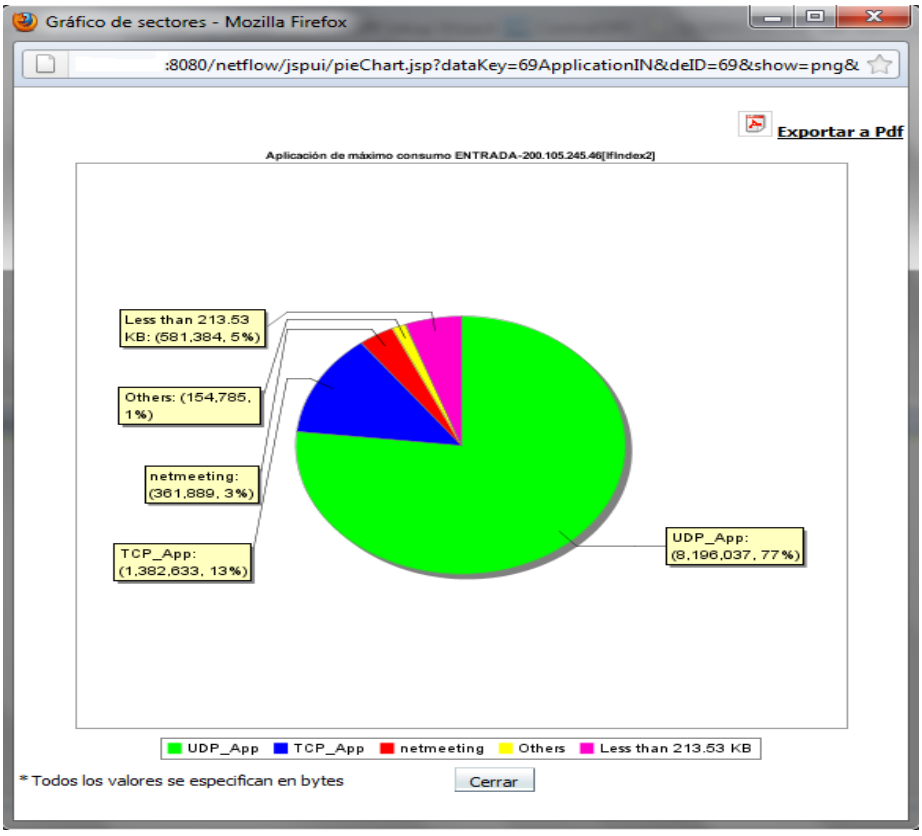
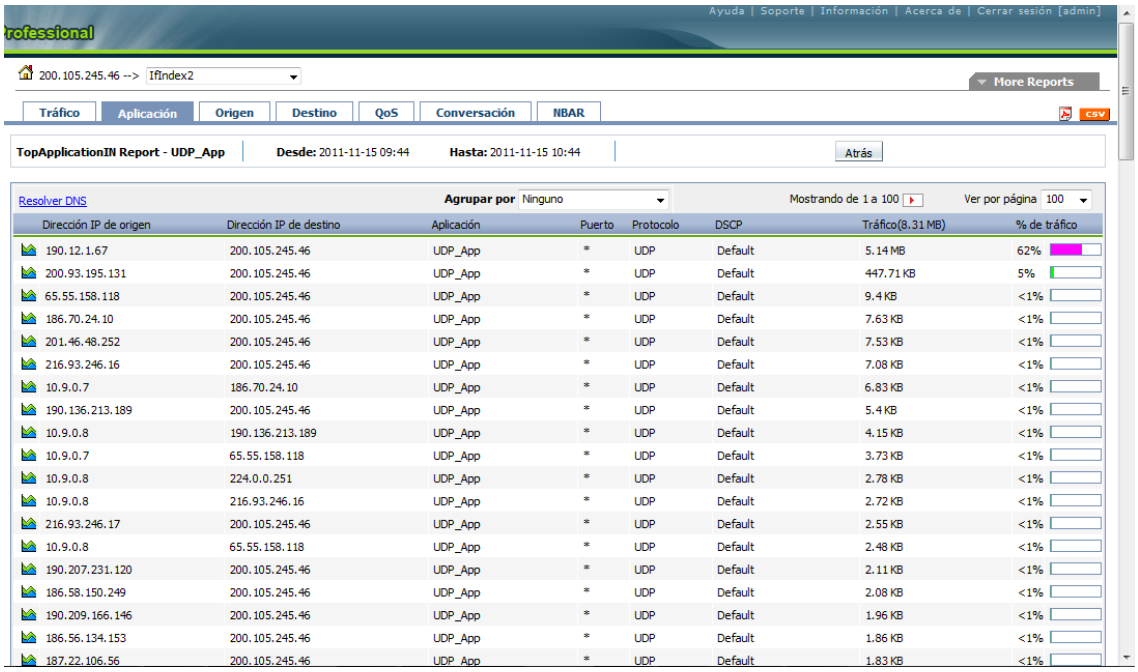


FIG. 61 MONITOREO CONEXIÓN VPN



Dirección IP de origen	Dirección IP de destino	Aplicación	Puerto	Protocolo	DSCP	Tráfico(8.31 MB)	% de tráfico
190.12.1.67	200.105.245.46	UDP_App	*	UDP	Default	5.14 MB	62%
200.93.195.131	200.105.245.46	UDP_App	*	UDP	Default	447.71 KB	5%
65.55.158.118	200.105.245.46	UDP_App	*	UDP	Default	9.4 KB	<1%
186.70.24.10	200.105.245.46	UDP_App	*	UDP	Default	7.63 KB	<1%
201.46.48.252	200.105.245.46	UDP_App	*	UDP	Default	7.53 KB	<1%
216.93.246.16	200.105.245.46	UDP_App	*	UDP	Default	7.08 KB	<1%
10.9.0.7	186.70.24.10	UDP_App	*	UDP	Default	6.83 KB	<1%
190.136.213.189	200.105.245.46	UDP_App	*	UDP	Default	5.4 KB	<1%
10.9.0.8	190.136.213.189	UDP_App	*	UDP	Default	4.15 KB	<1%
10.9.0.7	65.55.158.118	UDP_App	*	UDP	Default	3.73 KB	<1%
10.9.0.8	224.0.0.251	UDP_App	*	UDP	Default	2.78 KB	<1%
10.9.0.8	216.93.246.16	UDP_App	*	UDP	Default	2.72 KB	<1%
216.93.246.17	200.105.245.46	UDP_App	*	UDP	Default	2.55 KB	<1%
10.9.0.8	65.55.158.118	UDP_App	*	UDP	Default	2.48 KB	<1%
190.207.231.120	200.105.245.46	UDP_App	*	UDP	Default	2.11 KB	<1%
186.58.150.249	200.105.245.46	UDP_App	*	UDP	Default	2.08 KB	<1%
190.209.166.146	200.105.245.46	UDP_App	*	UDP	Default	1.96 KB	<1%
186.56.134.153	200.105.245.46	UDP_App	*	UDP	Default	1.86 KB	<1%
187.22.106.56	200.105.245.46	UDP_App	*	UDP	Default	1.83 KB	<1%

FIG. 62 MONITOREO CONEXIÓN VPN

En esta gragica podemos ver la IP publica (190.12.1.67) con la cual nos estamos conectando para levantar nuestro tunel “VPN” siendo esta nuestra IP origen y la IP 200.105.245.46 nuestra IP destino, como ya lo comentamos el protocolo “UDP” es el que usamos para levantar nuestra “VPN”.

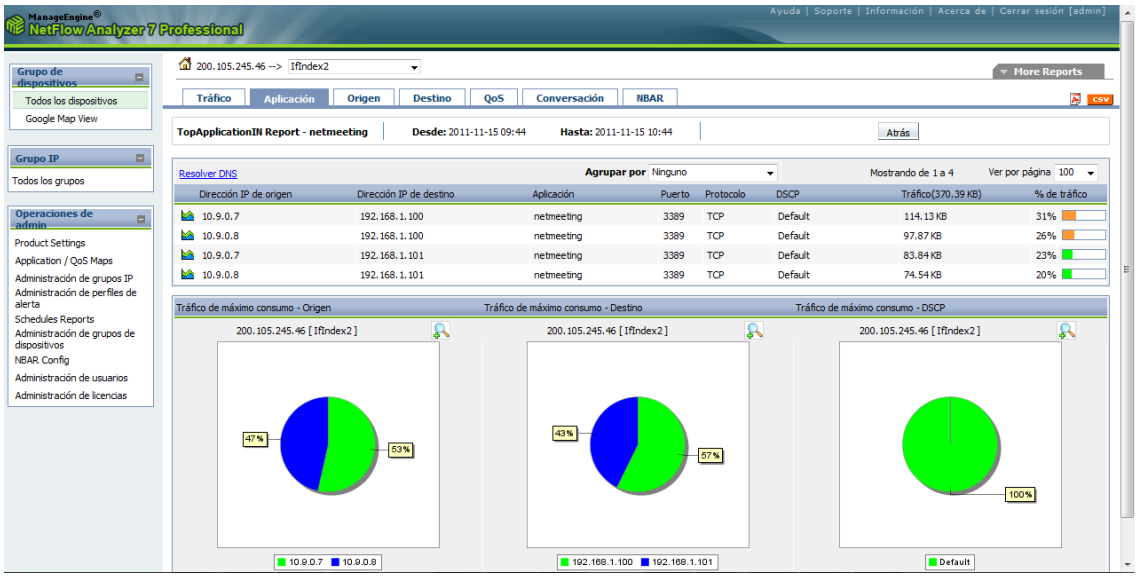


FIG 63 MONITOREO CONEXIÓN VPN

En el netflow el “RDP” (remote Desktop Protocol) lo reconoce como netmeeting, pues si nos damos cuenta utiliza el mismo protocolo y mismo puertos, si nos damos cuenta al conectarnos a nuestra “VPN” por “DHCP” nos esta asignando a nuestra maquina la red 10.9.0.0/ 24 (IP origen) y nos conectamos por “RDP” a la IP 192.168.1.100 que es nuestro servidor virtual y la IP 192.168.1.101 es uno de nuestros host virtualizados.

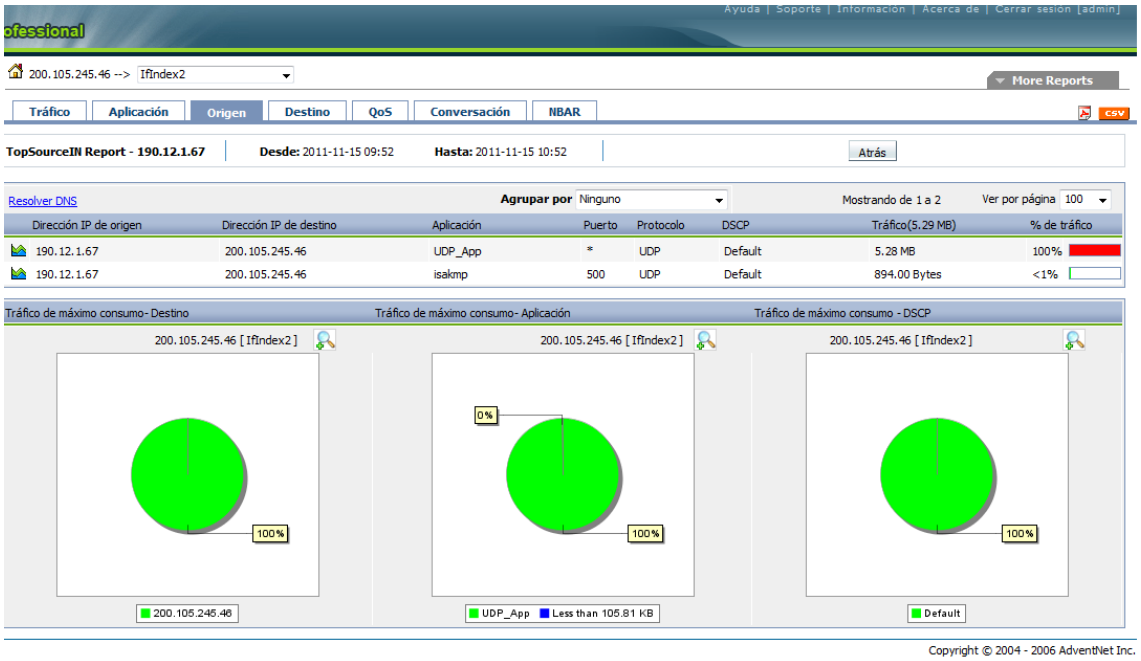
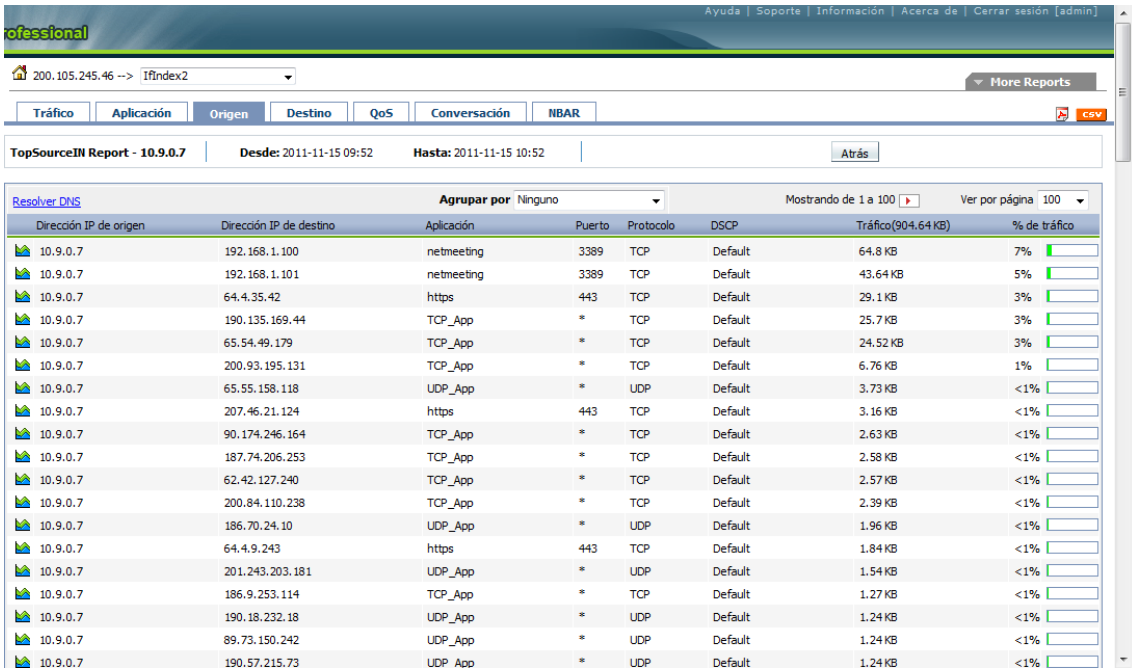


FIG. 64 MONITOREO CONEXIÓN VPN

En esta grafica podemos constatar que con la “IP” pública que no conectamos (190.12.1.67) usamos el protocolo “UDP” para establecer la conexión con nuestro router (200.105.245.46), además un dato importante es que visualizamos nuestro protocolo usado para la autenticación “ISAKMP” (usado en el “IPSEC”).



Dirección IP de origen	Dirección IP de destino	Aplicación	Puerto	Protocolo	DSCP	Tráfico(904.64 KB)	% de tráfico
10.9.0.7	192.168.1.100	netmeeting	3389	TCP	Default	64.8 KB	7%
10.9.0.7	192.168.1.101	netmeeting	3389	TCP	Default	43.64 KB	5%
10.9.0.7	64.4.35.42	https	443	TCP	Default	29.1 KB	3%
10.9.0.7	190.135.169.44	TCP_App	*	TCP	Default	25.7 KB	3%
10.9.0.7	65.54.49.179	TCP_App	*	TCP	Default	24.52 KB	3%
10.9.0.7	200.93.195.131	TCP_App	*	TCP	Default	6.76 KB	1%
10.9.0.7	65.55.158.118	UDP_App	*	UDP	Default	3.73 KB	<1%
10.9.0.7	207.46.21.124	https	443	TCP	Default	3.16 KB	<1%
10.9.0.7	90.174.246.164	TCP_App	*	TCP	Default	2.63 KB	<1%
10.9.0.7	187.74.206.253	TCP_App	*	TCP	Default	2.58 KB	<1%
10.9.0.7	62.42.127.240	TCP_App	*	TCP	Default	2.57 KB	<1%
10.9.0.7	200.84.110.238	TCP_App	*	TCP	Default	2.39 KB	<1%
10.9.0.7	186.70.24.10	UDP_App	*	UDP	Default	1.96 KB	<1%
10.9.0.7	64.4.9.243	https	443	TCP	Default	1.84 KB	<1%
10.9.0.7	201.243.203.181	UDP_App	*	UDP	Default	1.54 KB	<1%
10.9.0.7	186.9.253.114	TCP_App	*	TCP	Default	1.27 KB	<1%
10.9.0.7	190.18.232.18	UDP_App	*	UDP	Default	1.24 KB	<1%
10.9.0.7	89.73.150.242	UDP_App	*	UDP	Default	1.24 KB	<1%
10.9.0.7	190.57.215.73	UDP_App	*	UDP	Default	1.24 KB	<1%

FIG. 65 MONITOREO CONEXIÓN VPN

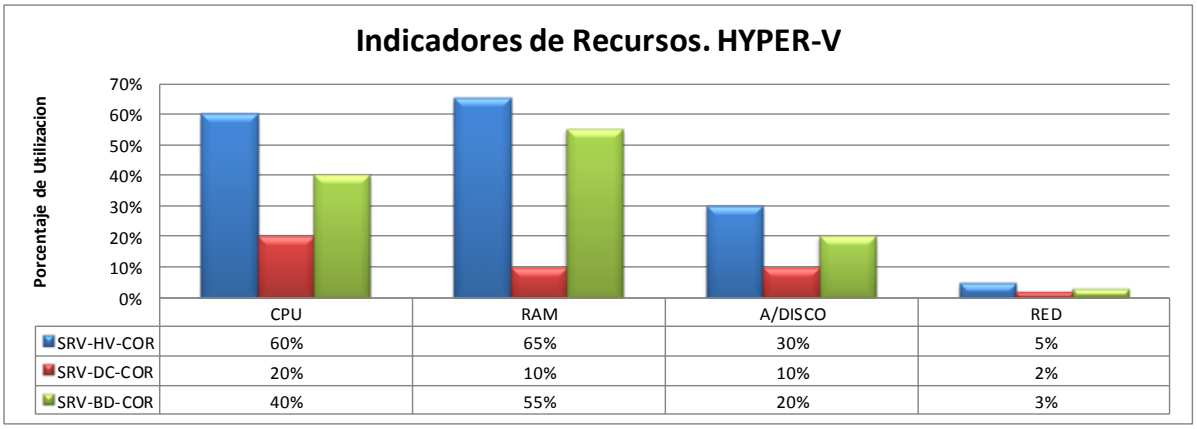
En esta grafica podemos ver como la IP que se nos asignó via “DHCP” al conectarnos a la “VPN” tienen acceso a la red 192.168.1.0/24 donde están los servidores y además tiene acceso para salir al internet. De tal forma confirmamos que el ancho de banda mínimo para establecer la conexión y administración de nuestras máquinas virtuales.

CAPÍTULO 5

5 INDICADORES

5.1 INDICADORES HYPER-V.

En la siguiente grafica se muestra el resumen de monitoreo del rendimiento tanto de nuestros servidor “HOST” como de nuestros servidores “GUEST”.



	CPU	RAM	A/DISCO	RED
SRV-HV-COR	60%	65%	30%	5%
SRV-DC-COR	20%	10%	10%	2%
SRV-BD-COR	40%	55%	20%	3%

Como podemos apreciar en nuestra grafica tenemos separadas los recursos como CPU, RAM. Disco y Red, los mismos que han sido asignados con diferentes valores a cada “GUEST”.

Podemos decir con respecto del CPU, que del 60 % de Procesos del “HOST” un 33.33 % (20/60=0.3333) de procesos totales están siendo utilizados por el DC y un 66.66 % (40/60= 0.6666) de procesos totales están siendo utilizados,

cabe recalcar que estos valores han sido sacados en horas donde las transacciones hacia cada servidor es más concurrente, además que sobre todo no siempre llegan a ocupar al 100 % sus recursos asignados.

Con respecto a la RAM, podemos decir que del 65 % de uso del “HOST” un 15.40% (10/65=0.1539) de estos recursos están siendo asignados al DC pero solo un 7.5% de los asignado está siendo usado, ya que si revisamos las gráficas en el capítulo 4 el “GUEST” no ocupa los 2 GB asignados sino 996 Mb de RAM, comparados con el 84.60% (55/65=0.8461) asignados a la BD, que del valor asignado llega a ocupar por lo general entre el 70% a 80% asignado es decir entre 3.2 Gb – 3.6 Gb de RAM.

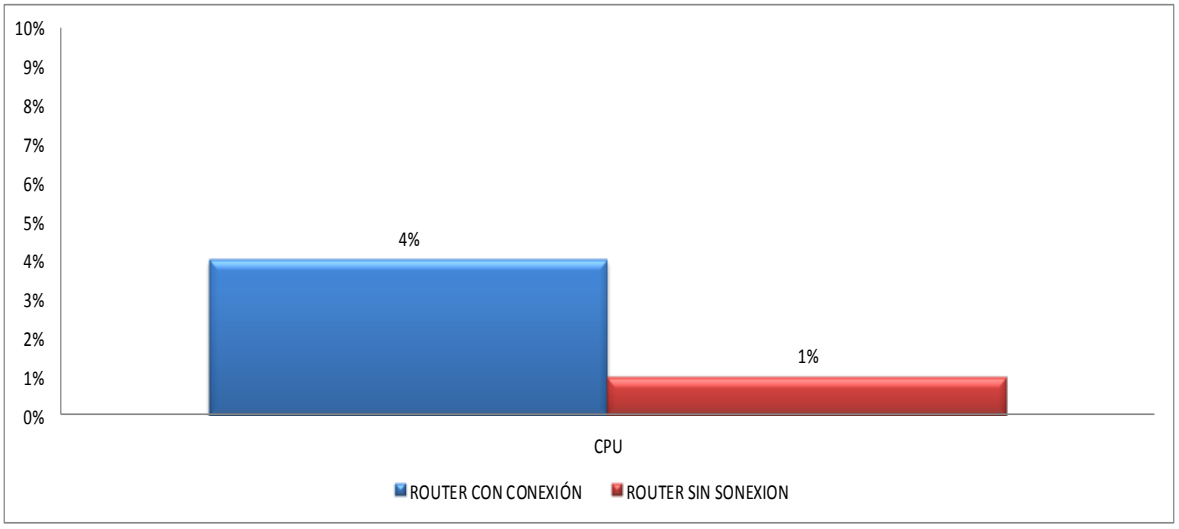
A nivel del disco, podemos decir que del 30 % usado del “HOST” un 33.33% fue asignada para el DC y un 66.66% fue asignado a la BD, un punto que tomar en cuenta es que la BD realiza más escritura en disco comparado con el DC.

En la tarjeta de red del “HOST” 10/100/1000, se ha asignado tarjetas 10/100 para los “GUEST” ocupando un 5% total del 1GB, de los cuales el 40% de las conexiones son provenientes del DC y el 60 % son de la BD de datos.

Si comparamos la MV, con un equipo físico, estamos administrando de una mejor manera los recursos ya que si el DC no los usara podrain ser asignados a la BD, en el caso del equipo físico, nos tocaria realizar una buena dimensión antes de implementar la solución y ver un equipo que peuda ser tan escalable, pero con la virtualziacion únicamente asignamso recursos.

5.2 INDICADORES MONITOREO.

Para nuestro Router cisco 1811 podemos realizar indicadores tomando el mismo perfil pero diferenciando en el momento de que realziamos el monitoreo y cuando no lo hacemos.



En la gráfica podemos ver a simple vista que cuando nosotros nos conectamos a la VPN nuestro equipo únicamente usa el 4 % de CPU no existe la conexión únicamente utiliza el 1 %, en el proceso de monitoreo se realizó pruebas de subir y levantar máquinas virtuales, crear uan copia de una amquina virtual y durante todo este proceso nunca paso del 5 % el CPU del Router cisco, cabe tomar en cuenta que solo se realizó una conexión, por lo cual podríamos decir que por cada administrador conectado podríamos está utilizando hasta 4 % de recursos del equipos, es decir que podríamos tener hasta 15 administradores conectados antes que afecte los recursos de CPU del equipo.

Otro valor importante es la Ancho de banda a utilizar según las pruebas realizadas y el monitoreo con el Netflow con 128 Kb era suficiente para iniciar nuestra conexión VPN, pero existen pico en los cuales recomendamos 192Kb

por conexión, si queremos que más administradores se conecten podemos tener una conexión 1:1 de 1MB y podemos llegar a conectar hasta 12 personas, a nivel de capacidad del equipo permite hasta 52 conexiones simultaneas.

CONCLUSIONES.

1. La “VIRTUALIZACIÓN” es la solución donde convergen resultados económicos y de calidad que sirve de interfaz directa hacia sus clientes. Debido a la productividad que puede tener una infraestructura virtualizada, incrementa la versatilidad del negocio ya que brinda mayores facilidades de adaptación a las nuevas y cambiantes necesidades de la empresa como consecuencia podemos realizar mejoras en la calidad del servicio y ubicar a la “VIRTUALIZACIÓN” en una posición competitiva ante el mercado.

2. Entre las principales características de la “VIRTUALIZACIÓN” es el aprovechamiento mayor de la potencia de cómputo de las máquinas físicas y la velocidad con la que se comunican las máquinas, que al estar ejecutándose sobre la misma máquina física no dependerán del ancho de banda de una red Ethernet por ejemplo, sino del ancho de banda del bus de la propia máquina física, además se obtiene un sistema ampliamente escalable, es decir, si se requieren más máquinas, estás pueden ser máquinas virtuales. De esta forma, no se incurre en más gastos, ni se necesita más espacio físico para alojar otra máquina física.

3. Nuestra “VPN” es una tecnología que podemos usar para conectarnos a nuestro trabajo de una forma seguro y sobre todo abaratando costos ya que

con un simple servicio de internet podemos estar conectados remotamente hacia nuestros servidores de producción.

4. Con la conexión a través de la “VPN” podemos trabajar desde cualquier sitio, pudiendo de tal formar administrar nuestras Máquinas virtuales como si estuviéramos detrás de nuestro servidor, optimizando así nuestros tiempos de respuesta ante cualquier incidencia.

RECOMENDACIONES

1. Cuando trabajamos en un ambiente virtualizado siempre debemos considerar los niveles de contingencia ya que varios de nuestros servidores dependen de un equipo físico por ello se recomienda manejar esquemas de clúster entre equipos “HOST” del tiempo de respuesta que puede ser brindado.

2. En almacenamiento de nuestros equipos virtuales es preferible que se aloje dentro de una “SAN” para de esta forma en el caso de existir algún problema con el “HOST” podamos redirigir nuestras maquinas hacia otro equipo y estas puedan levantarse sin problema alguno con un mínimo tiempo de caída.

3. Los niveles de seguridad adecuados a nivel de autenticación, autorización y cifrado deben ser lo más adecuados ya que el internet es tan fácil poner un “SNIFFER” y capturar todo tipo de información que pase por la red, en toda red hay un hacker que quiere saber más.

4. Al momento de crear cuentas de usuarios las contraseñas no deben ser tan cortas ni usar palabras de diccionarios, además de asignar privilegios menores en el router.

GLOSARIO.

ACL.-Una lista de control de acceso o ACL (del inglés, *access control list*) es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

Las ACL permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición. Sin embargo, también tienen usos adicionales, como por ejemplo, distinguir "tráfico interesante" (tráfico suficientemente importante como para activar o mantener una conexión) en RDSI.

ACTIVE DIRECTORY: Active Directory (AD).- es el término que usa Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos (principalmenteLDAP, DNS, DHCP, Kerberos...).

Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.

Active Directory permite a los administradores establecer políticas a nivel de empresa, desplegar programas en muchos ordenadores y aplicar actualizaciones críticas a una organización entera. Un Active Directory almacena información de una organización en una base de datos central, organizada y accesible. Pueden encontrarse desde directorios con cientos de objetos para una red pequeña hasta directorios con millones de objetos.

ATM.- El Modo de Transferencia Asíncrona o Asynchronous Transfer Mode (ATM) es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

BIOS.- El BIOS (sigla en inglés de basic input/output system; en español "sistema básico de entrada y salida") es un software que localiza y reconoce todos los dispositivos necesarios para cargar el sistema operativo en la memoria RAM.

CHAP.- Protocolo de encapsulamiento Point to Point. Realiza comprobaciones periódicas para asegurarse de que el nodo remoto todavía posee un valor de contraseña válido. El valor de la contraseña es variable y cambia impredeciblemente mientras el enlace existe.

CDP.- CDP (*Cisco Discovery Protocol*, 'protocolo de descubrimiento de Cisco', es un protocolo de red propietario de nivel 2, desarrollado por Cisco Systems y usado en la mayoría de sus equipos. Es utilizado para compartir información sobre otros equipos Cisco directamente conectados, tal como la versión del sistema operativo y la dirección IP. CDP también puede ser usado para realizar encaminamiento bajo demanda (ODR, *On-Demand Routing*), que es un método para incluir información de encaminamiento en anuncios CDP, de forma que los protocolos de encaminamiento dinámico no necesiten ser usados en redes simples.

CPD.- Se denomina centro de procesamiento de datos (CPD) a aquella ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización. También se conoce como centro de cómputo en Latinoamérica, o centro de cálculo en España o centro de datos por su equivalente en inglés data center.

Dichos recursos consisten esencialmente en unas dependencias debidamente acondicionadas, computadoras y redes de comunicaciones.

CPU.- Acrónimo en inglés de CENTRAL PROCESSING UNIT, Acronimo en español LA UNIDAD CENTRAL DE PROCESAMIENTO,

UNIDAD CENTRAL DE PROCESAMIENTO.- es el componente del computador y otros dispositivos programables, que interpreta las instrucciones contenidas en los programas y procesa los datos.

DATACENTER.- Un centro de datos datacenter es una instalación utilizada para los sistemas de ordenador de la casa y los componentes asociados, como las telecomunicaciones y sistemas de almacenamiento. Por lo general, incluye fuentes de alimentación redundantes y copia de seguridad, conexiones redundantes de comunicaciones de datos, los controles ambientales (por ejemplo, aire acondicionado, extinción de incendios) y dispositivos de seguridad.

DATAGRAMA.- Un datagrama es una unidad de transferencia básica asociada a una red de conmutación de paquetes en los que la entrega, la hora de llegada, y el orden no están garantizados.

DHCP.- El Dynamic Host Configuration Protocol (DHCP) es un protocolo de configuración de red para los hosts de Internet Protocol (IP). Los equipos que están conectados a redes IP debe configurarse antes de que puedan comunicarse con otros hosts.

DIAL-UP.- es una forma barata de acceso a Internet en la que el cliente utiliza un módem para llamar a través de la Red Telefónica Conmutada (RTC) al nodo del ISP, un servidor de acceso (por ejemplo PPP) y el protocolo TCP/IP para establecer un enlace módem-a-módem, que permite entonces que se enrute a Internet.

DNS.- Domain Name System o DNS (en español: sistema de nombres de dominio) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

FRAME RELAY.- Es una técnica de comunicación mediante retransmisión de tramas para redes de circuito virtual, introducida por la ITU-T a partir de la recomendación I.122 de 1988. Consiste en una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de tramas o marcos (“frames”) para datos, perfecto para la transmisión de grandes cantidades de datos.

GUEST.- “Software huésped” es un sistema operativo completo, se ejecuta como si estuviera instalado en una plataforma de hardware autónoma

HEADER.- Contiene información de direcciones de la capa de red

HYPERVISOR.- Un hipervisor (en inglés *““HYPERVISOR” ”*) o monitor de máquina virtual (*virtual machine monitor*) es una plataforma que permite aplicar diversas técnicas de control de “VIRTUALIZACIÓN” para utilizar, al mismo tiempo, diferentes sistemas operativos (sin modificar o modificados en el caso de para”VIRTUALIZACIÓN”) en una misma computadora. Es una extensión de un término anterior, “supervisor”, que se aplicaba a kernels de sistemas operativos

HYPER V.- Microsoft “HYPER-V” es un programa de “VIRTUALIZACIÓN” basado en un hipervisor para los sistemas de 64-bits[1] con los procesadores basados en AMD-V o Tecnología de “VIRTUALIZACIÓN” Intel (el instrumental de gestión también se puede instalar en sistemas x86). Una versión beta de “HYPER-V” se incluyó en el Windows Server 2008 y la versión definitiva se publicó el 26 de junio de 2008.[2]

HOST.- es un programa de control que simula un entorno computacional (máquina virtual)

HOSTNAME.- Hostname es el programa que se utiliza para mostrar o establecer el nombre actual del sistema (nombre de equipo). Muchos de los programas de trabajo en red usan este nombre para identificar a la máquina. El NIS/YP también utiliza el nombre de dominio.

Cuando se invoca sin argumentos, el programa muestra los nombres actuales. Hostname muestra el nombre del sistema que le devuelve la función gethostname(2).

La versión actual de “HYPER-V” , incluida en Windows Server 2008 R2 como rol de servidor, agregó mejoras y nuevas funcionalidades como Live Migration, almacenamiento en máquinas virtuales dinámicas, y compatibilidad mejorada con procesadores y redes

IETF.- La Internet Engineering Task Force (IETF) desarrolla y promueve estándares de Internet, en estrecha colaboración con el W3C e ISO / IEC organismos de normalización y de abordar, en particular con las normas del protocolo TCP / IP y la suite de protocolo de Internet. Se trata de una organización de estándares abiertos, sin participación formal o los requisitos de afiliación.

IKE.- Internet key exchange (IKE) es un protocolo usado para establecer una Asociación de Seguridad (SA) en el protocolo IPsec. IKE emplea un intercambio secreto de claves de tipo Diffie-Hellman para establecer el secreto

compartido de la sesión. Se suelen usar sistemas de clave pública o clave pre-compartida.

IP.- Internet protocol (IP), es el principal protocolo de comunicaciones utilizado para transmitir los datagramas (paquetes) a través de una interconexión de redes utilizando la suite de protocolo de Internet. Responsable de encaminar paquetes a través de las fronteras de la red, es el protocolo principal que establece la Internet.

IPS: Un Sistema de Prevención de Intrusos (IPS) es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de *Prevención de Intrusos* es considerada por algunos como una extensión de los Sistemas de Detección de Intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos.

IPSEC AH.- Authentication Header (AH) es un miembro de la suite de protocolos IPsec. AH garantiza la integridad sin conexión y autenticación del origen de los datos de los paquetes IP. Además, opcionalmente, puede proteger contra los ataques de repetición utilizando la técnica de ventana deslizante y el descarte de paquetes antiguos.

IPSEC ESP.- Encapsulating Security Payload (ESP) es un miembro de la suite de protocolos IPsec. En IPsec que proporciona autenticidad de origen, la integridad y protección de la confidencialidad de los paquetes. ESP también soporta configuraciones de sólo cifrado y sólo autenticación, pero utilizar cifrado sin autenticación está totalmente desaconsejado porque es inseguro.

ISAKMP.- SAKMP (Internet Security Association y Key Management Protocol) es un protocolo definido por el RFC 2408 para el establecimiento de asociaciones de seguridad (SA) y las claves de cifrado en un entorno de Internet. ISAKMP sólo proporciona un marco para la autenticación y el intercambio de claves y está diseñado para ser independiente de intercambio de claves, tales como protocolos de Internet Key Exchange y negociación de claves de Kerberos de Internet autenticado proporcionar material de claves para su uso con ISAKMP.

LAN.- Una red de área local, red local o LAN (del inglés local area network) es la interconexión de una o varias computadoras y periféricos.

L2F.- “Layer 2 Forwarding” es un protocolo de tunneling desarrollado por Cisco Systems, Inc. para establecer conexiones virtuales de la red privada a través de Internet. L2F no proporciona cifrado de confidencialidad por sí mismo, sino que se basa en el protocolo que se está túnel para proporcionar privacidad. L2F fue diseñado específicamente para hacer un túnel punto a punto (PPP),

L2TP.- Layer 2 Tunneling Protocol (L2TP) es un protocolo de túnel utilizado para apoyar las redes privadas virtuales (VPN). No proporciona ningún tipo de cifrado o la confidencialidad por sí mismo, sino que se basa en un protocolo para cifrar lo que pasa dentro del túnel para proporcionar privacidad.

NETFLOW.- NetFlow es un protocolo de red desarrollado por Cisco Systems para recopilar información de tráfico IP. NetFlow se ha convertido en un estándar industrial para la vigilancia del tráfico y con el apoyo de otras plataformas de Cisco IOS y NXOS tales como routers Juniper, conmutadores Enterasys, vNetworking en la versión 5 de vSphere, Linux, FreeBSD, NetBSD y OpenBSD

MAC.- A Media Access Control address (MAC address) es un identificador único asignado a las interfaces de red para las comunicaciones en el segmento de red física. Las direcciones MAC se utilizan para las tecnologías de red de numerosas y la mayoría de las tecnologías de red IEEE 802 Ethernet incluidos. Lógicamente, las direcciones MAC se utilizan en la dirección Media Access Control sub-protocolo de capa del modelo de referencia OSI.

MÁQUINA VIRTUAL.- En informática una máquina virtual es un software que emula a una computadora y puede ejecutar programas como si fuese una computadora real. Este software en un principio fue definido como "un duplicado eficiente y aislado de una máquina física". La acepción del término

actualmente incluye a máquinas virtuales que no tienen ninguna equivalencia directa con ningún hardware real.

PARAVIRTUALIZACION.- Es una técnica de programación informática que permite virtualizar por software a sistemas operativos.

PDU.- Las unidades de datos de protocolo, también llamadas PDU (en inglés protocol data unit), se utilizan para el intercambio entre unidades parejas, dentro de una capa del modelo OSI.

PAP.- Protocolo de encapsulamiento Point to Point. PAP es un proceso muy básico de dos vías, no hay cifrado: el nombre de usuario y la contraseña se envían en texto sin cifrar, si esto se acepta, la conexión se permite.

PAYLOAD.- A veces conocido como los datos reales o el cuerpo, es la carga de una transmisión de datos. Es la parte de los datos transmitidos.

PPP.- the Point-to-Point Protocol (PPP) es un protocolo de enlace de datos comúnmente utilizados para establecer una conexión directa entre dos nodos de red. Puede proporcionar autenticación de la conexión, el cifrado de la transmisión y la compresión

PPTP.- The Point-to-Point Tunneling Protocol (PPTP) es un método para implementar redes privadas virtuales. PPTP utiliza un canal de control a través de TCP y un túnel GRE de funcionamiento para encapsular los paquetes PPP.

RADIUS.- Acrónimo en inglés de Remote Authentication Dial-In User Server. Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

RAM.- La memoria de acceso aleatorio (en inglés: random-access memory, cuyo acrónimo es RAM) es la memoria desde donde el procesador recibe las instrucciones y guarda los resultados.

RFC.- Acrónimo de Request For Comments. son una serie de notas sobre Internet, y sobre sistemas que se conectan a internet, que comenzaron a publicarse en 1969

RDP.- Remote Desktop Protocol (RDP) es un protocolo propietario desarrollado por Microsoft que permite la comunicación en la ejecución de una aplicación

SAN.- Una red de área de almacenamiento, en inglés SAN (storage area network), es una red concebida para conectar servidores, matrices (arrays) de

discos y librerías de soporte. Principalmente, está basada en tecnología fibre channel y más recientemente en iSCSI. Su función es la de conectar de manera rápida, segura y fiable los distintos elementos que la conforman.

SNIFFER.- Un sniffer es un programa informático que registra la información que envían los periféricos, así como la actividad realizada en un determinado ordenador.

SNMP.- Simple Network Management Protocol (SNMP) es un "estándar de Internet, el protocolo para la gestión de dispositivos en redes IP. Dispositivos que soportan SNMP incluye routers, switches, servidores, estaciones de trabajo, impresoras, módem de bastidores, y mucho más.

SSH.- (Secure SHell, en español: intérprete de órdenes segura) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

SSL.- Acrónimo en ingles de SECURE SOCKETS LAYER.

SECURE SOCKETS LAYER.- El protocolo SSL es un sistema diseñado y propuesto por Netscape Communications Corporation. Se encuentra en la pila OSI entre los niveles de TCP/IP y de los protocolos HTTP, FTP, SMTP, etc.

Proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico

SQL.- El lenguaje de consulta estructurado o SQL (por sus siglas en inglés *structured query language*) es un lenguaje declarativo de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en estas. Una de sus características es el manejo del álgebra y el cálculo relacional permitiendo efectuar consultas con el fin de recuperar -de una forma sencilla- información de interés de una base de datos, así como también hacer cambios sobre ella.

TCP.- TCP (Transmission Control Protocol) es un conjunto de reglas (protocolo) que se utiliza junto con el Protocolo Internet (IP) para enviar datos en forma de unidades de mensajes entre ordenadores a través de Internet. Mientras que IP se encarga del manejo de la entrega real de los datos, TCP se encarga de hacer el seguimiento de las distintas unidades de datos (llamados paquetes) que se divide un mensaje para el enrutamiento eficiente a través de Internet.

TOPOLOGIA DE RED.- La topología de red se define como la cadena de comunicación usada por los nodos que conforman una red para comunicarse.

TUNNEL IP.- Un túnel de IP es un protocolo de Internet (IP) del canal de comunicaciones entre dos redes. Se utiliza para el transporte de otro protocolo de red mediante la encapsulación de los paquetes.

UDP.- UDP (User Datagram Protocol) es un protocolo de comunicaciones que ofrece una cantidad limitada de servicio cuando se intercambian mensajes entre ordenadores en una red que utiliza el Protocolo Internet (IP). UDP es una alternativa al Transmission Control Protocol (TCP) y, junto con la IP, a veces es referido como UDP / IP

VIRTUALIZACIÓN.- es la creación -a través de software- de una versión virtual de algún recurso tecnológico, como puede ser una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento u otros recursos de red

VPN o RED PRIVADA VIRTUAL.- Acrónimo en inglés de Virtual Private Network, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

VM.- Siglas de “Máquina Virtual” o en ingles “Virtual Machine”

VMM.- Siglas de Virtual Machine Manager.

VIRTUAL MACHINE MANAGER.- Permite a sus clientes centralizar la gestión de Data Center virtualizados.

WAN.- Una red de área amplia, con frecuencia denominada WAN, acrónimo de la expresión en idioma inglés *wide area network*, es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km, proveyendo de servicio a un país o un continente. Un ejemplo de este tipo de redes sería RedIRIS, Internet o cualquier red en la cual no estén en un mismo edificio todos sus miembros (sobre la distancia hay discusión posible).

WEBSITE.- Un sitio web es una colección de páginas web relacionadas y comunes a un dominio de Internet o subdominio en la World Wide Web en Internet.

WEP.- (Wired Equivalent Privacy, Privacidad Equivalente al Cable) es el algoritmo opcional de seguridad para brindar protección a las redes inalámbricas, incluido en la primera versión del estándar IEEE 802.11, mantenido sin cambios en las nuevas 802,11a y 802.11b, con el fin de garantizar compatibilidad entre distintos fabricantes

WIFI.- es un mecanismo de forma inalámbrica la conexión de dispositivos electrónicos

WPA.- Es la abreviatura de Wifi Protect Access, y consiste en un mecanismo de control de acceso a una red inalámbrica, pensado con la idea de eliminar las debilidades de WEP. También se le conoce con el nombre de TSN (Transition Security Network).

X.25.- Es un estándar ITU-T para redes de área amplia de conmutación de paquetes. Su protocolo de enlace, LAPB, está basado en el protocolo HDLC (publicado por ISO, y el cual a su vez es una evolución del protocolo SDLC de IBM)

ANEXO A

ROUTER CISCO 1800.

Cisco 1800 Series (Fixed-Configuration)

Cisco is redefining best-in-class enterprise and small- to medium-sized business routing with a new line of Integrated Services Routers that are optimized for the secure delivery of data services. Founded on 20 years of leadership and innovation, the Cisco 1800 Series Integrated Services Routers intelligently embed data, security, and wireless technology into a single, resilient system for fast, secure, scalable delivery of mission-critical business applications. The Cisco 1800 Series architecture has been specifically designed to meet requirements of small- to medium-sized businesses (SMBs), small enterprise branch offices, and service provider-managed services applications for delivery of concurrent services for broadband access. The integrated secure systems architecture of the Cisco 1800 Series delivers maximum business agility and investment protection.

Benefits and Advantages

Cisco 1800 Series Integrated Services Routers are the next evolution of the award-winning Cisco 1700 Series modular and fixed-configuration routers. The Cisco 1801, 1802, 1803, 1811, and 1812 Integrated Services Routers are fixed-configuration, while the Cisco 1841 Integrated Services Router is modular. The routers are designed for secure broadband, Metro Ethernet, and wireless connectivity, and provide significant performance improvements, feature capability, versatility, and additional value compared to prior generations of Cisco 1700 Series. The Cisco 1800 Series fixed-configuration routers provide:

- Secure broadband access with concurrent services for branch and small offices
- Integrated ISDN Basic Rate S/T interface (BRI), analog modem, or Ethernet backup port for redundant WAN links and load balancing
- Secure wireless LAN option for simultaneous 802.11a and 802.11b/g with use of two dual-mode antennas
- Advanced security including: Stateful Inspection Firewall, IP Security (IPsec) VPNs (Triple Data Encryption Standard [3DES] or Advanced Encryption Standard [AES]), Intrusion Prevention System (IPS), Antivirus support through Network Admission Control (NAC) and enforcement of secure access policies
- 8-port 10/100 managed switch with 802.1q VLAN support and optional Power over Ethernet (PoE)
- Easy deployment and remote-management capabilities through Web-based tools and Cisco IOS Software

Cisco 1801, 1802, and 1803 routers provide high-speed DSL broadband access through asymmetric DSL (ADSL) over basic telephone service (Cisco 1801), ADSL over ISDN (Cisco 1802), or Symmetrical High-Data-Rate DSL (G.SHDSL) (Cisco 1803) while helping to ensure reliable networking with integrated ISDN S/T BRI backup. The Cisco 1811 and 1812 provide high-speed broadband or Ethernet access through two 10/100BASE-T Fast Ethernet WAN ports and also provide integrated WAN backup through a V.92 analog modem (Cisco 1811) or ISDN S/T BRI interface (Cisco 1812).

Benefits and Advantages continued

The Cisco 1800 Series fixed-configuration routers help enable a network infrastructure for SMBs and enterprise small branch offices, providing access to the Internet, corporate headquarters, or other remote offices, while securing and protecting critical data with integrated Cisco IOS Software security features and capabilities. They also help businesses reduce costs by enabling deployment of a single device to provide multiple services (integrated router with redundant link, LAN switch, firewall, VPN, IPS, wireless technology, and Quality of Service [QoS]) typically performed by separate devices. Cisco IOS Software allows this flexibility, providing the industry's most robust, scalable, and feature-rich internetworking support, using the accepted standard networking software for the Internet and private WANs.

Security Features

Cisco IOS Firewall

- Stateful firewall with URL filtering
- Per-user authentication and authorization
- Real-time alerts
- Transparent firewall
- IPv6 firewall

VPN

- Advanced Encryption Standard (AES) 128, 192, and 256
- Triple Data Encryption Standard (3DES), and DES encryption
- Embedded hardware-based VPN acceleration on the motherboard
- Cisco Easy VPN remote and server support
- Dynamic Multipoint VPN (DMVPN)
- Group Encrypted Transport VPN (GET VPN)

Onboard USB Port

- USB 2.0 ports (2) (Cisco 1811 and 1812 models only)

IPS

- More than 700 IPS signatures supported in Cisco IOS Software, with the ability to load and enable selected IPS signatures

URL Filtering

- Local URL filtering in Cisco IOS Software based on external server (Websense and N2H2)
- Stateful firewall contains URL filtering

Cisco SDM

- Cisco Router and Security Device Manager (SDM)

IOS WebVPN (SSL VPN)

- Secure remote access for mobile users without installing PC client software
- Integrated into the router—no separate appliance required
- Cisco 1801 and 1812 supports up to 10 users
- Requires IOS WebVPN feature license FL-WEBVPN-10
- Requires an IOS security feature set (IOS security feature set is included in all secure router bundles)

Cisco 1800 Series (Fixed-configuration)

Small Offices and Small Enterprise Branch Offices

- Secure, concurrent services for broadband access with WAN high availability
- Manageability and reliability of Cisco IOS Software Business-class Security
- Stateful firewall with URL filtering
- VPN 3DES encryption and Advanced Encryption Standard (AES) encryption
- Dynamic Multipoint VPN (DMVPN)
- Intrusion Prevention System (IPS) Fixed Configuration
- Secure broadband access at broadband performance
- Integrated ISDN Basic Rate S/T Interface (BRI), analog modem, or Ethernet backup port for redundant WAN links and load balancing
- Secure wireless LAN option for simultaneous 802.11a and 802.11b/g with use of multiple antennas
- 8-port 10/100 managed switch with 802.1q VLAN support and optional Power over Ethernet (PoE)

Cisco 1800 Series (Modular)

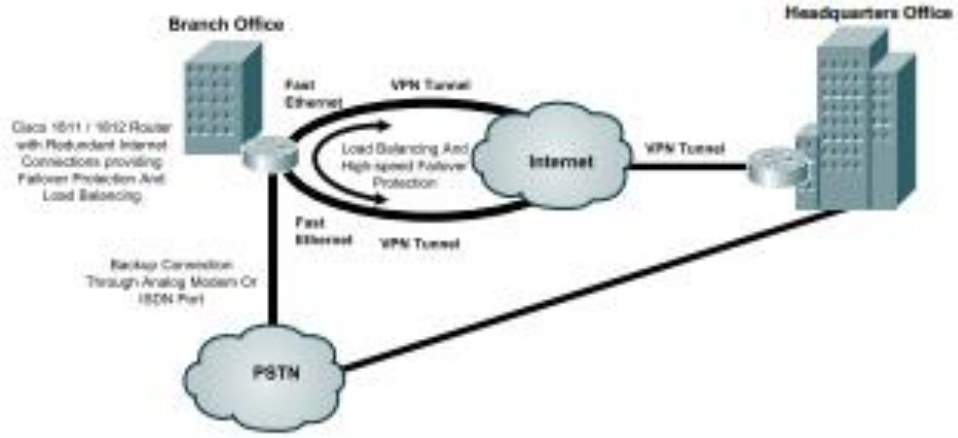
Small- to Medium-sized Businesses and Small Enterprise Branch Offices

- Wire-speed performance with secure data services enabled at up to T1/E1/xDSL rates
- Increased services density for secure data services
- Support for next-generation High-speed WAN Interface Cards
- Increased flexibility through support of internal AIM slot for high-speed VPN and future applications
- Built-in dual Fast Ethernet ports
- Support for over 30 existing and new modules Secure Networking
- Hardware-based VPN acceleration on motherboard
- Antivirus defense
- Intrusion Prevention System (IPS) Support

Cisco Fixed FE WAN 1800

	Cisco 1811, 1812
Form Factor	Desktop
Rack/Wall Mountable	Yes
DRAM (default)	128 MB
DRAM (maximum)	384 MB
Flash (default)	32 MB
Flash (maximum)	128 MB
Integrated LAN Switch	8-port Switch
Fast Ethernet WAN	2 Ports
Gigabit Ethernet WAN	No
Back-up WAN	v.92 Modem (1811)/ ISDN S/T BRI (1812
Wireless Option	Integrated 802.11a/b/g
USB Ports (v 2.0)	2 Ports
Integrated Power over Ethernet Support	Optional
Real Time Clock	Yes

High-Availability Features Example



Platform Overview

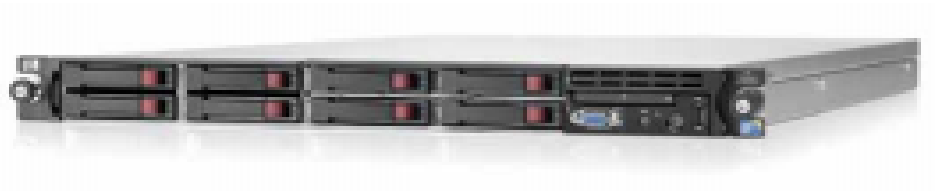
Models	FE WAN Ports	Switch Ports	WAN	Wireless Option	DRAM (MB) Default	DRAM (MB) Max	Compact Flash (MB) Default	Compact Flash (MB) Max	Power Supply
Cisco 1801	1	8	ADSL	Yes	256	384	64	128	AC
Cisco 1802	1	8	ADSLoISDN	Yes	256	384	64	128	AC
Cisco 1803	1	8	G.SHDSL	Yes	256	384	64	128	AC
Cisco 1805	2	4	DOCSIS 2.0	Yes	256	384	64	128	AC
Cisco 1811	2	8	10/100 Ethernet	Yes	256	384	64	128	AC
Cisco 1812	2	8	10/100 Ethernet	Yes	256	384	64	128	AC

Series Specifications

Dimensions (H x W x D)	12.5 x 9.5 in. (34.3 x 27.4 cm)
Console Port	1 (up to 115.2 Kbps)
Auxiliary Port	1 (up to 115.2 Kbps)
USB Port	2 (USB 2.0) on Cisco 1811 and 1812 only. The Cisco 1801, 1802, and 1803 do not offer USB support
Wireless LAN	IEEE 802.11a,b,g (W models)
V.92 Analog Modem Port	One analog modem port on Cisco 1805 and 1811
Integrated Channel Service Unit/Data Service Unit (CSU/DSU)	No, see Cisco 1841
Voice/Data Support	Only data support
Encryption	Hardware support on motherboard (3DES and AES)
10/100 Switch Ports	8 10/100BASE-T fully managed switch ports with 802.3af PoE support 4 10/100BASE-T fully managed switch ports with 802.3af PoE support (Cisco 1805 Model only)
Integrated Modems	1 (Cisco 1805 and 1811 models only) V92
Default 10/100 WAN Ports	1 (Cisco 1801, 1802, 1803, and 1812 models), 2 (Cisco 1805, 1811 and 1812 models)
ISDN Basic Rate Interface (BRI) Ports S/T	1 (Cisco 1801, 1802, 1803, and 1812 models only)

ANEXO B

SERVIDOR HP PROLIANT DL360 G7 E5606.



HP ProLiant DL360 G7 Server

Data sheet

Get superior performance in a compact footprint

If space is a premium consideration, quality is a priority and consolidation is the need, then look no further – the HP ProLiant DL360 G7 Server is designed to work well in limited spaces and delivers superior performance with improved consolidation over earlier servers.

Combining concentrated 1U compute power, HP Insight Control management software, HP Data Center Smart Grid technology and essential fault tolerance, the HP ProLiant DL360 G7 Server is designed for space-constrained installations. With the latest Intel® Xeon® 5600 series processors, DDR3 Registered or unbuffered DIMMs, Serial Attached SCSI (SAS), PCI Express Gen 2 technology and four 1 Gb network interface connections, the ProLiant DL360 G7 is a high-performance server – ideal for the full range of scale-out applications.

Do more with less

- Up to two Intel Xeon 5600 or 5500 series processors with Turbo Boost technology automatically regulate power consumption and intelligently adjust server performance, resulting in higher efficiency and superior performance. The ProLiant DL360 G7 Server comes with the latest Intel QuickPath Interconnect (QPI) architecture with an option for six-core, quad-core, or dual-core processors.
- HP Integrated Lights-Out 3 (iLO 3), part of Insight Control, delivers remote control performance almost 800 per cent[1] faster than iLO 2. Also, with 360 per cent[1] faster Virtual Media capability, everyday maintenance and deployment can be done faster than previous versions. It sends alerts from iLO 3 regardless of the state of the host server, and helps users access advanced troubleshooting features. Now users can manage their data centre remotely – significantly reducing the expense for onsite personnel and travel time to the server site. For more information about iLO 3 for ProLiant servers, visit: www.hp.com/go/iLO
- Four NIC ports help sustain unmatched network availability and reliability.

Key features and benefits

- **Enhanced server performance for space-constrained environments**
  - Latest six-core and quad-core Intel Xeon 5600 or 5500 series processors automatically regulate power consumption and intelligently adjust server performance according to application needs. These processors make the ProLiant DL360 G7 Server ideal for demanding scale-out applications and virtualisation.
  - Up to 384 GB of DDR3 memory (speeds vary between 800 MHz, 1066 MHz and 1333 MHz, depending on DIMM population and processors installed) with enhanced memory capacity meets the requirements of memory-intensive applications.
  - Concentrated 1U compute power is ideal for space-conscious customers.
- **Improved server lifecycle management**
  - HP Insight Control is essential server management software that helps deploy servers quickly, proactively manage the health of virtual or physical servers, streamline power consumption and access remote control from anywhere.

[1] HP Performance Engineering Team, 2010 benchmark

– iLO 3, part of Insight Control, is a standard component of the HP ProLiant DL360 G7 Server, facilitating server health and remote server manageability. As it includes an intelligent microprocessor, secure memory and a dedicated network interface, iLO 3 is independent of the host server and its operating system.

– Together, HP SmartStart, HP Insight Control, Preboot Execution Environment (PXE) and ROM-Based Setup Utility (RBSU) simplify server configuration and deployment.

– Insight Control helps manage HP servers running Microsoft® Windows®, Linux, VMware and Citrix XenServer environments. In addition, users can integrate Insight Control with leading third-party enterprise management consoles, such as Microsoft System Center and VMware vCenter Server.

– Systems Insight Display is a robust slide-out system diagnostics display that makes it easy to find troubleshooting information at the front of the server, helping to save administrator time.

Watch the demo of HP ProLiant DL360 G7 Server by the HP product marketing manager

- **HP Data Center Smart Grid technology – driving new levels of energy efficiency**

– The **HP Sea of Sensors** technology enhances server performance while reducing energy usage and expense. Achieve significant reduction in power usage at the server level with the HP Sea of Sensors, the heart of the HP Data Center Smart Grid technologies. Up to 32 smart sensors automatically track thermal activity across the server, dynamically adjusting system components such as fans, memory and I/O processing to enhance system cooling. In other words, the HP Sea of Sensors makes intelligent decisions about how much cooling is needed for the server to perform efficiently.

– **Dynamic Power Capping** can lock and reduce power consumption and improve capacity of your ProLiant servers. Insight Control and Dynamic Power Capping together allow users to monitor and cap power usage levels and protect circuit breakers in the rack – without impacting performance.

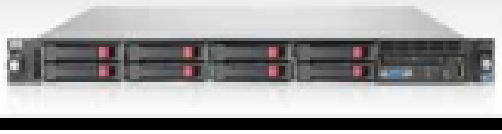
– **HP Common Slot Power Supply** is an HP universal power bay design that provides users with a common power supply across multiple platforms – saving on the cost of spares and offering power solutions that match users' needs. Common Slot designates a common power supply across multiple servers. Many HP ProLiant servers come with Common Slot, which means high-efficiency and right-sized power supplies. The new Common Slot power supplies are designed to provide power efficiency without compromising on performance. These power supplies can have efficiency ratings up to 94 per cent.[2] You can choose from multiple right-sized power options available, depending on the configuration of your server.

To check for power supply options supported in the DL360 QuickSpecs, visit: **http://h18004.www1.hp.com/products/quickspecs/13598_div/13598_div.html**

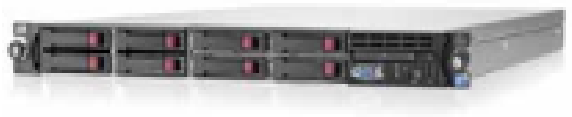
HP Common Slot Power Supplies meet compliance standards with Climate Savers Computing Gold, 80PLUS Gold/Platinum and ENERGY STAR® power supply ratings. You have an option of choosing from the 460 W, 750 W, 1200 W and -48 Vdc (for special DC environments) power supplies to more closely match the actual power your server is using. To help you select the right power supply option that suits your configuration, we recommend the HP Power Advisor.

To learn more about the HP Power Advisor, visit: **www.hp.com/go/proliant-energy-efficient** or **www.hp.com/go/hppoweradvisor**

Click here to review the specifications of the HP ProLiant DL360 G7 Server



HP ProLiant DL360 G7 Server



Processor and memory	
Number of processors	Up to 2
Processor cores	Six-core, quad-core and dual-core
Processors supported	Intel Xeon 5600 and 5500 series
Cache	12 GB L3 4 GB L3 (on some models)
Memory type	DDR3 RDIMM or UDIMM
Standard memory	DDR3
Maximum memory	Up to 384 GB (speeds vary between 800 MHz, 1066 MHz and 1333 MHz, depending on DIMM population and processors installed)
Advanced memory protection	Advanced error checking and correcting (ECC), mirrored memory; online spare (5600 series only)
Memory slots	18 DIMM
Storage	
Storage type	Hot-plug SFF SAS Hot-plug SFF SATA Hot-plug SFF SDD
Maximum internal storage	Up to 4.8 TB
Maximum internal drive bays	8
Expansion slots	2 PCIe Gen 2 Card slots
Storage controller	Smart Array P410i Controller with optional upgrades to 256 MB, 512 MB battery-backed write cache (BBWC), 512 MB flash-backed write cache (FBWC) and 1 GB FBWC options
Deployment	
Form factor	Rack
Rack height	1U
Networking	2 HP NC382i Dual Port Multi-function Gigabit Server Adapters – 4 x 1 Gb NIC ports
Server management	iLO 3, HP Insight Control featuring Integrated Lights-Out Advanced
Redundant power supply	Fans: N+1 non-hot plug Power supplies: N+1 hot plug
Power supplies	460 W, 750 W (92% or 94% Eff); -48 Vdc power options
Security	TPM
Warranty	3-year parts/3-year labour/3-year onsite

BIBLIOGRAFIA

BIBLIOGRAFIA

[1] Larson Robert, Windows Server® 2008 “HYPER-V” (TM) Resource Kit, Janique Carbone and Microsoft Windows Virtualization Team, Jun 10 2009.

[2] Ruest Nelson, Configuring Windows Server® Virtualization, MCTS Self-Paced Training Kit (Exam 70-652), Jun 17 2009

[3] Kelbley John, Sterling Mike and Stewart Allen, Windows Server 2008 “HYPER-V” : Insiders Guide to Microsoft's ““HYPERVISOR”, Serious Skills, Apr 20 2009.

[4] Wade Edwards, Tom Lancaster, Eric Quinn and Jason Rohm, CCSP: Secure PIX and Secure VPN Study Guide (642-521 and 642-511), SYBEX Inc., Nov 03 2003.

[5] Hucaby Dave, Cisco ASA, PIX, and FWSM Firewall Handbook (2nd Edition), Cisco system Inc., Aug 19 2007.

[6] Deal Richard A., CCNA Cisco Certified Network Associate Security Study Guide with CDROM (Exam 640-553), Mc Graw Hill, Jul 17 2009

[7] Lucas Michael, Network Flow Analysis, Ansel Staton, Jul 05 2010

[8] Cisco System, Cisco CNS NetFlow Collection Engine Installation and User Guide , Cisco Systems, Inc., 1999

[9] Fundación Wikimedia, Cisco VPN Conceptos http://es.wikipedia.org/wiki/Red_privada_virtual, Nov 2011

[10] Cisco System, Cisco VPN Configuracion, http://www.cisco.com/en/US/products/sw/secursw/ps2308/index.html, Nov 2011

[11] Microsoft, Virtualizacion, http://www.microsoft.com/spain/windowsserver2008/virtualization/hyperv_install.mspx, Nov 2011

[12] IPSEC HOW TO, IPSEC, http://www.ipsec-howto.org/spanish/x161.html, Nov 2011.

[13]Netflow Analizer, Netflow, www.manageengine.com/products/netflow/spanish/index.html, Nov 2011