

CAPÍTULO III

3. PROPUESTA DE DISEÑO DE LA HONEYNET VIRTUAL.

3.1 Generalidades de la propuesta.

En este capítulo se plantea el problema ante una carencia de herramienta de seguridad que permita mantener protegidos los sistemas de información de la Universidad Francisco Gavidia y que hacen necesaria la propuesta de diseño de Honeynets Virtuales utilizando Vmware.

Se plantea el estudio de factibilidad tanto técnica como económica de la propuesta, una propuesta genérica que define los componentes informáticos que integran el esquema de red con las características necesarias para poder garantizar la seguridad del sistema informático y disponer de una herramienta para monitorear y controlar el tráfico y analizarlo, permitiendo proteger aquella información en producción .

Posteriormente de describir los componentes que integran un diseño genérico de honeynets virtual y los requerimientos para su apropiada implementación se procede a presentar un diseño orientado para ser aplicado a la necesidad de la Universidad Francisco Gavidia, en la cual se plasma las herramientas, equipo de cómputo y software que serán utilizadas para desarrollar el prototipo de diseño para su posterior implementación por la Dirección de Tecnología y Comunicaciones.

3.1.1 Objetivos de la propuesta del diseño de la honeynet.

General

Proporcionar un diseño de configuración de red que incluya la Honeynet, que permita conocer, controlar y analizar el tráfico de datos y tomar medidas que contribuyan a la mejora de la seguridad informática de la Universidad, protegiendo los servicios en producción que se están brindando.

Específicos

- a. Elaborar una propuesta diseño de red que incluya la Honeynet.
- b. Brindar herramientas técnicas que permitan proteger la red de ataques informáticos externos e internos.
- c. Lograr que la Universidad Francisco Gavidia cuente con un diseño de seguridad para proteger y fortalecer los sistemas contra intrusos informáticos mediante redes falsas simuladas.

3.1.2 Justificación de la propuesta del diseño de la honeynet.

Debido a que es imprescindible el contar con el diseño de una herramienta de solución de seguridad el cual impida el acceso de usuarios no deseados y fortalezca de la red interna para así proteger la información y datos importantes que se transmiten a través de toda la infraestructura de la red de información de la Universidad Francisco Gavidia.

Con el presente diseño, la Universidad Francisco Gavidia podrá realizar un mejor aseguramiento de los servidores de la red universitaria, siendo la herramienta de los honeynets punto de distracción de los sistemas reales ante cualquier ataque o atacante, salvaguardando la información.

Con el diseño de la herramienta implementado se podrá contar con elementos para el análisis de situaciones anómalas o ataques, teniendo la información necesaria para poder evitar y realizar correcciones o un mejor aseguramiento en los componentes externos para cerrar las posibles entradas que pudiese tener un atacante.

De la misma forma se podrá contar con elementos para estudiar cual es el comportamiento de los ataques, elementos que actualmente la Universidad Francisco Gavidia no posee.

Situación actual.

La universidad Francisco Gavidia cuenta infraestructura de red renovada en Junio de 2007, lo cual le permite de gozar de un muy buen medio para el transporte de la información a lo largo del campus universitario. La distribución de forma esquemática puede ser observada en la figura 4.

Tradicionalmente el uso de estos sistemas y elementos (cortafuegos) son utilizados como sistema de seguridad puramente defensivos y reactivos debido a que estos toman un tipo de acción ya sea de inspección o de clausura de intercambio de información al tener un tipo ataque contra él o la red que protege.

Debido a esto, es que el uso de herramientas adicionales que conjuntamente interactúen y realicen actividades proactivas de seguridad son mandatorios, dando la facultad de ser los manejadores de intrusos y sus ataques, resguardando de una mejor manera la información en los periodos de incidentes y no bajo un esquema de presentarse a merced del atacante que es lo que se logra con esquema defensivos como el que actualmente se utiliza en la universidad.

Entre estos elementos se pueden mencionar a los IPS (sistemas de protección/prevención ante intrusos) los cuales pueden ser adquiridos en una gran gama de fabricantes como tipping point, cisco y mcafee.

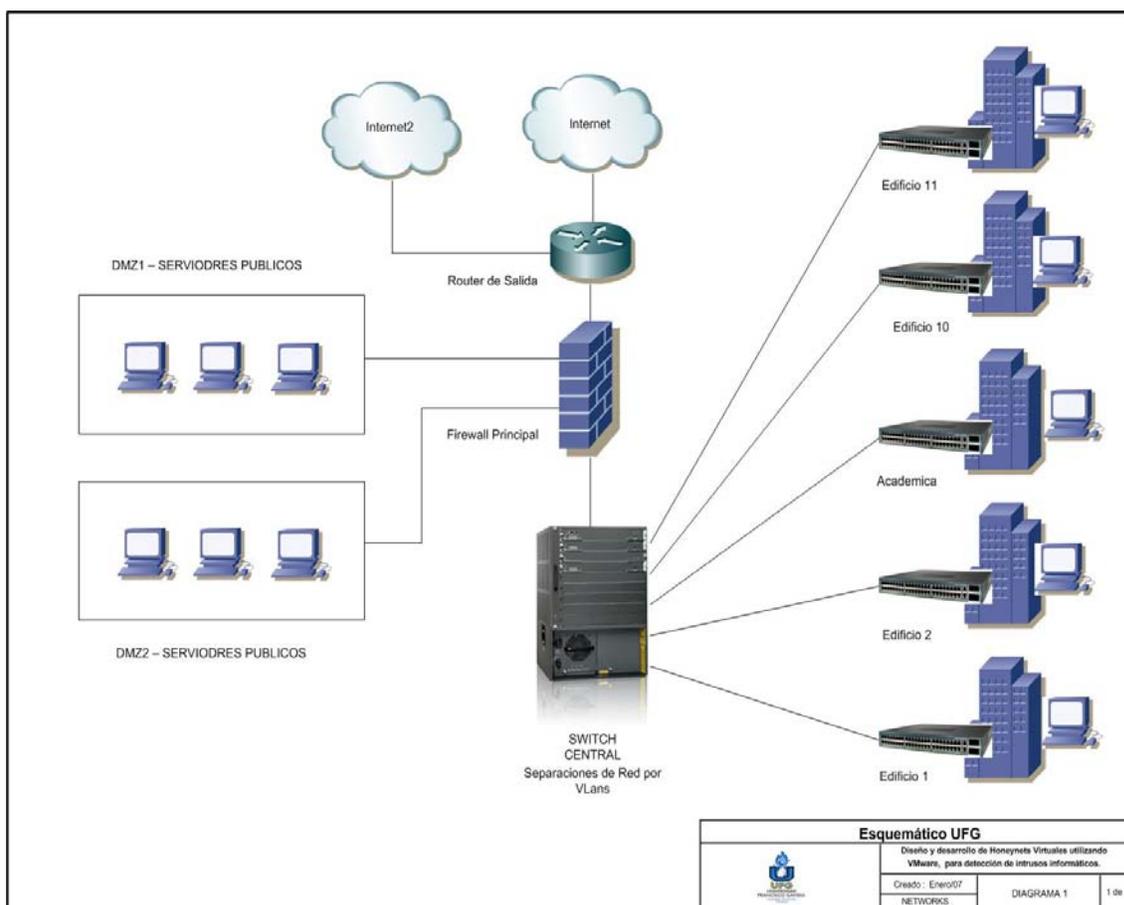


Figura 5: Diagrama esquemático de la Universidad Francisco Gavidia realizada a través de información recolectada.

Con respecto a elementos que resguardan la seguridad de la información en la red se encuentra un cortafuego perimetral, elemento que funge con su desempeño como única solución de protección en toda la red.

Una solución viable para resguardar la integridad de la infraestructura de la red de datos es la herramienta denominada Honeynets, la cual recoge información sobre los atacantes y permite tomar medidas de protección para los sistemas importantes a un bajo costo, resultando ser una herramienta ideal para ser desarrollada e implementada

Debido a lo anterior, entre las razones que justifican el desarrollo del presente trabajo de investigación son:

- a. La Universidad Francisco Gavidia carece de sistemas o herramientas proactivas que formen en conjunto al cortafuegos un sistema de seguridad
- b. La Universidad Francisco Gavidia solo posee un único elemento de seguridad en toda la red
- c. La Universidad Francisco Gavidia no dispone de una herramienta denominada Honeynet como sistema de seguridad informática a bajo costo.
- d. En base a este sistema se permitirá al personal de la Dirección de Tecnología y Comunicaciones mantener resguardada la información teniendo un sistema actualizado en la seguridad de la red del campus contra ataques de constantes técnicas novedosas por los intrusos informáticos.

- e. Fortalecer la seguridad existente y complementarla con una herramienta que se presenta como un sistema vulnerable que desviará la atención de los atacantes de los sistemas o servicios en producción protegiéndolos de accesos no autorizados.

3.2 Importancia y beneficios de la propuesta del diseño de la honeynet.

Es necesario que en la actualidad se disponga de un sistema de seguridad cuando se brinda servicios para el acceso público, la mayoría de las veces por simple desconocimiento se empieza a preocupar solo cuando ocurre algún problema, algunas veces con muy poco remedio.

Muchos sistemas están expuestos a "agujeros" de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje.

Estas vulnerabilidades ocurren por variadas razones, y miles de "puertas invisibles" han sido descubiertas en aplicaciones de software, sistemas operativos, protocolos de red, browsers de Internet, correo electrónico y toda clase de servicios en LAN o WANs.

Por tal razón es muy importante la propuesta puesto que los sistemas Honeynet presentan un enfoque innovador con respecto a los sistemas de seguridad tradicionales. En vez de repeler las acciones de los atacantes, utilizan técnicas para monitorizarlas y registrarlas

Estos sistemas trampa están diseñados para imitar el comportamiento de aquellos sistemas que puedan ser de interés para un intruso.

Suelen contar con mecanismos de protección para que un atacante con éxito no pueda acceder a la totalidad de la red, naturalmente, si un intruso consigue entrar en un sistema trampa, no debe percatarse de que está siendo monitorizado o engañado.

La propuesta beneficiara directamente a la Universidad Francisco Gavidia y en caso puntual a la Dirección de Tecnología y comunicaciones que es la entidad designada para garantizar y velar por un óptimo funcionamiento de las estructuras de cómputo, telecomunicaciones y servicios en línea, las cuales deben protegerse valiéndose del diseño de los sistemas trampa denominado Honeynets.

3.3 Alcance de la propuesta del diseño de la honeynet.

La propuesta que incluye el diseño de Honeynet Virtual con Vmware, para detección de intrusos informáticos permitirá:

- a. Proteger la red de ataques externos e internos.
- b. Monitorizar accesos a la red no autorizados o posibles ataques, así como registrarlos y activar las alarmas correspondientes.
- c. Engañar a posibles atacantes mediante redes falsas simuladas y registrar esos eventos.

3.4 Planteamiento del problema.

Como todo estudio que se realiza, es para darle solución a un problema existente, por lo tanto se presenta a continuación el planteamiento del problema por el método de la caja negra.

3.4.1 Método de la caja negra.

Estado Actual

1. La Universidad Francisco Gavidia, no cuenta con un sistema de seguridad que este orientado al desarrollo de Honeynets virtuales que permita la captura y control de los datos.
2. No existe un monitoreo constante de la información contra ataques constantes y técnicas novedosas por los intrusos informáticos.

PROCESO

Estado Futuro

1. Con el diseño de la propuesta de Honeynets virtuales utilizando Vmware, para detección de intrusos informáticos orientada y acorde a la Universidad Francisco Gavidia se pretende satisfacer las necesidades de mejorar la seguridad de la información.

3.5 Estudio de factibilidad.

Los estudios de factibilidad establecen si el proyecto es posible realizarse, a fin de que se cuente con los recursos y capacidades para cumplir con los objetivos y necesidades, con el propósito de considerar que es apropiado, aceptable e importante para desarrollarse.

3.5.1 Factibilidad técnica.

Desde el punto de vista técnico, es realizable, ya que se dispone en el mercado el equipo necesario para dar soporte al diseño que se va a desarrollar, que es el desarrollo de la propuesta de Honeynet virtuales utilizando Vmware, para la detección de intrusos informáticos orientada a la Universidad Francisco Gavidia, también se cuenta con el software y el recurso humano.

Con respecto al requerimiento necesario y mínimo de todas las computadoras serán los siguientes:

- Procesador Pentium IV.
- Velocidad 2 GHz.
- RAM de 1 GB.
- Disco Duro de 40 GB.
- Tarjetas de Red.

Se requerirán un total de 6 computadoras para una propuesta total y genérica, las cuales desempeñarán las siguientes características de funcionalidad.

Computadora 1. Cortafuegos.

Computadora 2. Honeynet Virtual.

Computadora 3. Proxy NAT.

Computadora 4. IDS.

Computadora 5. Servidor de Aplicaciones y Base de Datos.

Computadora 6. Monitoreo.

Recurso de red	Recurso de red
1 Switch para segmentación capa 3.	Administrable de 24 puertos Gigabit.
1 Switch para conectividad capa 2.	Administrable de 8 puertos Gigabit.

Tabla 1. Requerimientos de red.

Equipo	Software requerido
Cortafuegos	Linux RedHat versión 9
HoneyNet Virtual	Linux RedHat versión 9 VMware GSX Server
Proxy NAT	Linux RedHat versión 9
IDS	Linux RedHat versión 9
Servidor de Aplicaciones y Base de Datos	Linux Suse versión 10

Tabla 2. Requerimientos de software.

3.5.2 Factibilidad económica.

El costo que genera el diseño de la propuesta en cuanto a la tecnología que se empleará para el desarrollo y funcionalidad del mismo es económicamente factible, a continuación se detalla los costos del equipo.

Cantidad	Hardware	Costo
4	Computadoras	US\$3,600.00
Cantidad	Capacitación al personal	Costo
1	Capacitación para el uso del sistema de seguridad.	US\$2,500.00
Cantidad	Mantenimiento del sistema	Costo
1	Administrador de Seguridad	US\$2,000.00
Cantidad	Otros gastos	Costo
-	Mantenimiento a la Infraestructura de la Red	US\$4,000.00
-	Conexión a Internet 2 Mbps	US\$2,500.00
-	Energía eléctrica	US\$2,000.00
	Total en dólares	US\$16,600.00

Tabla 3. Presupuesto general para el desarrollo de honeynets.

3.6 Determinación de requerimientos.

3.6.1 Requerimientos funcionales.

Estos requerimientos definen el tipo de servicio esperado de la propuesta. Los requerimientos funcionales cubren las funciones y operaciones a realizar para que la propuesta genere los resultados de acuerdo a las necesidades de proteger la información de la Universidad.

- a. El administrador de la seguridad de la información será responsable de dar soporte y mantenimiento al sistema de Honeynet Híbrida.
- b. El administrador de la seguridad será el responsable de monitorear constantemente la información que entra y sale de la red de la universidad.
- c. Capacidad que tiene la propuesta de registrar y filtrar cualquier intento de acceso desde la red de honeynet al resto de la red externa.
- d. Capacidad que tiene la propuesta de engañar a posibles atacantes mediante redes falsas simuladas y registrar esos eventos.
- e. Capacidad que tiene la propuesta monitorear accesos a la red no autorizados o posibles ataques mediante un software en ambiente Web personalizado para la Universidad, así como registrarlos y activar las alarmas correspondientes.

3.6.2 Requerimientos no funcionales.

Son restricciones o limitantes ofrecidas por la propuesta.

- a. La propuesta no incluye equipos comerciales como IPS, Router.
- b. No incluye la implementación de la propuesta dentro de la infraestructura de la red de la Universidad, es responsabilidad de la Dirección de Tecnología y Comunicaciones realizar su implementación.

3.7 Diseño de la propuesta de honeynets virtuales utilizando vmware, para la detección de intrusos informáticos.

La propuesta está constituida por Honeypots que por su aplicación para la prevención, detección y respuesta a los ataques se puede llevar a cabo en dos escenarios, uno orientado a reforzar la seguridad de ambientes en producción y otro enfocado a la investigación.

Producción.

En este escenario, las redes de trampa se implantan en ambientes en producción, por ejemplo en la infraestructura de red de una entidad financiera o gubernamental. Sin embargo, esto no quiere decir que las redes de trampa procesen tráfico de producción.

Simplemente se instalan en el mismo ambiente de los sistemas en producción, esperando atraer a los enemigos para que las investiguen, ataquen o comprometan. Las siguientes ideas son algunas de las formas en las que un honeypot ayuda a reforzar la seguridad de la organización:

Cuando el honeypot detecta un ataque, se analizan las herramientas y tácticas utilizadas y se procede a reforzar los sistemas de seguridad para que el ataque no afecte a los sistemas de producción.

Cuando el atacante compromete a un honeypot, este se analiza en detalle para caracterizarlo, se buscan estos patrones en sistemas de producción y se determina si alguno también fue comprometido.

Así, los honeypots representan una herramienta altamente flexible y enfocada a recopilar únicamente tráfico producido por accesos no autorizados y que,

administrada por una política de seguridad de la organización, permite prevenir, detectar y responder a los ataques.

Investigación.

En este escenario, las redes de trampa se implantan para cumplir dos objetivos: investigar las tácticas, herramientas y motivos de la comunidad black-hat; y compartir las lecciones aprendidas.

Uno de los principales problemas en la Seguridad de la Información, es el poco conocimiento acerca de los atacantes y sus herramientas. Las redes de trampa aplicadas a la investigación se enfocan en detectar ataques y en generar y compartir el conocimiento requerido para que las diferentes organizaciones refuercen su infraestructura.

3.7.1 Ubicación de los honeypots.

La ubicación de los Honeypots es esencial para maximizar su efectividad, ya que debido a su carácter intrínsecamente pasivo una ubicación de difícil acceso eliminará gran parte de su atractivo para potenciales atacantes. Por otro lado, si su ubicación es demasiado artificial u obvia cualquier experimentado atacante la descubrirá y evitará todo contacto con ella.

Teniendo en cuenta que los Honeypots pueden servir tanto para la detección de atacantes internos como externos, se debe tener siempre en cuenta la posibilidad de establecer Honeypots internos para la detección de atacantes o sistemas comprometidos en la red (por ejemplo sistemas infectados con un gusano o virus).

Antes del firewall (Front of firewall).

Esta localización permite evitar el incremento del riesgo inherente a la instalación del Honeypot. Como este se encuentra fuera de la zona protegida por el firewall, puede ser atacado sin ningún tipo de peligro para el resto de la red.

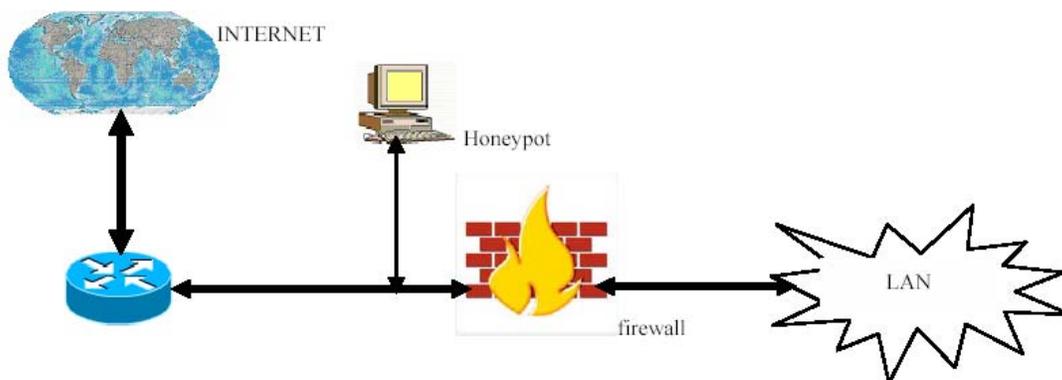


Figura 6: Ubicación del Honeypot antes del Firewall¹³

Esta ubicación nos permite tener un acceso directo a los atacantes, puesto que el firewall ya se encarga de filtrar una parte del tráfico peligroso o no deseado, obteniendo trazas reales de su comportamiento y estadísticas muy fiables sobre la cantidad y calidad de ataques que puede recibir nuestra red.

Cualquier atacante externo será lo primero que encuentra y esto generará un gran consumo de ancho de banda y espacio en los ficheros de log. Por otro lado, esta ubicación nos evita la detección de atacantes internos.

¹³ SEGURIDAD EN REDES IP: Honeypots y Honeynets, Gabriel Verdejo Alvarez, <http://tau.uab.es/~gaby>

Detrás del firewall (Behind the firewall).

En esta posición, el Honeypot queda afectado por las reglas de filtrado del firewall. Por un lado se tiene que modificar las reglas para permitir algún tipo de acceso al Honeypot por posibles atacantes externos, y por el otro lado, al introducir un elemento potencialmente peligroso dentro de la red podemos permitir a un atacante gane acceso al Honeypot, un paseo triunfal por la red.

La ubicación tras el firewall permite la detección de atacantes internos así como firewalls mal configurados, máquinas infectadas por gusanos o virus e incluso atacantes externos.

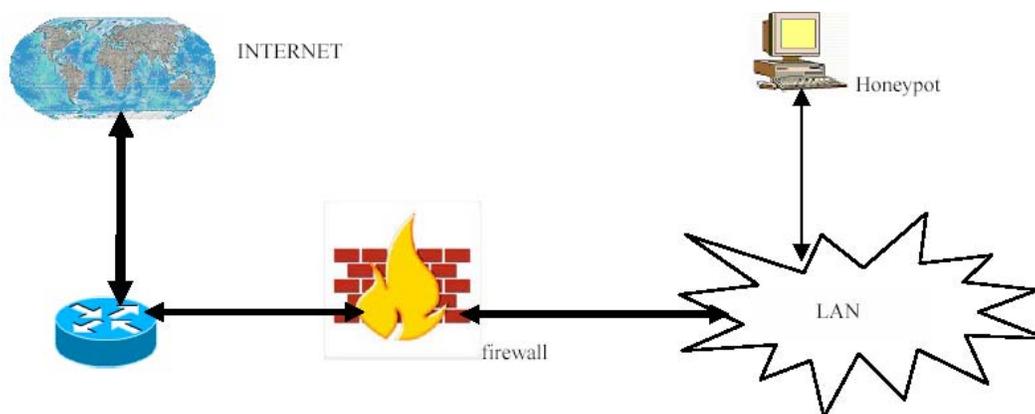


Figura 7: Ubicación del Honeypot tras el Firewall¹⁴

Sin embargo las desventajas más destacables son la gran cantidad de alertas de seguridad que generarán otros sistemas de seguridad de la red (Firewalls, IDS) al recibir ataques el Honeypot y la necesidad de asegurar el resto de la red contra el Honeypot mediante el uso de firewalls extras o sistemas de bloqueo de acceso, ya que si un atacante logra comprometer el sistema tendrá vía libre en su ataque a toda la red.

¹⁴ SEGURIDAD EN REDES IP: Honeypots y Honeynets, Gabriel Verdejo Alvarez, <http://tau.uab.es/~gaby>

La zona desmilitarizada (into DMZ).

La ubicación en la zona desmilitarizada permite por un lado juntar en el mismo segmento a los servidores de producción con el Honeypot y por el otro controlar el peligro que añade su uso, ya que tiene un firewall que lo aísla de resto de la red local.

Esta arquitectura permite tener la posibilidad de detectar ataques externos e internos con una simple reconfiguración del sistema de firewall puesto que se encuentra en la zona de acceso público.

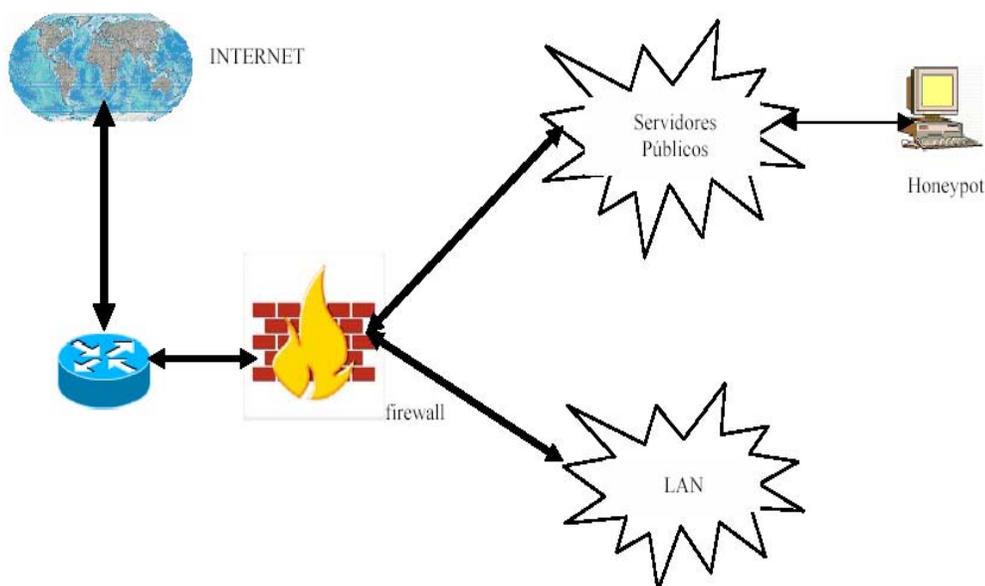


Figura 8: Ubicación del Honeypot en la zona desmilitarizada (DMZ)¹⁵

¹⁵ SEGURIDAD EN REDES IP: Honey-pots y Honey-nets, Gabriel Verdejo Alvarez, <http://tau.uab.es/~gaby>

3.7.2 Elementos de la honeynet.

La Honeynet que es una extensión de honeypots, es una red controlada y monitoreada la cual ha sido diseñada para ser comprometida pero al mismo tiempo se monitorea y se analiza toda la actividad en ella, y cualquier tráfico es sospechoso por naturaleza. Dentro de los requerimientos de una Honeynet se debe de contemplar dos elementos críticos para su correcta implementación: la captura de datos, y el control de datos.

Captura de datos.

El objetivo de toda Honeynet es el obtener información tanto de las amenazas que atacan contra los sistemas de información, así como del comportamiento de los intrusos y sus motivos. Esto quiere decir que todo el tráfico de entrada y salida, así como la actividad en cada equipo dentro de la Honeynet debe de ser registrado para su posterior análisis.

Una de los puntos más importantes en la captura de datos es la descentralización de los mecanismos de captura. Esto quiere decir, que deben de existir una infraestructura de captura por capas, de manera que si un sistema de captura de datos llegase a fallar, no esté todo perdido. Otro punto importante es que por ningún motivo se debe de almacenar información en los Honeypots, debido a que el intruso podría darse cuenta de que se encuentra dentro de un Honeypot (depende del control de datos) y borrar la información obtenida por el Honeypot, o peor aún, modificarla y así obtendremos información errónea sobre el incidente.

En la figura 8 se puede observar un diseño de una Honeynet con varias capas dedicadas a la captura de datos. Para que un intruso llegue a los Honeybots, tiene que pasar por el firewall (comúnmente implantado como un firewall invisible) en el cual se tiene el primer registro de la actividad hacia la Honeynet.

Después de esto, debido a que el firewall permite todo el tráfico de entrada hacia la Honeynet, el router funciona como una segunda capa, en la que se puede obtener algunos datos sobre la actividad hacia los Honeybots, y además existe un detector de intrusos que nos ayudará a obtener información identificada como un escaneo o algún ataque.

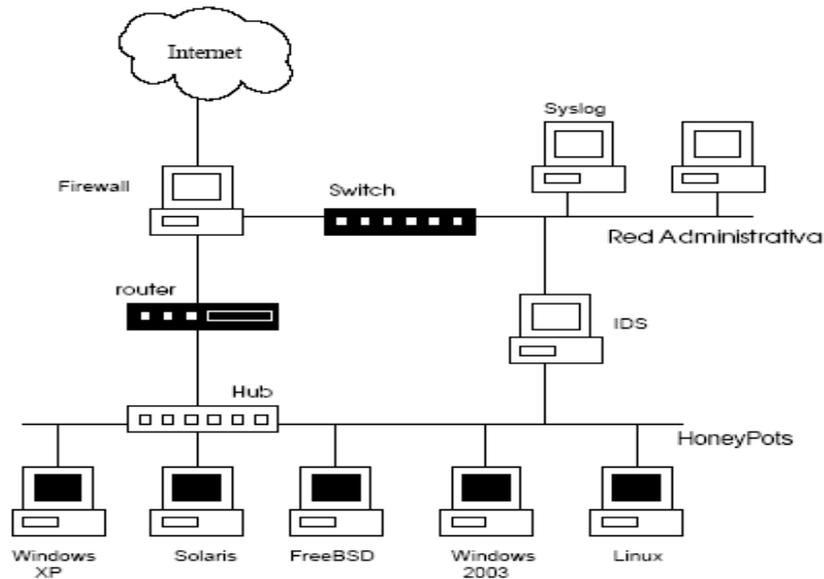


Figura 9: Diagrama de Honeynet¹⁶

¹⁶ Honeynet Project. Know Your Enemy; Revealing the Security Tools, Tactics, and Motives of the Blackhat Community. Addison Wesley, 2002.

Control de datos.

El control de datos dentro de una Honeynet nos permitirá limitar el tráfico que salga desde ella, debido a que si un equipo es comprometido, se debe evitar que sea utilizado para comprometer a otros sistemas fuera de la Honeynet. Sin embargo esto podría delatar el propósito del equipo al cual el intruso ha entrado, de manera que cuando se dé cuenta que la actividad hacia la red está limitada, el equipo no será de su interés y podría borrar toda la evidencia que ha generado, y nosotros perderíamos la oportunidad de aprender más sobre el intruso.

Una manera de evitar esto, es el permitir cierta cantidad de tráfico desde la Honeynet hacia el exterior, además de limitar los servicios a los cuales se puede conectar desde la Honeynet.

Por ejemplo, después de comprometer un sistema, el intruso podría intentar atacar a otros equipos utilizando un ataque de denegación de servicio, pero para ello, podría necesitar conectarse a un servidor externo para obtener sus herramientas para lanzar el ataque, y por ello necesitará salida a un servidor ftp por ejemplo.

El punto clave en el control de datos es la automatización. Una idea práctica de llevar un control de datos adecuado es el verificar en el tráfico de salida la configuración de banderas en conexiones TCP, o el numero de paquetes UDP que salen de un Honeypot, de igual manera habrá que verificar el tráfico ICMP en caso de que se utilice para ataques de DoS.

Cuando se exceda un umbral predefinido, se puede agregar una regla al firewall para que impida más tráfico desde el Honeypot, y enviar una alerta al administrador ya sea por correo electrónico o por cualquier otro medio, para informarle de dicho suceso.

Con todo lo anterior se puede determinar que la finalidad de la propuesta es definir la configuración de las componentes informáticas que van a formar el sistema (tanto para la aplicación como para la seguridad de la red) y la definición de un esquema de red con las características necesarias para poder garantizar la seguridad del sistema.

3.7.3 Esquema genérico de la propuesta.

La propuesta presenta la mejor forma de aplicar las opciones de implementación de una red de Honeynet Virtual con una computadora configurada para un ambiente de producción, cuya ubicación está en la zona desmilitarizada (DMZ), el diseño permite proteger la red de intrusos tanto externo como interno mediante técnicas de filtrado de paquetes (cortafuegos) como control de datos.

Además permite monitorear los accesos a la red que no son autorizados y se registran en archivos Log, para esto se utiliza técnicas de detección de intrusos (IDS: sistemas de detección de intrusos) como captura de datos, por lo que la categoría de la Honeynet Virtual a diseñar es, **la Híbrida**.

Para llevar a cabo el prototipo de la propuesta se requiere de los siguientes 7 equipos:

- a. Una computadora que haga la función de Cortafuego 1.
- b. Una computadora que haga la función de ProxyNAT.
- c. Una computadora que haga la función de HONEYNET.
- d. Una computadora que haga la función de IDS1.
- e. Una computadora que haga la función de Cortafuego 2.

- f. Una computadora que haga la función de IDS2.
- g. Una computadora que haga la función de Aplicaciones y Bases de Datos.
- h. Para efectos de monitoreo y acceso a la red se requiere una Laptop para monitoreo y acceso.

Esquema genérico de la propuesta.

Se ha realizado un diseño de red estructurado en capas o niveles de seguridad:

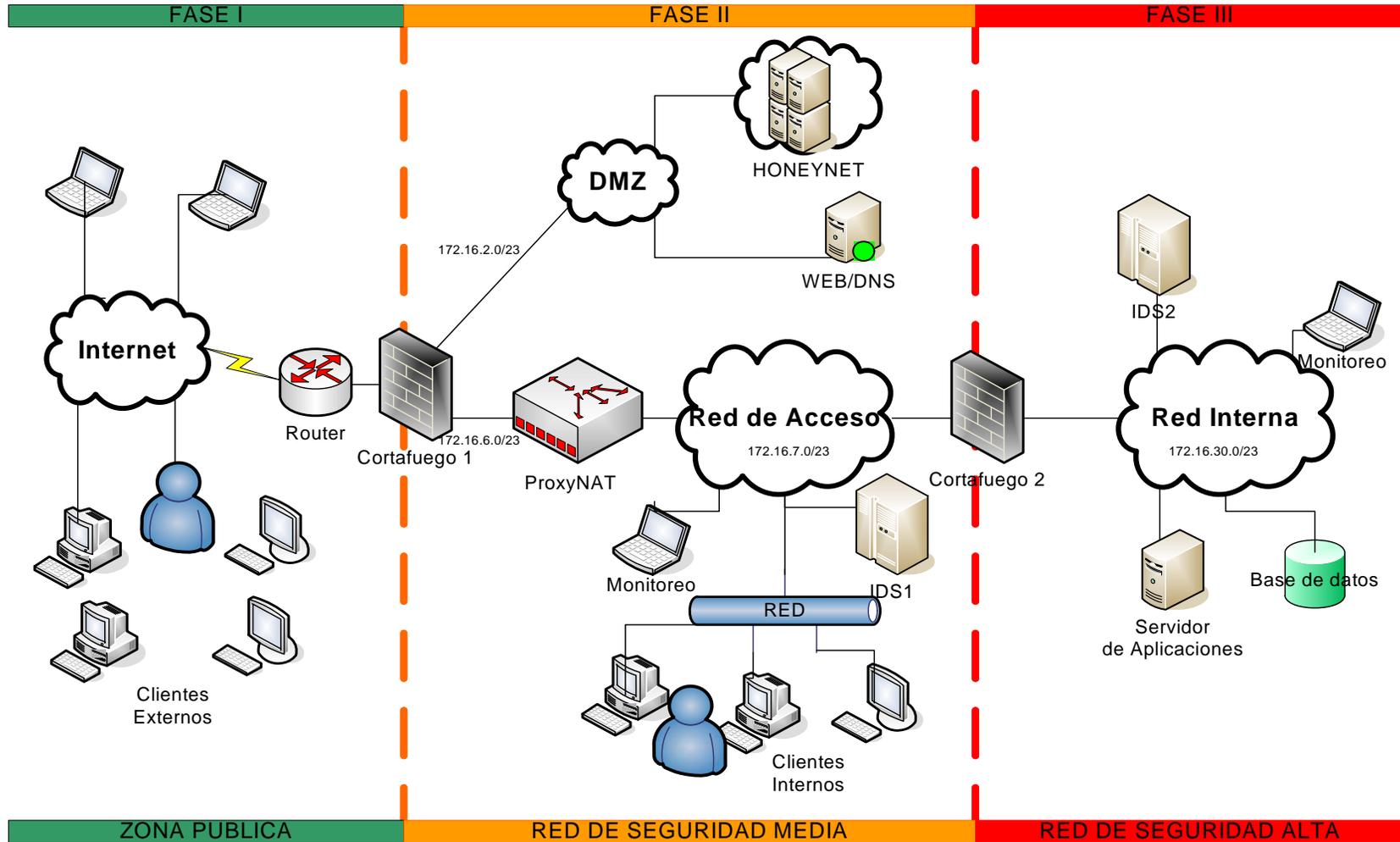


Figura 10: Diseño de esquema genérico de la Red

3.7.4 Descripción de la propuesta genérica.

A continuación se describen en qué consiste cada una de las fases de la figura 9:

Fase I.

Zona pública: Esta zona es de uso público y pertenece a la Internet pública. Desde esta zona se van a conectar los usuarios que accedan a los sistemas por Internet.

Esta zona está constituida por el router exterior conectado a Internet y obliga que todo el tráfico entrante pase a través del cortafuego, el cortafuego es una computadora existente entre el usuario y el mundo exterior para proteger todo el sistema Universitario de los intrusos, que en la mayoría de las circunstancias, los intrusos proceden de Internet y de las miles de redes que se interconectan.

El router proporciona una seguridad básica en la zona, frente a la red exterior o un área menos controlada y desde la interior, proporcionando un punto de aislamiento para que el resto de la estructura de la red interna no se vea afectada.

El cortafuego se instala entre la zona pública y la zona de seguridad media, cuyo propósito es dejar pasar todo paquete de entrada a la DMZ que van dirigidos a la HoneyNet y paquetes de consulta a los servidores públicos y filtrar los paquetes que van dirigidos a la red interna y a la zona de alta seguridad

Fase II.

Red de seguridad media: Esta es la red donde se conectarán los usuarios internos. Estará monitorizada por un sistema de detección de intrusos (IDS1), siendo este el dispositivo de “captura de datos” para el diseño complementario de la HONEYNET híbrida.

El IDS es una herramienta de seguridad encargada de monitorizar los eventos que ocurren en un sistema informático en busca de intentos de intrusión. Definimos intento de intrusión como cualquier intento de comprometer la confidencialidad, integridad o disponibilidad de un sistema informático, o de eludir los mecanismos de seguridad de éste. Las intrusiones se pueden producir de varias formas:

- a. Atacantes que acceden a los sistemas desde Internet.
- b. Usuarios autorizados del sistema que intentan ganar privilegios adicionales para los cuales no están autorizados.
- c. Usuarios autorizados que hacen un mal uso de los privilegios o recursos que se les ha sido asignados.

Objetivos de un IDS:

- a. Prevenir problemas al disuadir a individuos hostiles: Al incrementar la posibilidad de descubrir a los atacantes, el comportamiento de algunos cambiará de forma que muchos ataques no llegarán a producirse.

Esto también puede resultar atractivo, puesto que la presencia de un sistema de seguridad sofisticado puede hacer crecer la curiosidad del atacante por ver qué es eso que tanto intentamos proteger.

- b. Detectar violaciones de seguridad que no pueden ser prevenidas: Los atacantes pueden conseguir accesos no autorizados a muchos sistemas cuando vulnerabilidades conocidas no son corregidas.

Esta corrección no siempre es posible, ya sea por problemas de tiempo por parte del administrador o simplemente por un fallo de configuración. Aunque un IDS podría no detectar cuando un atacante en un sistema ha tenido éxito explotando un fallo no corregido, sí puede avisar al administrador para que lleve a cabo inmediatamente un backup del sistema y evitar así que se pierda información valiosa.

- c. Detectar preámbulos de ataques: Cuando un individuo ataca un sistema, lo hace típicamente en fases predecibles. En la primera fase, un atacante hace pruebas y examina el sistema o red en busca de un punto de entrada óptimo.

En sistemas o redes que no disponen de un IDS, el atacante es libre de examinar el sistema con un riesgo mínimo de ser detectado. Esto le facilita la búsqueda de un punto débil en la red. La misma red con un IDS monitorizando sus operaciones le presenta una mayor dificultad.

Aunque el atacante puede examinar la red, el IDS observará estas acciones, las identificará como sospechosas, avisará al personal de seguridad de lo ocurrido para que tome las acciones pertinentes.

- d. Proveer información útil sobre las intrusiones que ocurren: Incluso cuando los IDS no son capaces de bloquear ataques, pueden recoger información detallada y relevante sobre éstos.

Esta información puede, bajo ciertas circunstancias, ser utilizada como pruebas en actuaciones legales. También se puede usar esta

información para detectar fallos en la configuración de seguridad o en la política de seguridad de la organización.

El Cortafuegos 1 que da acceso a los usuarios externos deberá tener reglas de filtrado para asegurar que los paquetes vayan al destino esperado.

El cortafuegos 2 dará paso a los paquetes exclusivos para la zona de alta seguridad en donde se concentran los servidores de aplicaciones y bases de datos.

Tanto el cortafuegos 1 y 2 son dispositivos de “**control de datos**” para el diseño complementario de la HONEYNET híbrida.

El dispositivo ProxyNAT tiene el objetivo de ofrecer un tercer punto de filtrado, con las mismas reglas que el cortafuego entre la zona pública y la zona de seguridad media, redireccionar los paquetes entrantes (basándose en el puerto), hacia las máquinas correspondientes y ocultar las direcciones IP de las redes internas.

Se instalará una red perimetral (o DMZ) para instalar el servidor WEB/DNS y un servidor HoneyNet.

El equipo Honeynet se encargara de simular servidores, de forma que se podría engañar a un posible atacante de la red, si intentase acceder a estos.

Estos dispositivos no ofrecerán ningún obstáculo para acceder al sistema, para el caso de implementación se tiene dos opciones, utilizar el método del “User Mode” de Linux o el software VMware.

La honeynet que se presenta en este diseño es la Honeynet Híbrida, combinación de la clásica Honeynet y del software virtual. Control de Datos, como por ejemplo

cortafuegos, y captura de datos, como por ejemplo sensores IDS y almacenamiento de logs, están en un sistema separado y aislado.

Este aislamiento reduce el riesgo de compromiso. Sin embargo, todas las honeynets son virtualmente ejecutadas en una única máquina.

Fase III.

Red de seguridad Alta (red de servidores): Esta red es donde van a estar todos los servidores. Estará protegida por un cortafuegos 2, sistema que también hará las labores de filtro entre esta red y la red de acceso para evitar los posibles accesos no autorizados a estos servidores.

Esta red también estará monitorizada por otro sistema de detección de intrusos (IDS2).

3.7.5 Propuesta de esquema para la Universidad Francisco Gavidia.

La propuesta presenta un esquema adaptable a la infraestructura de red de la Universidad Francisco Gavidia, así mismo se plantea el modelo propuesto de la Honeynet Virtual ubicada en la zona desmilitarizada tres (DMZ 3).

El esquema parte de incluir los componentes que no están presentes en el diseño original de Red de la Universidad, siendo estos complementarios al Router y Firewall que están en función actualmente. Los componentes a incluir son los siguientes:

- a. Una computadora que haga la función de Honeynet Virtual.
- b. Una computadora que haga la función de IDS1.

- c. Una computadora que haga la función de Cortafuego 2.
- d. Una computadora que haga la función de IDS2.

La Honeynet virtual sigue siendo la Híbrida para el diseño de la Red de la Universidad (Figura 10) y en el modelo del Honeynet en la DMZ 3 será la auto-contenida (Figura 11).

Esquema de la propuesta orientada a la UFG.

Se ha realizado un diseño de red estructurado en capas o niveles de seguridad:

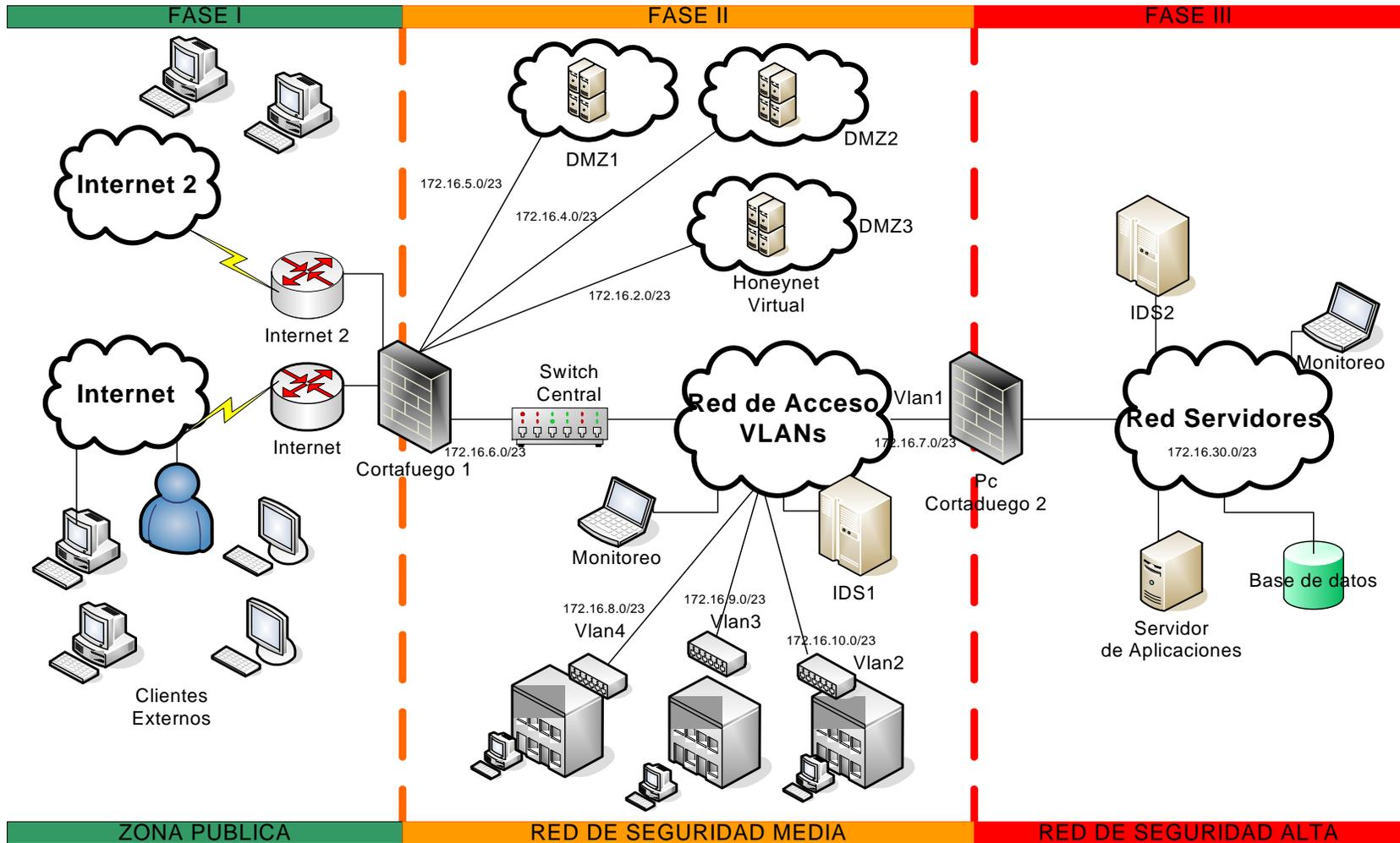


Figura 10: Diseño de la propuesta orientada a la de la Red-UFG

3.7.6 Descripción de la propuesta de la Universidad Francisco Gavidia.

La propuesta se ha elaborado para que sea desarrollado en tres fases, en las cuales se detallan los aspectos principales para poder comprender el propósito de cada una de ellas y que permitirá ser implementada por el personal de la Universidad Francisco Gavidia, específicamente por la Dirección de Tecnología y Comunicaciones, sin necesidad de contratar a una empresa para que realice dicho trabajo.

Fase I.

Zona pública: Esta zona está constituida por dos router externos, uno de ellos conectado a Internet comercial y el otro a la red avanzada conocida como Internet 2, ambos router obligan que todo el tráfico entrante pase a través del Firewall, este cortafuego es un equipo existente entre el usuario y el mundo exterior para proteger todo el sistema Universitario de los intrusos.

Tanto los router y el firewall están en función actualmente en la infraestructura la de red de la Universidad.

Fase II.

Red de seguridad media: Esta zona estará constituida por los siguientes equipos:
Una computadora que hará la función de IDS1, este equipo será instalado bajo el sistema operativo Linux, concretamente RedHat versión 9, el IDS que se utilizará es SNORT, un sistema de detección de intrusos de código abierto personalizado para ser administrado en la UFG.

Para realizar la monitorización del IDS, se instalará una consola de análisis de sistemas IDS, el software ACID, también de código abierto. Además se utilizarán las siguientes librerías y Servidor Apache:

- a. Snort 2.1.0
- b. Apache 2.0.48
- c. PHP 4.3.4
- d. ADODB v3.30
- e. Base
- f. Zlib 1.1.4
- g. JPGGraph 1.11
- h. LibPcap 0.8.1

El direccionamiento IP que se utilizará es 172.16.0.0/16 para ser distribuida en rangos de 512 IPs en toda la infraestructura de la Red de la UFG por segmento.

Una computadora que hará la función de Honeynet Virtual en la DMZ 3, cuyo modelo se detalla en la figura 11, la herramienta de virtualización que se ocupará es VMware Server.

Es una red compuesta por un sistema físico y tres virtuales, distribuidos en tres segmentos, el sistema anfitrión es el equipo físico que albergará el software de virtualización sobre el que se va ejecutar la red virtual.

De las conexiones que presenta el sistema anfitrión, se encuentra la conexión con el Honeywall, denominado así por sus tareas de control, captura y recolecciones de datos en un solo equipo, la conexión con el Firewall para la administración remota de la Honeynet.

La tarea de control de las acciones del intruso para evitar que lance ataques contra sistemas del exterior desde los Honeypots se realizará en el Honeywall,

para esto se configurará en modo Bridge (switch virtual) y se utilizará la acción combinada de Iptables y Snort Inline.

Iptables es un cortafuegos que funciona como un módulo de las versiones de Linux y es capaz de filtrar tráfico, Snort Inline es una versión modificada de Snort que inspecciona el tráfico que le llega en busca de patrones conocidos de ataque. El comportamiento del Honeywall es:

- a. Registrar y permitir cualquier intento de conexión desde el exterior de la Honeynet a un sistema de la red de Honeypots.
- b. Registrar y descartar cualquier intento de ataque desde la red de Honeypots.
- c. Registra y permite el envío de logs desde los honeypots al servidor remoto y desde el propio Honeywall al sistema anfitrión.
- d. Registra y filtra el tráfico generado en los honeypots dirigido a sistemas del exterior de la Honeynets en función de los patrones de ataques conocidos por Snort Inline.

El Honeywall se va a encargar de registrar los intentos de conexión que tengan como origen o destino alguno de los Honeypots de la Honeynet, donde serán analizados en tiempo real mediante el software Walleye, que es la interface web administrativa del Honeywall.

El modo en que se capturará el tráfico de red VMware simula switches para interconectar las pcs virtuales. Los switches virtuales pueden configurarse de dos modos:

- a. Switches Host-only permite interconectar PCS virtuales entre sí, así como el sistema anfitrión, en cuyo interior se genera una interfaz de red virtual.
- b. Switch en modo Bridge, se asocia a una interfaz física de red del sistema anfitrión. A través de esta tarjeta las PCS virtuales conectadas al switch pueden acceder, con una dirección IP propia, al mismo segmento físico del sistema anfitrión, como si fueran unos equipos más de los conectados al segmento.

Los segmentos VMnet0 y VMnet2 de la figura 11 son switches virtuales configurados en modo bridge.

Desde el sistema Honeywall, utilizando Snort, se capturará a través de las interfaces asociadas a cada uno de los switches todo el tráfico que atraviese los segmentos y los últimos serán los propios Honeybots de la red, en ellos se recopilará información tanto sobre lo que ocurra en el sistema operativo, las aplicaciones y los servicios que se ejecuten.

En el segmento inferior se encuentran dos PCS virtuales que serán los Honeybots que se van a exponer con la intención de recibir los ataques de la comunidad de intrusos.

Para la captura de sesiones del intruso se va a utilizar Sebek en los sistemas Linux y Windows.

Sebek es un módulo de Kernel que captura las teclas pulsadas por el intruso y los ficheros descargados por este en el sistema comprometido. Este software se oculta en el sistema para evitar ser detectado o desinstalado y envía la información recopilada al servidor remoto.

Los discos duros virtuales se pueden configurar de los siguientes modos:

- a. Persistente: Las modificaciones se realizan en tiempo real en el disco duro virtual.
- b. No persistente: Las modificaciones realizadas se descartan al apagar la pc virtual, volviéndose al estado normal.
- c. Restaurables: Al apagar el sistema se ofrece al usuario la opción de fijar o descartar los cambios en el disco duro.

Se utilizará discos duros en modo restaurable, las modificaciones se irán almacenando en ficheros con extensión REDO en el directorio de la PC virtual.

Modelo propuesto de honeynet virtual ubicada en la zona desmilitarizada.

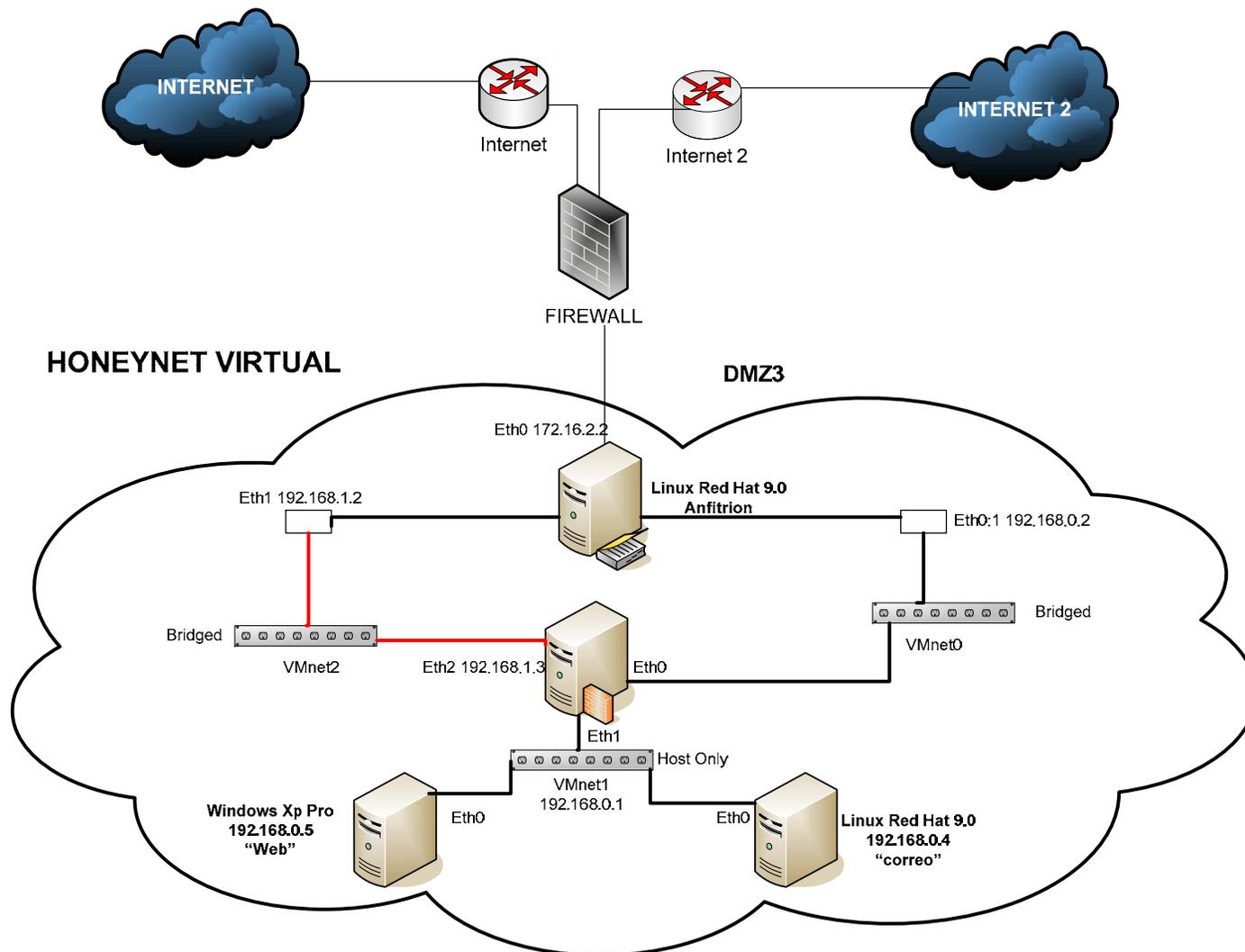


Figura 11: Diseño de la Honeynet Virtual-DMZ

Red de seguridad Alta (red de servidores): Estará constituida por un cortafuego, cuya función la hará Iptables de Linux, configurado en una PC con RedHat 9 de Linux.

También estará monitorizada por otro sistema de detección de intrusos (IDS2), esta computadora será instalada bajo el sistema operativo Linux RedHat versión 9, el IDS que se utilizará es SNORT con las mismas librerías y software que el IDS1.

3.8 Recomendaciones.

- a. A través de la propuesta se llegó a la conclusión que mejorará la seguridad de la infraestructura de la red de la Universidad ya que permitirá controlar y monitorizar el tráfico de la información.
- b. Permitirá obtener información de los eventos de intrusión y ser analizado posteriormente.
- c. Permitirá que el Administrador de la Seguridad de la Universidad este en constante actualización, lo que permitirá también actualizar las versiones de las aplicaciones propuestas en el diseño de solución.
- d. Se recomienda realizar copias de seguridad periódicamente de la información y aplicaciones de la propuesta de diseño cuando esta se halle operando.
- e. Se recomienda actualizar los sistemas tanto en software como en hardware de los componentes de seguridad debido a que la tecnología cambia constantemente.
- f. Se recomienda la implementación de la propuesta de diseño orientada a la Universidad para su seguridad en el manejo de la información, a fin de que este protegido contra ataques de intrusos informáticos.

3.9 Conclusiones.

- a. La herramienta honeynet, representa una solución de bajo costo complementaria a todas las herramientas de seguridad comerciales en el mercado, permitiendo a la Universidad Francisco Gavidia u organizaciones interesadas en proteger y resguardar de una mejor forma el activo primordial, la información.
- b. La información del prototipo presentado es una herramienta de solución funcional de seguridad adicional para el fortalecimiento de una existente, el cual permite capturar y controlar ataques hacia la información que se maneja.
- c. La información del prototipo presentado puede ser tomado como base para el desarrollo en la UFG, ya que cumple con las necesidades actuales de la Universidad Francisco Gavidia.
- d. La solución de seguridad con estos tipos de elementos y la realización del prototipo puede ser de utilidad para las áreas de investigación y el fortalecimiento de la misma a través de estudio de patrones anómalos.