UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

IMPLEMENTACIÓN DE UN LABORATORIO DE NETWORKING PARA EL DESARROLLO DE REDES DE PRÓXIMA GENERACIÓN Y APLICACIÓN DE PENTESTING

TESIS
PARA OBTENER EL GRADO DE
INGENIERO EN REDES

PRESENTA
DAMIÁN JANITZIO CORTÉS BRICEÑO

DIRECTOR DE TESIS
MTI. VLADIMIR VENIAMIN CABAÑAS VICTORIA

ASESORES
MSI. LAURA YÉSICA DÁVALOS CASTILLA
DR. JAVIER VÁZQUEZ CASTILLO
MSI. RUBÉN ENRIQUE GONZÁLEZ ELIXAVIDE
DR. JAIME SILVERIO ORTEGÓN AGUILAR

CHETUMAL QUINTANA ROO, MÉXICO, JUNIO DE 2018

UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

TRABAJO DE TESIS TITULADO

"IMPLEMENTACIÓN DE UN LABORATORIO DE NETWORKING PARA EL DESARROLLO DE REDES DE PRÓXIMA GENERACIÓN Y APLICACIÓN DE PENTESTING"

ELABORADO POR

DAMIÁN JANITZIO CORTÉS BRICEÑO

BAJO SUPERVISIÓN DEL COMITÉ DE ASESORÍA Y APROBADO COMO REQUISITO PARCIAL PARA OBTENER EL GRADO DE:

INGENIERO EN REDES

COMITÉ DE TESIS

DIRECTOR:

MTI. VLADIMIR VENIAMIN CABAÑAS VICTORIA

ASESORA:

MSI. LAURA YESICA DÁVALOS CASTILLA

ASESOR:

DR. JAVIER VÁZQUEZ CASTILLO

ASESOR:

MSI. RUBÉN ENRIQUE GONZÁLEZ ELIXAVIDE

ASESOR:

DR. JAIME SILVERIO ORTEGÓN AGUILAR

CHETUMAL QUINTANA ROO, MÉXICO, JUNIO DE 2018.

Dedicatoria

A los maestros, a la carrera y a los alumnos de Ingeniería en Redes de la Universidad de Quintana Roo.

Agradecimientos

A Dios, a mi madre, mi hermana y a los maestros de la carrera de Ingeniería en Redes, en especial al maestro Vladimir que me ha ayudado y tendido la mano en momentos difíciles.

Resumen

El presente trabajo de investigación y desarrollo de un nuevo laboratorio de networking tiene dos objetivos principales: Proveer a los estudiantes de la carrera de ingeniería en redes una base tecnológica para el desarrollo de redes de próxima generación, como es el caso de redes híbridas, basadas en software u otra tendencia pertinente en este tema, el segundo objetivo se basa en la propuesta de escenarios para llevar a cabo pruebas de penetración en seguridad informática. Todo esto soportado por tecnología de virtualización de los equipos informáticos y de telecomunicaciones comúnmente utilizados en el ámbito profesional.

En el primer capítulo se describe la situación actual de la seguridad en el mundo real y se aborda el planteamiento del problema, el cual deja de manera clara la necesidad de contar con herramientas informáticas para hacer frente a los retos en materia de seguridad informática y avances en las tecnologías de redes.

El capítulo dos provee los conceptos mínimos necesarios para entender la seguridad informática, y un análisis breve de las tecnologías de virtualización para poder aplicar las propuestas tecnológicas del presente proyecto.

En el capítulo tres se detalla el desarrollo y la implementación de la base tecnológica en la cual se podrán montar los diferentes escenarios en el desarrollo de redes de próxima generación y las pruebas de penetración a sistemas informáticos.

En el capítulo cuatro se exponen los resultados de la implementación de esta base tecnológica virtualizada, así como las conclusiones a las que he llegado después de llevar a cabo este proyecto.

Tabla de contenido

Lista de figuras

CAPÍTULO I Introducción.

"El conocimiento es poder".

Francis Bacon.

La seguridad informática es un campo muy extenso e interesante dentro del mundo de las tecnologías de la información y comunicación, se encuentra presente en muchos ámbitos, por ejemplo, en la educación, en la industria, en el gobierno, en prácticamente cualquier actividad de los seres humanos que se apoya o utiliza la tecnología.

La información tiene un efecto significativo al individuo como tal respecto a su privacidad, ya que puede cobrar distintas dimensiones dependiendo de la cultura del mismo. En la seguridad de la información es importante señalar que su manejo está basado en la tecnología y debemos de saber qué puede ser confidencial; de ser divulgada, mal utilizada, robada, borrada o saboteada afectará su disponibilidad y la pone en riesgo.

La información es poder, y según las posibilidades estratégicas que ofrece, ésta se clasifica como: (Reyes Krafft, y otros, 2016)

- Crítica: Es indispensable para la operación de la empresa
- Valiosa: Es un activo de la empresa y muy valioso.
- Sensible: Debe de ser conocida solo por las personas autorizadas

Los peligros se han multiplicado de la noche a la mañana. Los dispositivos que alguna vez fueron útiles y entretenidos se han convertido espontáneamente en amenazas. Las primeras computadoras estaban ocultas en los laboratorios y sus usuarios eran ingenieros y científicos. La computación como instrumento del crimen no estaba en la mente de nadie. Pero esto ha cambiado. Ahora en lugar de ser protegidas, las computadoras grandes y pequeñas se exponen de manera que no podría haber sido imaginado por sus inventores. (Waschke, What's Biting Us?, 2017)

Muchos errores que permiten la acción de los criminales podrían ser fácilmente corregidos; pero lamentablemente muchas compañías prefieren pasar por alto estos problemas, y en muchos casos incluso son muy displicentes. La falta de conciencia de los administradores y los usuarios son identificados como los principales obstáculos para implementar la seguridad en las empresas. Éstas mismas admiten sufrir ataques en los últimos doce o seis meses. Lo peor de todo es que algunos no saben si han sido o si están siendo atacados o no y, a pesar del aumento esperado en problemas con la seguridad y el crecimiento del índice de ataques e invasiones, las encuestas actuales muestran que sólo la mitad e incluso menos cuentan con planes de acción en caso de ataque. (Ulbrich & Della Valle, 2004)

A continuación se muestra una lista de las amenazas y objetivos más comunes: (Waschke, What's Biting Us?, 2017)

- Objetivos más vulnerables y comprometidos.
    - Corporaciones.
    - Tablets y smartphones.
    - Tecnologías inalámbricas.
    - Dispositivos IoT.
- Ataques más utilizados.
    - Ingeniería social.
    - Phishing.
        - Malware a través de phishing.
    - MITM.
    - Malware.
        - Troyanos.
        - Herramientas de acceso remoto.
        - Gusanos.
        - Virus.
        - Ransomware.
    - Día cero.
    - Cracking de contraseñas.

- DDOS.
- Botnets.
- Abusos de medios sociales.
    - Cyberbullying.

Como resultado de la lista anterior podemos determinar las principales brechas de seguridad que enfrentan las empresas desde grandes a pequeñas y obviamente el personal que labora en ellas:

- Comunicaciones inseguras
- Robo de información.
- Aplicaciones de software desactualizadas.
- Políticas de seguridad deficientes.
- Falta de inversión en seguridad digital y no digital.
- Falta de cultura informática.
- Desinformación.

Planteamiento del problema.

El proceso de aprendizaje entre los estudiantes de la Universidad de Quintana Roo del Programa Educativo de Ingeniería en Redes se puede realizar de diversas maneras; pero por lo general existen dos muy comunes: el autodidacta y el guiado (con sus variaciones).

El aprendizaje en el tema de seguridad informática concretamente en la carrera de Ingeniería en Redes cuenta con un gran interés; sin embargo, aún no se cuenta con la infraestructura suficiente para llevar a cabo prácticas avanzadas en un laboratorio de seguridad informática; al ser un campo muy amplio, requiere de diversos esquemas de diseño, análisis, implementación y pruebas con diferentes enfoques para poder ser abordado; en este proyecto nos enfocaremos en nuestra condición de instituto de educación superior.

Actualmente el Programa de Ingeniería en Redes tiene acceso a un pequeño laboratorio de seguridad informática donde se pueden realizar algunas prácticas básicas y de manera limitada, lo que no cubriría lo esencial de un buen adiestramiento en hacking ético. Los conocimientos

que van adquiriendo los estudiantes en muchas ocasiones no pueden ponerse en práctica debido a esta situación.

Justificación.

Gran parte de la carrera de Ingeniería en Redes nos permite el entendimiento de las diferentes técnicas que se emplean en las pruebas de intrusión, ésta hace que se tenga ventaja y se amenice muchos temas que muchas veces las personas que apenas se están inicializando en ésta se les dificulte o su camino hacia el aprendizaje sea más largo.

La seguridad informática en el mundo real es muy solicitada por empresas, organizaciones tanto privadas y/o públicas, gobiernos e instituciones de todo tipo. Es entonces que sería una gran oportunidad de ampliar de manera directa el campo laboral para los alumnos de esta academia. Dar ese “empujón” hacia más oportunidades e incluso de estilos de vida.

Podemos con éstos ampliar la cultura informática por medio de la educación y más concretamente en la seguridad. Así de este modo podemos poco a poco con lo que concierne en esta ciudad y en esta universidad, cerrar aún más esas brechas que ocasionan muchos problemas y hasta peligros.

Propuesta.

Existen muchas ideas frecuentes para poder remediar o al menos tratar estos inconvenientes y dar orientación a la justificación; primero debemos de empezar con la parte material mencionando las opciones disponibles que se puedan cristalizar hacia un nuevo laboratorio:

- Crear una plataforma cien por ciento virtual en el cual el individuo pueda probar las distintas herramientas de auditoría.
- Crear una plataforma híbrida, es decir, un escenario en el cual se mezclen tanto computadores virtuales y computadores en un ambiente real, es decir, que los equipos de red sean físicos y que las maquinas sean virtuales o viceversa.
- Crear un ambiente cien por ciento tangible en el cual la persona pueda explotar sus destrezas de manera como si estuviera en el mundo real.

Segundo, empezar a proponer la sección ética, es decir, crear las pautas para el campo de lo formal hasta de concientización. Aquí se planea fundamentar la mentalidad de la responsabilidad que conlleva el hacking ético, como se menciona en el planteamiento del problema y usar metodologías en las cuales les de dirección a las diferentes pruebas de auditoria ya sean a plataformas base, web, inalámbricas etcétera.

En último lugar, dar apertura de tiempo para los grupos de trabajo de la carrera de redes a poder completar las prácticas generales de redes u de otra tecnología en proceso de investigación dado así el aprovechamiento del pequeño espacio que actualmente se posee de forma eficaz y eficiente.

Objetivo general

Implementar una plataforma de red híbrida, virtual y controlada para el desarrollo de redes de nueva generación y aplicación de prácticas de pentesting.

Objetivos particulares.

- Diseñar e implementar una topología de red con equipos reales adecuados y suficientes para soportar la instalación de la plataforma virtual.
- Seleccionar e implementar la plataforma de software que emula redes reales.
- Diseñar e implementar un escenario virtual con diversos protocolos de red, servidores, clientes, equipo para realizar pentesting, firewalls, enrutadores, conmutadores etc.
- Realizar pruebas de conectividad de los escenarios.
- Habilitar el acceso remoto a estudiantes para la realización de las prácticas avanzadas de seguridad informática.

Consideraciones

Teniendo una perspectiva de alcance y tomando en cuenta el costo-beneficio con relación a la elección de los tres tipos de laboratorios propuestos, se debe mencionar que en todas las opciones presentadas en los puntos anteriores se tiene como intención un ambiente controlado, es decir, si el laboratorio es virtual entonces que se dedique una terminal para soportar los

diferentes tipos de sistemas operativos y arquitecturas, y si es en un ambiente real que estén en un ambiente aislado del ambiente de producción.

Es imprescindible también señalar como propósito, que el acceso a los recursos también será de manera remota con cualquiera de los tres tipos de ambiente que se quieran optar. Con esta manera el cursante podrá de modo presto tener comodidad desde su hogar cuando sus demás prioridades cuando se vean enfocados a las tareas de la materia en cuestión, teniendo las restantes cumplidas o reprogramadas.

Cuando el alumno sepa cómo funcionan los equipos, cómo se comunican entre ellos y cómo manejarlos o darles ordenes, se pasará a aprender las diferentes técnicas y el uso de herramientas que irán formando como profesional en la seguridad informática para justamente llegar a estos puntos como aspiración de parte del estudiante:

- Ataques a la red e infraestructura, ya sea cableada o inalámbrica.
- Ataques de aplicación, independiente del lenguaje o implementación.
- Ataques de factor humano, normalmente enfocados en las personas y como engañarlas.

El resumen y explicación de este bloque, es la fundación de un laboratorio de seguridad informática con materiales necesarios y adecuados, implementados con cualquiera de las tres propuestas principales y con acceso remoto, ofreciendo además una ventana para la investigación de distintas tecnologías.

Conociendo el objetivo general de este proyecto, a continuación, se expondrá los efectos concluyentes que podrán darse al llevarse a cabo con lo anterior plasmado. Como siempre, hay que tener en cuenta que siempre habrá alguna que otra excepción con relación a la perspectiva de cada alumno o de los conocimientos adquiridos por éste.

Una de las preguntas frecuentes que se realizan los individuos que estén atraídos por la seguridad informática son: ¿realmente se puede ser un hacker ético y qué necesito para empezar en este mundo? Aquí inicia el camino para empezar con los objetivos particulares ya que el saber diferenciar entre un hacker malicioso y uno ético, la cual, es la primera finalidad que se piensa tratar en este nuevo plan entre otros que se verán mostrados más adelante.

Si se trata el asunto de manera sistemática podemos llegar por medio de metodologías y pasos correspondientes, a enumerar las capacidades que el estudiante puede tener tomando los diferentes temas y por supuesto practicando en el laboratorio sugerido en este escrito.

Se dividirá en dos partes, los objetivos empíricos y los objetivos éticos. Los empíricos trataran la parte material que el interesado experimentará conforme tome las diferentes lecciones, y los éticos se referirán a la parte normativa que se aprenderá al tomar todos los adiestramientos:

- Conocimientos empíricos.
    - Metodologías usadas para realizar un pen-testing.
    - Recolección de información y reconocimiento.
        - Reconocimiento de objetivos.
        - Técnicas de enumeración pasiva.
        - Hacking con buscadores.
        - Uso de Inteligencias de Fuentes Abiertas (OSINT)
        - Extracción y análisis de metadatos
        - Técnicas de ingeniería social para recolección.
    - Enumeración.
        - Técnicas de enumeración activa.
        - Escaneo de puertos, servicios, SO.
        - Identificación de usuarios.
        - Escaneo de vulnerabilidades.
    - Análisis.
        - Modelado de infraestructura y objetivos.
        - Identificación de fallos conocidos.
        - Determinación de rutas rápidas para la obtención de objetivos.
    - Explotación y post-explotación.
        - Ataques a recursos y equipos de red.
        - Explotando fallos conocidos.
        - Fuerza bruta a servicios encontrados.
        - Ataques a aplicaciones web.

        - Ataques a aplicaciones Cliente/Servidor.
        - Ataques a implementaciones VoIP.
        - Ataques DDOS.
        - Técnicas para ataques de MITM.
        - Ataques a rede inalámbricas.
        - Ataques a controladores de dominio (DC).
        - Técnicas de ataques dirigidos a usuarios.
        - Consiguiendo y conservando el acceso.
        - Manejo de Shell.
        - Identificación de entorno.
        - Extracción de evidencias.
        - Escalado de privilegios.
        - Pivoteo.
        - Salto de contramedidas (firewalls, antivirus, IDS, IPS).
    - Documentación.
        - Envío de informe de fallos altamente críticos.
        - Generación de informes técnicos.
        - Generación de informes ejecutivos.
        - Presentación de resultados.
- Conocimientos éticos.
    - Conceptos básicos de hacking ético.
    - Verdades y mentiras sobre el hacking ético.
    - Toma de responsabilidades al realizar un pen-testing.
    - Toma de precauciones al realizar un pen-testing.

Metodología.

El complejo mundo de la seguridad informática presenta novedades día a día y requiere que el auditor o pen-tester se encuentre en constante crecimiento profesional. Los auditores de

seguridad suelen disponer de un kit de herramientas con las que realizar sus proyectos. (González Pérez, Sánchez Garcés, & Soriano de la Cámara, 2015)

Para alcanzar estos objetivos se necesita un temario o una guía para dar la ruta correspondiente y adecuada a las enseñanzas de estos temas y las reglas para el buen uso del laboratorio propuesto. En ellas también se tendrán las políticas de comportamiento y de advertencias en caso de no acatar las normas.

Se debe de crear una asignatura opcional que trate concretamente estos temas relacionados con la seguridad informática o el hacking ético con todos sus fines englobados tanto generales y particulares. Para ello el alumno debería saber los siguientes temas:

- Redes y sistemas de comunicaciones.
- Sistemas operativos de red: Windows Server y Linux Server.
- Conocimiento de términos respecto a TCP/IP.
- Manejo intermedio de comandos en Linux.
- Manejo de bases de datos.
- Conocimiento en el manejo de sistemas operativos cliente.
- Bases de programación.

Una vez teniendo estos requisitos previos el estudiante tiene la capacidad de poder resolver problemas de este ámbito y realizar sus tareas sin muchas dificultades durante la enseñanza. Anterior de ello se debe de tomar un assessment o re-evaluación para saber en qué nivel de conocimiento se encuentra el cursante y ver así si es apto o no llevar dicha asignatura y también para reforzar algunos conceptos que se solicitarán en el curso.

Durante las lecciones el participante demandará un laboratorio establecido; pero no sin antes tener un ambiente virtual temporal exclusivamente para las diferentes lecciones y prácticas. Ésto es posible con software que esté especializado en emular imágenes de routers, switches y a su vez contar con la característica de enlazar máquinas virtuales y demás dispositivos.

Cuando se terminen de tomar todo el programa se tendrá a disposición retos en las cuales se verá el verdadero desempeño y aprendizaje, éstos se reflejarán como puntajes extras además

de los ya obtenidos por las investigaciones que se habrán hecho durante el transcurso de la asignatura.

CAPÍTULO II Marco teórico.

Como un término amplio, la privacidad digital se refiere a cualquier información de identificación suministrada en línea cuando se realizan comunicaciones personales o de negocios a través de redes públicas. Últimamente, el debate sobre la privacidad digital se concentró en las preocupaciones en el manejo de los datos, tal como se ven desde dentro de estos servicios. Las revelaciones de los documentos de Edward Snowden sobre programas de vigilancia masiva alimentó los debates públicos sobre la importancia de legalizar las actividades de vigilancia y aumentó la conciencia pública sobre la importancia de proteger sus datos personales cuando se trabajan en línea. (Hassan & Hijazi, 2017)

Existen dos conceptos las cuales son la seguridad de la información y la seguridad informática. Concretamente, la seguridad de la información tiene como objetivo el evitar en los sistemas el acceso, uso, divulgación, interrupción o destrucción no autorizada de información y comprende diversos aspectos entre ellos la disponibilidad, comunicación, identificación de problemas, análisis de riesgos, la integridad, confidencialidad, y recuperación. Precisamente la reducción o eliminación de riesgos asociado a una cierta información es el objeto de la seguridad informática. (Reyes Krafft, y otros, 2016)

Los dos conceptos se parecen porque tienen un mismo fin; pero al mismo tiempo tienen diferencias sutiles, estas diferencias radican principalmente en el enfoque, las metodologías utilizadas, y las zonas de concentración ya que involucra la implementación de estrategias que cubran los procesos en donde la información es el activo primordial. Estas estrategias deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran. (Reyes Krafft, y otros, 2016)

Damos a entender y dar definición, en síntesis, que la seguridad de la información es un concepto que abarca varios tópicos entre ellos la seguridad informática y que cuenta con varios objetivos y que la seguridad informática es un medio para la detección y prevención de riesgos.

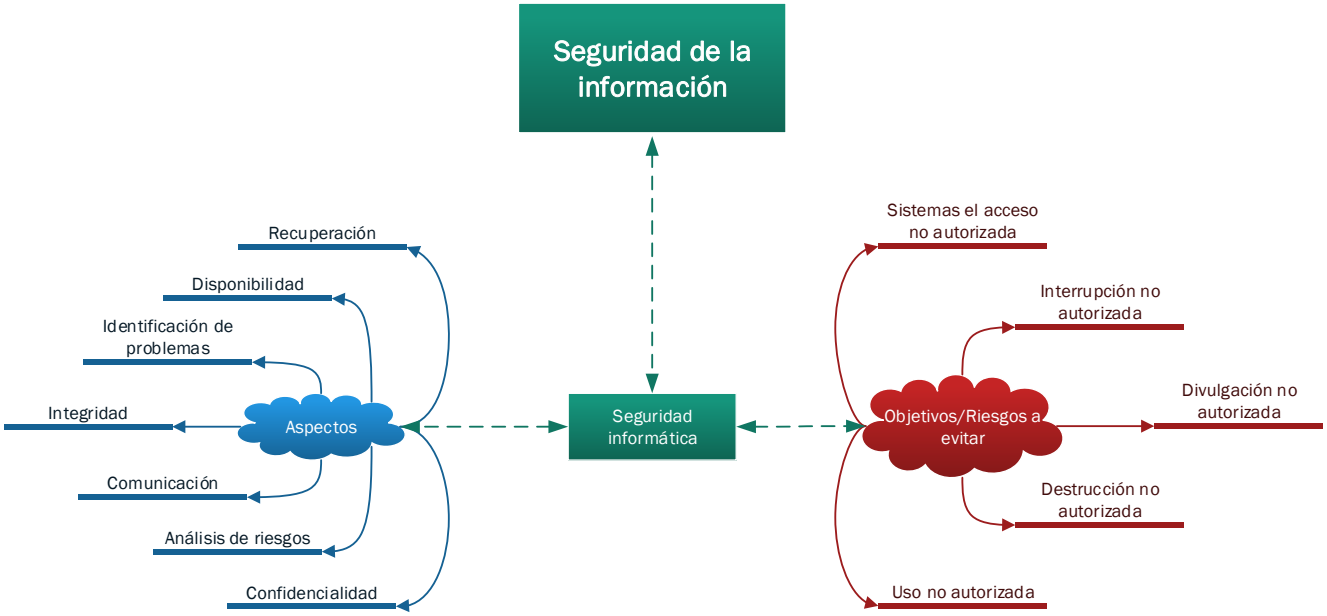

Figura 1. Esquema de relación de la seguridad de la información con la seguridad informática.

Hablando ahora de este medio que es la seguridad informática, se define por el conjunto de conceptos, componentes y mecanismos que toman sentido a través de muchas metodologías existentes hoy en día, se encarga de la protección de la información digital entre equipos informáticos y todo lo relacionado con la computación y la electrónica. Los mecanismos de seguridad detectan, previenen ataques y restauran los sistemas con éxito. Analizar la seguridad de un sistema requiere una comprensión de los mecanismos que hacen cumplir la política de seguridad. También requiere un conocimiento de los supuestos y la confianza relacionados, que conducen a las amenazas y el grado en que se pueden realizar. Estos conocimientos permiten diseñar mejores mecanismos y políticas para neutralizar estas amenazas. Este proceso conduce al análisis de riesgo. Los seres humanos son el eslabón más débil en los mecanismos de seguridad de cualquier sistema. Por lo tanto, las políticas y los procedimientos deben tomar en cuenta a la gente. (Bishop, 2005)

Los componentes básicos de la seguridad informática son la confidencialidad, la integridad y la disponibilidad. Las interpretaciones de estos aspectos están dictadas por las necesidades de los individuos, clientes y de las leyes de una particular organización, ya que varían por el contexto. (Bishop, 2005)

Componentes.

Confidencialidad: es la ocultación de información o recursos. La necesidad de mantener la información secreta surge del uso de computadoras en campos delicados o sensibles. Las instituciones militares y civiles del gobierno a menudo restringen el acceso a la información a quienes necesitan dicha información. Este principio también se aplica a las empresas industriales, que mantienen sus diseños de propiedad privada protegidos para que sus competidores no intenten robar los planos. Todos los tipos de instituciones mantienen registros de personal secretos y para poder tener los permisos necesarios se necesita de mecanismos de control de acceso. (Bishop, 2005)

Por ejemplo, Bob no quiere que Trudy sepa cuánto tiene en su cuenta de ahorros. El banco de Alicia también se enfrentará a problemas legales si no protege la confidencialidad de dicha información. (Stamp, 2011)

Integridad: se refiere a la fiabilidad de los datos o recursos, y por lo general se expresa en términos de prevención de cambios inadecuados o no autorizados. Ella incluye la integridad de los datos (el contenido de la información) y la integridad del origen (la fuente de los datos, a menudo llamada autenticación). La fuente de la información puede influir en su exactitud y en la confianza que las personas ponen en la información. Esta dicotomía ilustra el principio de que el aspecto de integridad conocido como credibilidad es fundamental para el correcto funcionamiento de un sistema. (Bishop, 2005) Los mecanismos de integridad que soportan este componente recaen en dos tipos: mecanismos de prevención y mecanismos de detección. (Stamp, 2011)

Por ejemplo, el Banco de Alicia debe proteger la integridad de la información de la cuenta para evitar que Trudy, por ejemplo, incremente el saldo de su cuenta o cambie el saldo de la cuenta de Bob. Tenga en cuenta que la confidencialidad y la integridad no son lo mismo. Por ejemplo, incluso si Trudy no puede leer los datos, podría ser capaz de modificar estos datos ilegibles, que, si no se detecta, destruiría su integridad. En este caso, Trudy podría no saber qué cambios había hecho en los datos (ya que no puede leerlo); pero puede que no le importe, a veces sólo con causar problemas es suficiente. (Stamp, 2011)

Trabajar con integridad es muy diferente de trabajar con confidencialidad. Con la confidencialidad, los datos pueden estar comprometidos o no; pero la integridad incluye tanto la corrección como la fiabilidad de los datos. El origen de los datos (cómo y de quién se obtuvo), qué tan bien se protegieron los datos antes de llegar a la máquina actual y qué tan bien los datos están protegidos en la máquina actual afectan a la integridad de los datos. Por lo tanto, evaluar la integridad a menudo y en teoría muy difícil, porque se basa en suposiciones sobre la fuente de los datos y sobre la confianza en esa fuente, dos fundamentos de seguridad que a menudo se pasan por alto. (Bishop, 2005)

Disponibilidad: se refiere a la capacidad de utilizar la información o el recurso deseado. La disponibilidad es un aspecto importante de la fiabilidad, así como del diseño del sistema porque un sistema no disponible es al menos tan malo como ningún sistema en absoluto. El aspecto de la disponibilidad que es relevante para la seguridad es que alguien puede deliberadamente denegar el acceso a los datos o a un servicio haciendo que no esté disponible. Los diseños de sistemas usualmente asumen un modelo estadístico para analizar los patrones de uso esperados, y los mecanismos aseguran disponibilidad cuando ese modelo estadístico se mantiene. (Bishop, 2005) Los mecanismos que apoyan la este componente son por lo general de alta disponibilidad.

Un ejemplo es cuando tanto para el banco de Alicia como para la web de Bob, si los sitios no están disponibles, entonces Alice no puede ganar dinero con las transacciones de los clientes y Bob no puede hacer su trabajo. Bob podría entonces tomar su negocio en otra parte. Si Trudy tiene un resentimiento contra Alice, o si sólo quiere ser malicioso, podría intentar un ataque de denegación de servicio en el Banco Online de Alicia. (Stamp, 2011)

Actualmente la denegación de servicio o los ataques DoS son un concepto y una preocupación relativamente reciente. Tales ataques intentan reducir el acceso a la información. Como resultado del aumento de los ataques DoS, la disponibilidad de datos se ha convertido en un tema fundamental en la seguridad de la información. (Stamp, 2011)

Mecanismos.

Los controles de acceso: sirven para dar entrada solo a personas, grupos, software o equipos autorizados por medio de métodos y tecnologías hacia ficheros, lugares de red, discos locales y equipos. (Bishop, 2005) Está basado en tres conceptos fundamentales: identificación, autenticación y autorización. (Stamp, 2011)

Mecanismos de prevención: mantienen la integridad de los datos bloqueando cualquier intento no autorizado de cambiar los datos o de cualquier intento de cambiar los datos de manera no autorizada. La distinción entre estos dos tipos de intentos es importante. La primera se produce cuando un usuario que no tiene autoridad, intenta cambiar los datos. La segunda ocurre cuando un usuario autorizado realiza ciertas modificaciones en los datos e intenta manipular los datos de otras maneras. Por ejemplo, supongamos que un sistema de contabilidad está en una computadora. Alguien entra en el sistema e intenta modificar los datos de contabilidad. Entonces, un usuario no autorizado ha tratado de violar la integridad de la base de datos de contabilidad. Pero si un contador contratado por la empresa para mantener sus libros trata de malversar el dinero enviándolo al extranjero y ocultando las transacciones, un usuario (el contador) ha intentado cambiar los datos (los datos contables) de manera no autorizada (moviéndola a una cuenta bancaria suiza). La autenticación adecuada con controles de acceso adecuados por lo general se detendrá el robo desde el exterior; pero la prevención del segundo tipo de intento requiere controles muy diferentes. (Bishop, 2005)

Mecanismos de detección: no intentan prevenir las violaciones de la integridad; simplemente informan que la integridad de los datos ya no es digna de confianza. Los mecanismos de detección pueden analizar eventos del sistema (acciones del usuario o del sistema) para detectar problemas o (más frecuentemente) analizar los propios datos para ver si las restricciones requeridas o esperadas aún se mantienen. Los mecanismos pueden reportar la causa real de la violación de integridad (una parte específica de un archivo fue alterada), o simplemente pueden reportar que el archivo está corrupto. (Bishop, 2005)

Mecanismos de alta disponibilidad: es la proporción de acceso a los datos, aplicaciones y lugares de red como servidores web, de archivos, base de datos etc., en caso de una interrupción

de los servicios que intente la denegación de la disponibilidad. Estos mecanismos permiten la compartición de recursos para proveer copias de seguridad, así mismo suministran por lo general la creación y gestión de varios sistemas y medios definidos dentro del entorno de alta disponibilidad. En síntesis, este mecanismo traen en si un concepto clave que es la resiliencia. (IBM, 2014)

Conceptos.

Identificación: es la capacidad de reconocer a usuarios, sistemas o aplicaciones de manera exclusiva para el correspondiente acceso. Es muy importante para las empresas, compañías, organizaciones etc., tener una administración de identidades y asegurarse de los diferentes niveles de acceso, las razones podrían ser varias, por ejemplo, el número de empleados y/o de dispositivos, la geografía de cada locación, o incluso los mismos niveles de autorización podrían llegar a estropear la aplicación de este concepto si no se tomas las medidas de gestión correspondientes, una solución serían las políticas de seguridad llevadas a nivel tecnológico como los directorios activos o los modelos LDAP. (Jain, 2013)

Existen distintas tecnologías que actualmente ofrecen medios a los distintos tipos de identificación, estas técnicas pueden ser de carácter de posesión que van desde el sistema básico de usuario-contraseña hasta los sistemas biométricos. En resumen, la identidad se clasifica en cuatro referentes: (Almehmadi & El-Khatib, 2015)

- Algo que se sabe (ej. Contraseña).
- Algo que se tiene (ej. Distintivos, toquen, tarjetas inteligentes, certificados).
- Donde se está (ej. Usando una terminal particular).
- Algo que se es (ej. Huellas digitales, ADN, iris).

Autenticación: nos sirve para asegurar que un usuario/sistema es auténtico o quien/que dice ser. Si no se autentica correctamente a los usuarios, es posible que los impostores se hagan pasar por usuarios legítimos y accedan a información confidencial, lo que provoca numerosos tipos de infracciones y aumenta los niveles de riesgo.

Si bien, los distintos medios que ayudan a identificar a los usuarios cumplen su función, también se debe de confirmar la misma identidad de dicha persona por medio de métodos complejos que se mencionaran a continuación; por lo tanto, a la autenticación se le conoce como la verificación de la identidad e igualmente se podría relacionar en un principio al concepto anterior; pero en sí la autenticación va más allá de una simple lectura de huellas digitales por decir un ejemplo.

Los métodos más reconocidos para efectuar este concepto son las firmas digitales asimétricas; los algoritmos de integridad como MD5 y SHA, de autenticidad como RSA, PSK y Diffie-Hellman y de confidencialidad como DES, 3DES y AES, éstos mismos son aplicados a las mismas firmas digitales conocidas actualmente como certificados, así mismo a protocolos tales como SSH, RADIUS, Kerberos, TKIP, EAP, CHAP, PAP, SSL-TLS, IPsec etc. La mayoría vienen implementados en dispositivos como los *firewalls*, *switches*, *routers*, AP etc.; a tecnologías como las VPN, bases de datos, Wireless etc., y hacia otros protocolos como HTTP, SMTP, TCP/IP, RDP, FTP etc.

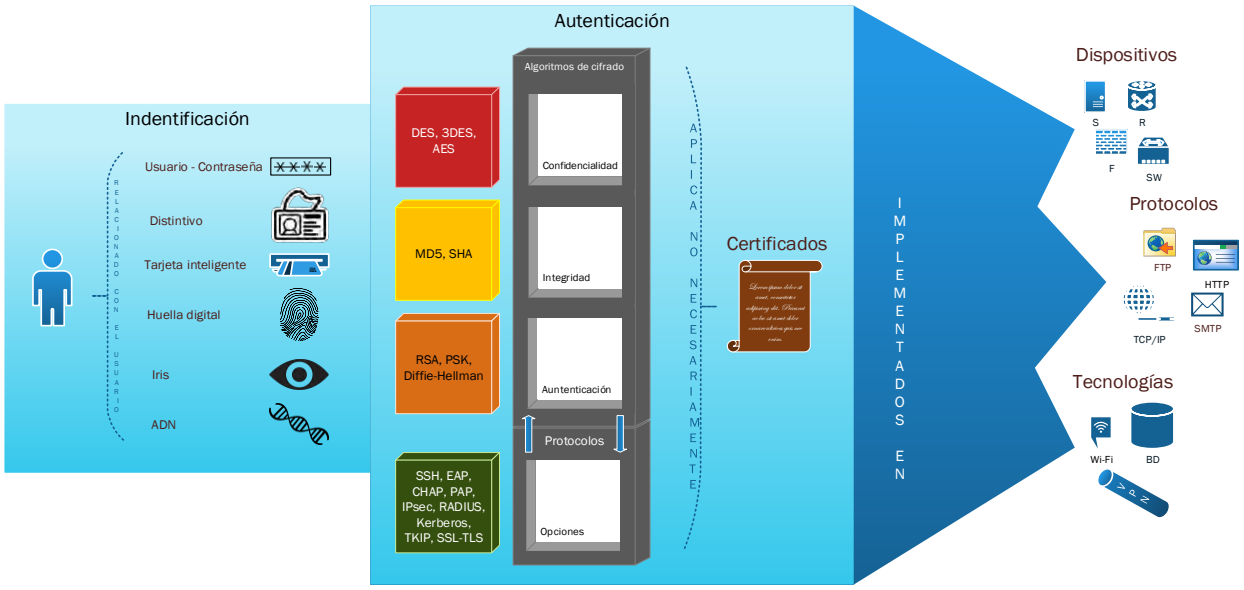

Figura 2. Identificación y autenticación.

Autorización: es la parte del control de acceso relacionada con las restricciones en las acciones de los usuarios autenticados. La autorización es un aspecto del control de acceso y la autenticación es otra. En su forma más básica, la autorización se refiere a la situación en la que

ya hemos autenticado por ejemplo a Alicia y queremos aplicar restricciones sobre lo que tiene permitido hacer. Tenga en cuenta que, aunque la autenticación es binaria (ya sea que un usuario esté autenticado o no), la autorización puede ser un proceso mucho más detallado. (Stamp, 2011)

Los Modelos de Seguridad Multinivel (MLS por sus siglas en inglés) que en general son descriptivos; pero no restrictivos. Es decir, estos modelos nos dicen qué debe protegerse, mas no responden a la pregunta real, es decir, a cómo proporcionar dicha protección. Esto no es un defecto en los modelos, ya que están diseñados para establecer un marco de protección; sin embargo, es una limitación inherente a la utilidad práctica del modelado de seguridad. Como ejemplo, el Departamento de Defensa de los Estados Unidos de América mejor conocido por U.S. DoD, emplea cuatro niveles de clasificaciones y autorizaciones, que se ordenan de la siguiente manera: (Stamp, 2011)

TOP SECRET> SECRETO> CONFIDENCIAL> DESCLASIFICADO

Se necesita de seguridad multinivel cuando sujetos y objetos en diferentes niveles usan los mismos recursos del sistema. El propósito de un sistema MLS es imponer una forma de control de acceso restringiendo a los sujetos para que solo accedan a los objetos para los que tienen la autorización necesaria. También hay interés en MLS en aplicaciones tales como firewalls de red. El objetivo en estos casos es mantener a un intruso, en un nivel bajo para limitar el daño que puede infligir después de que haya violado el *firewall*. (Stamp, 2011)

Actualmente existen muchos modelos de seguridad multinivel, cada uno tiene su complejidad; los más elementales son: (Stamp, 2011)

- Modelo Ben-LaPuda.
- Modelo Bilba.
- Modelo por compartimientos.
- Modelo por canal oculto.

Una de las brechas de seguridad es la inferencia de datos, esta amenaza se trata de minar datos mediante el análisis con el propósito de obtener ilegítimamente conocimientos sobre una base de datos. Una de las contramedidas que se pueden llevar a cabo es un control de inferencia, el cual

es un intento de evadir la “vista” completa a los usuarios de bajo nivel colocando trozos de información no relevantes.

Los CAPTCHA están diseñados para evitar que las máquinas accedan a los recursos, un CAPTCHA también se puede ver como una forma de control de acceso. Según el folclore, la motivación original para CAPTCHAs fue una encuesta en línea que pedía a los usuarios que votaran por la mejor escuela de postgrado en ciencias de la computación. En esta versión de la realidad, rápidamente se volvió obvio que las respuestas automáticas de MIT y Carnegie-Mellon estaban desviando los resultados y los investigadores desarrollaron la idea de un CAPTCHA para evitar que los "*bots*" automatizados llenaran las urnas. Hoy, los CAPTCHA se utilizan en una amplia variedad de aplicaciones. Por ejemplo, los servicios de correo electrónico gratuitos usan CAPTCHA para evitar que los remitentes de correo no deseado se registren automáticamente en un gran número de cuentas de correo electrónico. (Stamp, 2011)

Además, están los tipos de control de autorización son las aplicaciones o dispositivos como los firewalls ya que examinan las solicitudes de acceso a su red y deciden si pasan ciertas pruebas o reglas. Si es así, se les permite y, si no, se rechazan. Por lo general se adoptan y se clasifican en tres tipos de cortafuegos: (Stamp, 2011)

- Firewall por filtro de paquetes.
- Firewall por filtro de paquete con estado.
- Firewall por aplicación proxy.

Resiliencia: consiste en la capacidad de proveer y mantener un funcionamiento aceptable a pesar de fallas y desafíos a la operación normal, por ejemplo: sobrecargas de trabajo, tráfico malicioso, etcétera. (Polanco, 2013)

A continuación, se mencionarán algunas consideraciones a tomar en cuenta cuando una organización decide comenzar con una iniciativa para evaluar la resiliencia de su infraestructura: (Polanco, 2013)

- Definir un plan de pruebas que contemple los diferentes escenarios a los que la infraestructura está o pudiese estar expuesta.

- Contemplar la inyección de tráfico válido que refleje el comportamiento típico de las aplicaciones y de los usuarios, e inválido que incluya ataques DDoS, exploits, paquetes malformados, etcétera.
- Realizar pruebas periódicas para la definición de líneas base.
- Efectuar pruebas de seguridad y rendimiento después de cambios mayores a la infraestructura.
- Utilizar tecnologías avanzadas para automatizar este tipo de pruebas. Hoy en día ya existen herramientas avanzadas que permiten, entre otras cosas.
    - Definir escenarios tan complejos como se requiera, simulando aplicaciones comerciales y los protocolos más comunes.
    - Simular ataques que incluyen malware, DDoS, malware móvil, etcétera.
    - Simular millones de usuarios simultáneos.
    - Evaluar la capacidad de un dispositivo de manejar múltiples sesiones TCP concurrentes.
    - Realizar pruebas mezclando tráfico válido e inválido al mismo tiempo.
    - Alcanzar anchos de banda superiores a los 100 Gbps.
    - Capturar y recrear flujos de tráfico

En resumen, dada la mayor dependencia existente día con día en las tecnologías de la información, resulta indispensable conocer y evaluar permanentemente la resiliencia de los componentes de seguridad y de TI.

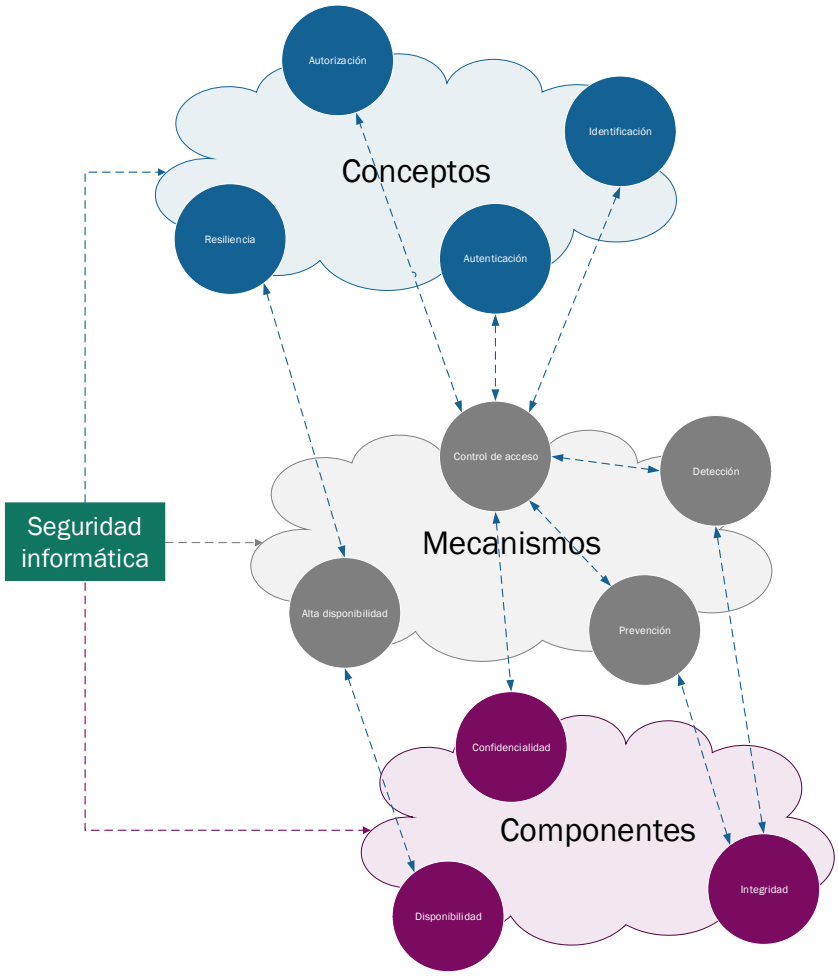

Figura 3. Relación entre componentes, mecanismos y conceptos en la seguridad informática.

Tecnologías y herramientas.

Para la gran mayoría de las pruebas que se harán con el laboratorio de seguridad propuesta, se necesitan de muchas herramientas y/o tecnologías que puedan cubrir lo suficiente las necesidades del investigador o del estudiante. La mayoría de ellas son complejas, pero gracias al avance de la informática nos han hecho más fácil la interacción entre los componentes, mecanismos y conceptos previamente descritos.

Podría parecer que en esta sección no tenga nada que ver con la seguridad informática, pero para poder tener una perspectiva y ambiente más llevado a la realidad se necesita de muchos intermedios. De esta manera, si uno quiere experimentar, por ejemplo, con paquetes

fragmentados a través de un cortafuego o un IDS, se necesita de un intermedio que sería el mismo cortafuego o IDS.

Por lo general todo aquel que esté desde una red local hasta la internet, estaremos siempre conectados por dispositivos intermedios para tener comunicación. Por lo tanto, los ataques realizados de manera remota siempre pasarán por enrutadores, conmutadores, firewalls etc.

Virtualización.

Mucho se sabe que, para experimentar con cierto tipo de ambientes, se requieren incontables veces de distintos tipos de sistemas operativos y/o arquitecturas, por lo tanto, se necesita de una solución que permita las diferentes pruebas sin afectar el sistema base que un usuario por lo general opera. La manera más cómoda, segura y económica de realizarlo es por medio de las máquinas virtuales.

La virtualización es una herramienta para el aislamiento, es la emulación de una computadora en la memoria de un sistema host. En una computadora virtual, se puede crear y destruir a voluntad. Hay muchos usos para las máquinas virtuales porque son más fáciles de administrar que una máquina real, especialmente cuando se implementan de tal forma que pueden migrar de máquina física a máquina física. (Waschke, How Does Computer Security Work?, 2017)

Probar un nuevo sistema operativo puede ser un problema. Si instala el sistema operativo directamente en una computadora, debe tomarse la molestia de restaurar desde una copia de seguridad si desea volver a su sistema anterior. Una VM soluciona ese problema. Cree una VM, instale el nuevo sistema operativo y experimente con él. Si decide que no le gusta el sistema operativo, apague la VM; el sistema operativo se ha ido, y su SO anfitrión no ha cambiado. (Waschke, How Does Computer Security Work?, 2017)

Una máquina virtual se puede configurar para utilizar la memoria en lugar de un disco duro para el almacenamiento. Cuando la máquina virtual se apaga, todo lo que ha escrito desaparece. Cada registro local de la actividad de los invitados se ha ido. Si se ha infectado con malware, la infección desaparecerá. Si le preocupa la privacidad, no hay registro. Alternativamente, se puede crear una

instantánea que haya tomado de una máquina en el estado que desea reproducir y tener un duplicado de la máquina. (Waschke, How Does Computer Security Work?, 2017)

Un investigador puede con seguridad probar diferentes tipos de ataque, así mismo, infectar deliberadamente con malware y tomarlos como objeto de estudios e incluso modificarlos a modo. De esta manera, se evita la propagación y los accidentes de seguridad dentro del entorno real. Los programas de virtualización más utilizados son:

- VMware®.
- Oracle VM VirtualBox.
- QEMU.
- Microsoft Hyper-V™.
- Dynamips.

Emuladores de red.

Dentro de estos tipos de herramientas se encuentran relacionados los emuladores de red las cuales permiten diseñar fácilmente topologías y luego ejecutarlas en él. A diferencia de lo simuladores, en éstos no son posibles integrar aplicaciones y/o appliances que en el argot informático anglosajón se refiere a dispositivos virtuales, por decir un ejemplo, pero no por ello son inútiles para el aprendizaje. Por consiguiente, las ventajas a favor de los emuladores de red frente a los simuladores, son las siguientes.

- Soporte y virtualización real de imágenes de dispositivos de red.
- Integración con máquinas virtuales.
- Integración de herramientas de análisis de red.
- Experiencia de ambiente más realista.
- Soporte adicional de protocolos de red.

Sus desventajas:

- Consumo de recursos computacionales.
- Pueden llegar a ser propiedad de marcas registradas; por lo tanto, de paga.
- Dificultad o imposibilidad para integrar tecnologías inalámbricas.

Hoy en día existen muchas herramientas de emulación de red como NetSim, IMUMES, Cloonix, Netkit, EVE-NG (que es un fork de UNetLab) etc., pero específicamente hay dos muy conocidas de manera comercial y popular. Éstas son: GNS3 y Cisco VIRL, cada una tiene sus pros y sus contras dependiendo de las necesidades del usuario. Para exponer y resumir más claramente, la siguiente tabla muestra la comparación entre ellas. (Bombal & Duponchelle, Getting Started with GNS3, 2018) y (The Cisco Learning Network Store, 2018)

	
Software de código abierto; por lo tanto, está disponible públicamente.	Software propietario de Cisco Systems®; por lo tanto, es de pago ($199 USD anuales).
Captura de paquetes y análisis de red con herramientas externas.	Visualización de protocolos, captura de paquetes y análisis de red con herramientas externas.
Integración y compatibilidad de diferentes tipos de appliances de otras arquitecturas.	Integración y admisión única de imágenes virtuales de Cisco Systems®.
Soporte de más de cien nodos disponibles.	Soporte de hasta veinte nodos disponibles.
Integración de máquinas virtuales externas.	No soporta integración de máquinas virtuales externas.
Admite hipervisores gratuitos y de pago (Oracle VM VirtualBox, VMware Workstation Pro, Player, ESXi, Fusion).	Disponible únicamente para su uso en VMware® y versiones como Workstation Pro, Player, ESXi, Fusion.
Soporte básico para routing & switching.[1,2,3]	Soporte avanzado para routing & switching.

Tabla 1. Comparación entre GNS3 y VIRL.

Alcances de GNS3.

[1] Originalmente GNS3 sin integraciones IOSv y también sin tomar en cuenta las demás arquitecturas de otros fabricantes como Juniper, Alcatel, Fortinet, Cumulus etc., este software emulador solo funciona con las implementaciones más básicas y built-in para realizar routing y switching.

Para trabajar con los binarios, se necesita de la autorización necesaria por parte de Cisco Systems® para primeramente poder obtenerlos ya sea por ser estudiante integrado en la academia, copiarlos directamente del dispositivo o ser proveedor delegado, tomando en cuenta que no todas las imágenes disponibles en el mercado están soportadas por este software emulador, pero son suficientes para tener un buen ambiente de laboratorio inicial. La siguiente lista expone los modelos y sus imágenes soportados por GNS3: (Duponchelle, Cisco IOS images for Dynamips, 2017)

- Modelos.
    - c1700 series.
        - c1700-adventerprisek9-mz.124-25d.bin (Principal).
        - c1700-adventerprisek9-mz.124-15.T14.bin (Implementación).
    - c2600 series.
        - c2600-adventerprisek9-mz.124-25d.bin (Principal).
        - c2600-adventerprisek9-mz.124-15.T14.bin (Implementación).
    - c3620.
        - c3620-a3jk8s-mz.122-26c.bin (Principal).
    - c3640.
        - c3640-a3js-mz.124-25d.bin (Principal).
    - c3660.
        - c3660-a3jk9s-mz.124-25d.bin (Principal).
        - c3660-a3jk9s-mz.124-15.T14.bin (Implementación).
    - c2691.
        - c2691-adventerprisek9-mz.124-25d.bin (Principal).

    - c2691-adventerprisek9-mz.124-15.T14.bin (Implementación).
- c3725.
    - c3725-adventerprisek9-mz.124-25d.bin (Principal).
    - c3725-adventerprisek9-mz.124-15.T14.bin (Implementación).
- c3745.
    - c3745-adventerprisek9-mz.124-25d.bin (Principal).
    - c3745-adventerprisek9-mz.124-15.T14.bin (Implementación).
- c7200 series.
    - c7200-adventerprisek9-mz.152-4.M7.bin (Mantenimiento).
    - c7200-a3jk9s-mz.124-25g.bin (Principal).
    - c7200-adventerprisek9-mz.124-24.T5.bin (Implementación).

El motivo principal de este número limitante de imágenes de Cisco es porque el motor de virtualización que integra GNS3 actualmente como dependencia por defecto, solo soporta esos modelos de dispositivos de red. Dicho motor que es capaz de virtualizarlos es dynamips, que originalmente y de manera independiente puede montar las imágenes en un servidor local por medio de una línea de comandos y sin una GUI, pero con GNS3 todo ese proceso es automatizado. (Grossmann & Saraiva, 2016)

[2] Cabe también remarcar que éstos son solo modelos de routers ya que para tener una experiencia más realista (pero no completa) para switching se necesita originalmente de una integración IOU (IOS sobre Unix) de capa dos y de igual forma, solo se pueden obtener siendo estudiante registrado en Cisco Systems® o siendo proveedor designado y teniendo un archivo-licencia para la operación de estas imágenes. Otra forma para experimentar en particular con este modo es probando con los módulos de etherswitch directamente de los modelos de enrutadores anteriormente mencionados, pero únicamente con las series de modelos: 2600s, 3600s y 3700s. (Duponchelle, Cisco IOS images for Dynamips, 2017)

¿Qué diferencias hay entre cada una de estas implementaciones básicas para switching y routing? Los binarios IOU son utilizados en laboratorios para implementar prácticas y posibles diseños, remarcando que estas imágenes no son oficialmente lanzadas al público por Cisco. Se ejecuta

bajo plataformas basadas en Unix: Solaris o Linux, por ejemplo. En este caso, GNS3 usa su complemento adicional para poder correr los archivos, este complemento se llama GNS3 VM la cual es una máquina virtual con núcleo Linux y basada en la distribución Ubuntu para poder reproducir de manera correcta los ficheros IOU. A diferencia, los módulos etherswitch así como los built-in instalados por defecto, no necesitan del complemento adicional ya que se pueden montar a través del servidor local de dynamips automatizado por GNS3, usando así los recursos computacionales directos. En cuestiones de funcionalidad, la siguiente lista nos muestra las diferentes capacidades **no** soportadas por dichas integraciones: (Bombal, Switching and GNS3, 2017)

- Módulos etherswitch. (Duponchelle, Cisco IOS images for Dynamips, 2017)
    - Acceso al template para Switch Device Manager (SDM).
    - ACL – Mejoramiento de algoritmo de merging.
    - Balanceo de carga para Multicast EtherChannel.
    - Balanceo de cargas para VLAN Flex Link.
    - BGP – Incremento de la compatibilidad de las listas de acceso as-path numeradas a 500.
    - BGP – Reinicialización de la sesión de vecinos después del max-prefix límite alcanzado.
    - Contadores DHCP Snooping.
    - Control de tormenta de paquetes.
    - Convergencia rápida bidireccional de Flex Link.
    - Detección de enlace unidireccional (UDLD).
    - DHCP Snooping.
    - Enrutamiento y conmutación de máquinas virtuales de proveedores.
    - ErrDisable timeout.
    - EtherCannel Guard.
    - EtherChannel – PAgP flexible.
    - Fallback Bridging.
    - Filtrado de MAC Unicast.

- Flex Links Interface Preemption.
- GOLD – Diagnósticos genéricos *online*.
- IEEE 802.1ab – Protocolo de descubrimiento de capa de enlace.
- IEEE 802.1q – ISL.
- IEEE 802.1s – VLAN Multiple Spanning Tree.
- IEEE 802.1s – Cumplimiento de estándares para Multiple Spanning Tree (MST).
- IEEE 802.1t.
- IEEE 802.1w – reconfiguración rápida de Spanning Tree.
- IEEE 802.1x – Auth Fail Open.
- IEEE 802.1x – Auth Fail VLAN.
- IEEE 802.1x – con Port Security.
- IEEE 802.1x – RADIUS Accounting.
- IEEE 802.1x – Soporte de Wake on LAN.
- IEEE 802.1x – VLAN Assignment.
- IEEE 802.1x – Autenticación multi-dominio.
- IEEE 802.3ad – Link Aggregation (LACP).
- IEEE 802.3af – Power over Ethernet.
- IGMP Fast Leave.
- IGMP Version 1.
- IGRP.
- IPSG (IP Source Guard).
- Jumbo Frames.
- L2PT – Protocolo de tunneling de capa 2.
- Límite de confianza (confianza extendida para dispositivos CDP).
- Limpieza de contadores por puerto.
- Lista de control de acceso de VLAN (VACL).
- MAC Bypass de autenticación.
- Mejoramiento de detección de teléfonos IP.
- Mensajes de syslog de STP.

- MLD Snooping.
- NAC – L2 IEEE 802.1x.
- NAC – L2 IP con Auth Fail Open.
- NAC – L2 IP.
- Opciones de diagnóstico en el arranque.
- Optimización ARP.
- Port Security en puertos de VLAN privadas.
- Port Security.
- Propagación de políticas de QoS a través del protocolo Border Gateway (QPPB).
- Rapid-Per-VLAN-Spanning Tree (Rapid-PVST).
- Reactivación de ErrDisable por puerto.
- Smart Port.
- Soporte para la política de outbund para BGP Route-Map Continue.
- SPAN remoto (RSPAN).
- Spanning Tree Protocol (STP) – Balanceo de cargas Uplink.
- Spanning Tree Protocol (STP) – Filtrado PortFast BPDU.
- Spanning Tree Protocol (STP) – Loop Guard.
- Spanning Tree Protocol (STP) – Portfast compatible para troncales.
- Spanning Tree Protocol (STP) – Root Guard.
- SRR (Shaped Round Robin).
- Supervisor en stanby para uso de puertos.
- Switching Database Manager (SDM).
- Teléfono IP mejorado – PHY detección de loop.
- Trunk Failover.
- Uso reducido de la dirección MAC.
- Vigilancia Per Port Per VLAN.
- VLAN Aware Port Security.
- VLAN’s privadas.
- Weighted Tail Drop (WTD).

- IOU. (Ciobanu, 2015)
    - 802.1q Tunneling.
    - Autenticación NTP.
    - DHCP Snooping.
    - ERSPAN.
    - HSRP las direcciones no hacen *ping*.
    - Inter-VLAN.
    - L2 PortChannel (no funciona en versiones 12.2, funciona en versiones 15.0).
    - L3 PortChannel.
    - Multicast con BSR.
    - NVI NAT (NAT clásico funciona solamente en imágenes TPGEN).
    - PPPoE (solo funciona en versiones 12.4, y 15.2(2.3) T).
    - QinQ.
    - Routing loops (IOL hace crash).
    - RSPAN.
    - SPAN.
    - Troncales Cisco ISL.
    - VLAN Privadas.
    - VTP versión 2 (VTP versión 1 funciona).

Alcances de IOSv y VIRL.

En contraste con lo demás expuesto, los archivos IOSv son pequeñas imágenes virtualizadas capaces de simular las características completas de un conmutador, enrutador y hasta de un appliance de seguridad avanzada ASA. Pero existe un detalle especial hacia la emulación de switches ya que recordemos que estos dispositivos trabajan con la capa de enlace de datos del modelo OSI e incluso con la capa de red y usa servicios de la capa física, por lo tanto, se emplea mucho de la parte tangible, es decir, del *hardware*. Esto resulta complicado tratar de emular y operar con solo una imagen de extensión ".bin" como lo vimos anteriormente y se necesita de algo más, ese "algo más" son los IOSv.

Lo que hace especial a este formato es que se trata de código de software de Cisco IOS utilizado en enrutadores y conmutadores compilados para ejecutarse en un hipervisor, es decir, tanto la parte física y lógica están agrupadas en un solo archivo listo para ser ejecutados en un software de virtualización, en este caso utilizando el complemento de GNS3 (GNS3 VM) y a la vez usando un motor de traductor binario llamado QEMU. Al igual que los IOU y de los binarios IOS, el alcance para el uso de estos archivos también está limitado solo a personal autorizado, pero, para tener ese privilegio en especial para los IOSv, se tiene que realizar un pago anual de $199 dólares estadounidenses para uso personal, como se mencionaba en la tabla antepuesta. (The Cisco Learning Network Store, 2018)

VIRL tiene a su disposición ocho tipos de appliances ya compilados y listos para su configuración en la CLI, y cada una tiene las siguientes capacidades cien por ciento soportadas por cada protocolo, servicio y tecnologías: (The Cisco Learning Network Store, 2016)

1. **IOSv**: proporciona un plano de control de capa tres completo y la funcionalidad de datos en plano. No soporta capa dos.
   Lista de capacidades soportadas:
   802.1Q, AAA, ACL, BGP, DHCP, DNS, EEM, EIGRP, EoMPLS, Flex Netflow + TNF, GRE, ICMP, IGMP, IP SLA, IPSec, IPv6, ISIS, L2TPv3, MPLS, MPLS L2VPN, MPLS L3VPN, MPLS TE, Multicast, NAT, NTP, OSPF, PfR, PIM, PPPoE, RADIUS, RIP, SNMP, SSH, SYSLOG, TACACS, TFTP, VRF-LITE, HSRP, VRRP, GLBP, EZVPN, QoS, LISP, ZBFW, Performance Monitor.
2. **IOSvL2**: es principalmente un conmutador de nivel dos con el plano de control y la funcionalidad de datos en plano de capa tres también que están presentes en la imagen.
   Lista de capacidades soportadas:
   Forwarding L2, switchport, 802.1q trunking, 802.1q VLAN's, Spanning Tree, Port-Channel (Pagp y Lacp), 802.1x Passthrough, Port-ACL's, inspección ARP dinámica, DHCP Snooping, IP device tracking, Switched Virtual Interfaces, forwarding sobre SVIs de L3, soporte para protocolos de enrutamiento, VTP v1-3, PVST, RPVST, QoS, enrutamiento Inter-VLAN, VLAN Access Maps (VACL's / lista de control de acceso para VLAN's),

funcionalidad ACL para paquetes de protocolo de L2 y L3, soporte para DTP, modo switchport protegido.

3. **IOS-XVRv**: es una máquina virtual que admite la virtualización completa (es decir, sin personalizaciones específicas de hipervisor) y, como tal, está generalizada para ejecutarse en cualquier hardware de cómputo x86 (servidor o computadora portátil) que ejecute hipervisores estándar.

   Esta plataforma de software proporciona el conjunto de funciones del software IOS XR que incluye: la administración XR, plano de control, enrutamiento y forwarding.

   IOS XRv no intenta proporcionar una representación virtual de ningún enrutador físico en particular, sino que es una representación del software y del sistema operativo IOS XR, y como tal, no presenta algunos componentes que cabría esperar en sistemas físicos como las line-cards, multi-chasis, que no son apropiados para la entrega de VM que proporciona IOS XRv.

   Lista de capacidades soportadas:

   IPv4, IPv6, BGP, MP-BGP, EIGRP, ICMP, OSPF, NTP, TFTP, MPLS, MPLS L3VPN, MPLS TE, ISIS, mVPN GRE / mLDP / P2MP TE, AAA, RADIUS, TACACS, SNMP, FLEX CLI, Multicast (PIM, MSDP, IPv6), syslog, VLAN's / QinQ (.1Q, .1AD), RPL, ACL's, SSH, VRF-LITE.

4. **NX-OSv**: es una plataforma de referencia para una implementación del sistema operativo Cisco Nexus, basado en las plataformas de la serie Nexus 7000, ejecutándose como una máquina virtual completa en un hipervisor.

   Proporciona funcionalidad de planos de control y datos planos parcial en capa tres. No admite capa dos.

   Lista de capacidades soportadas:

   802.1x, AAA, AMT, BGP, CDP/LLDP, EIGRP, FHRP-HSRP, GLBP, VRRP, ICMP, IGMP, IPv4, IPv4/6, IPv6, ISIS, protocolos de enrutamiento L3, LDAP, LISP, MLD, MSDP, NTP, OSPF, PIM/PIM6, Radius, RIP, SNMP, syslog, TACACS+, VRF, XML/Netconf, NX-API.

5. **CSR1000v**: es un enrutador de factoría virtual que ofrece funciones integrales de puerta de enlace WAN y servicios de red en entornos virtuales y en la nube. Permite a las empresas extender de manera transparente sus WAN en nubes alojadas.
   Lista de capacidades soportadas:
   802.1Q, AAA, ACL, BGP, DHCP, DNS, EEM, EIGRP, EoMPLS, Flex Netflow + TNF, GRE, ICMP, IGMP, IP SLA, IPSec, IPv6, ISIS, L2TPv3, MPLS, MPLS L2VPN, MPLS L3VPN, MPLS TE, Multicast, NAT, NTP, OSPF, PfR, PIM, PPPoE, RADIUS, RIP, SNMP, SSH, SYSLOG, TACACS, TFTP, VRF-LITE, HSRP, VRRP, GLBP, EZVPN, QoS, LISP, ZBFW, Performance Monitor.
6. **ASAv**: brinda funcionalidad completa de firewall a los entornos virtualizados para asegurar el tráfico del centro de datos y los entornos multi-tenant. (Cisco Systems, 2017)
   En este caso particular, VIRL en sí, solo admite tres tipos de ASAv las cuales son los ASAv5, ASAv10 y ASAv30 por cuestiones de recursos computacionales. (Cisco Systems, 2017) Aun así, los tres tienen capacidades de soporte en común. La siguiente tabla nos muestra de nueva cuenta cuáles son esas características y cuáles son sus variaciones. (Cisco Systems, 2017)

Capacidades	ASAv5	ASAv10	ASAv30
Inspección del *throughput* con estado (máximo).	100 Mbps	1 Gbps	2 Gbps
Inspección del *throughput* con estado (multiprotocolo)	50 Mbps	500 Mbps	1 Gbps
Estándar Avanzado de Cifrado (AES) con VPN *throughput*.	30 Mbps	125 Mbps	1 Gbps
VLAN’s	25	50	200
Grupos *bridge*.	12	25	100
Pares IPSec VPN	50	250	750

Modos	Enrutamiento y transparente.

Tabla 2. Capacidades comunes generales entre modelos ASA.

7. **NX-OS 9000v**: es una plataforma virtual que está diseñada para simular los aspectos del plano de control de un elemento de red que ejecuta el software Cisco Nexus 9000. El NX-OSv 9000 comparte la misma imagen de software que se ejecuta en la plataforma de hardware Cisco Nexus 9000, aunque no se implementa ninguna emulación de hardware específica. Cuando el software se ejecuta como una máquina virtual, el aprovisionamiento ASIC de la líne-card (LC) o cualquier interacción desde el plano de control al hardware del ASIC, se maneja mediante el plano de datos del software NX-OSv 9000.
   Lista de capacidades soportadas:
   CDP, LLDP, BGPv4, BGPv6, OSPFv2, OSPFv3, RIP, EIGRP, Switching Unicast L2, Switching Broadcast L2, Switching Multicast L2, aprendizaje MAC, Static/Router MAC, Switchport, 802.1q trunking, 802.1q access, STP, SVI L3, subinterfaces, VXLAN, vPC, Port-Channel. (Cisco Systems, 2018)
8. **IOS XRv 9000**: implementa el conjunto de características del software Cisco IOS XR. Funcionando en plataformas informáticas generales x86 virtualizadas, complementa las plataformas de enrutadores físicos Cisco® existentes que confían en el software IOS XR de Cisco, como los enrutadores del sistema de convergencia de red de Cisco, los enrutadores de la serie Cisco ASR 9000 y las plataformas del sistema de enrutamiento de Cisco (CRS).
   Lista de capacidades soportadas:
   NVF (vPE y vRR), BGP, OSPF, ISIS, MPLS, LDP, rutas estáticas, IEEE802.1q VLAN, IEEE802.1ad QinQ, SMU, BFD, BGP-PIC, H-QoS, ACL, uRPF, Lawful Intercept. (Cisco Systems, 2015)

Las demás imágenes virtuales son implementaciones como servidores de aplicación, nubes, módulos built-in y clústeres que también están compilados como las imágenes principales, con sus versiones más recientes para que de esta manera se competen los vente nodos disponibles.

[3] En síntesis, vemos claramente que VIRL como hipervisor, está más orientado al uso de los productos de su misma línea, lo cual, ofrece en ese aspecto una ligera ventaja frente a GNS3, ya que si un investigador desea sacarles mayor provecho a las tecnologías de Cisco Systems®, éste sería su mejor opción, al igual que si un alguien quiera prepararse para las diferentes certificaciones sería un complemento ideal para su objetivo. De este modo el soporte básico para conmutación y enrutamiento como comparación entre GNS3 y VIRL se anularía ya que éste los integra a la perfección.

¿Cómo funciona GNS3?

Cambiando de perspectiva y encaminándonos en el laboratorio propuesto en la introducción, primeramente, se tuvo en mente que en entornos reales no todos los dispositivos de red y de seguridad serán de una determinada marca o fabricante, así que, si vemos por ese lado, la mejor elección seria GNS3 ya que maneja muchas integraciones de distintos fabricantes tales como Juniper, Fortinet, Cumulus, Alcatel, pfSense etc., incluidos también los IOSv de VIRL, esto hace que este emulador sea más versátil al momento de crear entornos de laboratorio.

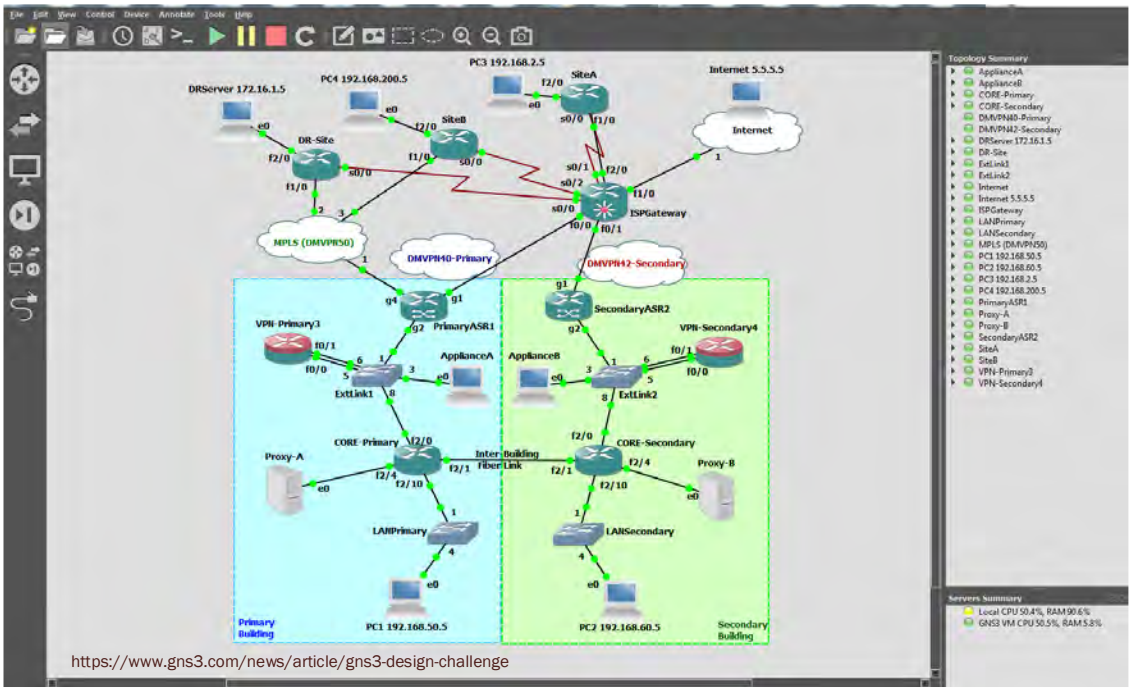

Figura 4. Ejemplo de una topología en GNS3.

Enfocándonos ahora en este emulador previamente electo, su funcionalidad es algo compleja, pero a pesar de ello, es fácil de usar y configurar. Por defecto GNS3 trabaja con el emulador dynagen/dynamips como medio para correr los binarios de Cisco IOS, este motor trabaja de manera inicial como un servidor local (dynamips server) en el cual sirve para cargar el IOS del modelo admitido en cuestión, luego existe dentro de la misma herramienta un motor para la conexión y el listado de las tarjetas de red de algún enrutador que esté en dicha topología. Para la carga de los binarios se necesita de un archivo en el que se especifique la configuración requerida para inicializar los archivos por medio de dynagen, entre las estas configuraciones, las principales que suplen suficientemente para poder operar con ellas son:

- Ruta de instalación de binario IOS.
- Nombre de host y cantidad.
- Valor Idle-PC, permite el uso eficiente del CPU, es único y debe ser calculado para cada equipo.
- Número de modelo soportado.
- Número e identificadores de interfaces.
- Conexión entre interfaces de red de vecino a vecino.

De estos puntos, la más importante es el Idle-PC, ya que sin ello dynamips intenta emular las instrucciones una a la vez lo más rápido posible, consumiendo hasta el 100% del CPU disponible. Para entender esto, veamos lo siguiente.

```
autostart = false
[localhost]
   [[3745]]
          image = C:\Program Files\Dynamips\images\c3745-
advipservicesk9-mz.123-24.bin
          idlepc = 0x60d7368c
#################################################################
###########
    [[router R1]]
        model = 3745
     S0/0 = R2 S0/0
#################################################################
###########
    [[router R2]]
        model = 3745
```

Figura 5. Ejemplo de configuración para dynagen.

Una pieza normal de software generalmente tiene uno o más lugares en el código donde el programa simplemente se aloja en un loop inactivo o comúnmente dicho “ocioso”; esperando a que se ejecute alguna acción como la presión de una tecla o la finalización de un temporizador para recordar enviar un mensaje. Sin embargo, dynamips es diferente, se trata de un emulador que toma un binario e interpreta cada instrucción de una en una y luego ejecuta esa instrucción en el host, por lo tanto, no existe un estado inactivo. Alguna de esas instrucciones se encontrará en pequeños grupos donde el enrutador emulado está inactivo, como para esperar que llegue un paquete y presionar una tecla en la consola. (Welsh, Dynamips/GNS3 Idle-PC explained. Finally!, 2013)

El problema es que dynamips no tiene idea de si el contador de programa (PC) actual apunta a una tarea importante. La solución ideal sería si de alguna manera dynamips pudiera saber cuándo el contador de programas (PC) apunta a cierta pieza de código que esté en un loop inactivo. Pero lamentablemente no se tiene la manera de saber si un nuevo contador está apuntando a un bucle parado. (Welsh, Dynamips/GNS3 Idle-PC explained. Finally!, 2013)

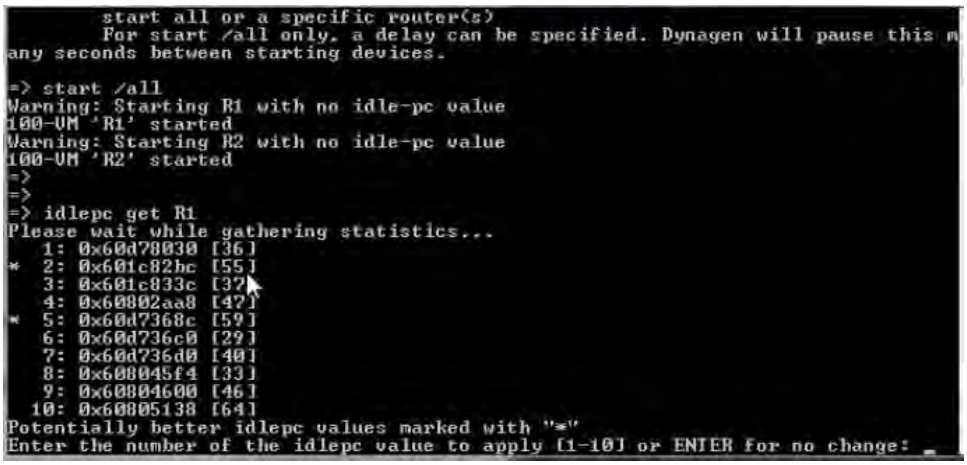

Figura 6. Ejemplo de cálculo de Idle-PC para dynamips.

Por consiguiente y en resumen, un valor Idle-PC es la “adivinación” de dónde el contador de programas tal vez esté apuntando hacia un loop inactivo dentro del router emulado. Si adivinamos en un lugar donde el enrutador emulado pasa mucho tiempo inactivo, entonces la computadora host tiene muchas posibilidades de continuar con otras cosas. Si adivinamos una PC (recuerde PC = contador de programa) donde el código se ejecuta raramente, la computadora host gastará

el 100% de su CPU ejecutando el bucle simple de dynamips. (Welsh, Dynamips/GNS3 Idle-PC explained. Finally!, 2013)

Como cada imagen de enrutador de Cisco tiene un conjunto diferente de instrucciones, estos loops inactivos estarán en lugares diferentes en diferentes imágenes. Pero una vez que se ha encontrado una buena Idle-PC para una imagen, debería ser buena para todas las emulaciones de esa imagen. (Welsh, Dynamips/GNS3 Idle-PC explained. Finally!, 2013)

Continuando con el funcionamiento de GNS3, el archivo mencionado debe de ser un ".net" para que podamos ejecutar los comandos desde una consola de comandos y poder calcular el valor de Idle-PC para un óptimo rendimiento en dynamips. Una vez configurado, dynamips inicia una conexión Telnet con el servidor local y con ello trabajar con los binarios cargados. Todo esto de manera automática por medio del enlace a la interfaz gráfica de GNS3.

El complemento más importante que tiene consigo GNS3 es su máquina virtual llamada GNS3 VM, ésta trabaja basada en la distro de Ubuntu de Linux, y en ella están instalados por defecto motores de virtualización como IOU VM, QEMU y dynamips, lo que quiere decir que está diseñado y listo para virtualizar las imágenes que tengamos disponibles. Inicialmente, GNS3 VM vino a remplazar principalmente a IOS VM para unificar los motores en solo una, ya que para poder emular los binarios IOU se necesitaba de este antiguo complemento. (Duponchelle, What's new in GNS3 1.4, 2016) Sus funciones principales son tres:

1. Cargar las diferentes imágenes hacia el hipervisor de GNS3.
2. Funcionar como servidor local para el almacenamiento.
3. Emular los distintos binarios con diferentes motores de virtualización

Una ventaja que nos da GNS3 VM es el motor QEMU, la cual nos virtualiza sistemas operativos como Windows, Fedora, CentOS etc., de forma portátil y más liviana que las máquinas virtuales nativas como VirtualBox y VMware®. Un ASAv, por ejemplo, puede ejecutarse de forma nativa en VMware® o en QEMU directamente dentro de una plataforma con distribución Linux. Los IOSv de VIRL son ejecutados por medio de este motor de virtualización, también sistemas de otras

fabricantes como BSD; navegadores como Firefox; appliances de seguridad Fortinet etc. (Bombal & Julien, Which emulator should I use?, 2017)

Se recomienda VMware® porque es más rápida y admite virtualización anidada (la VM dentro de la VM es acelerada por su CPU). La diferencia de velocidad es importante y algunos VM se van a ralentizar en VirtualBox. Además de que para imágenes como IOSv o appliances que requieran del motor de virtualización QEMU necesitan a fuerzas correr bajo VMware por cuestiones de aceleración y paravirtualización en KMV, la razón es que VMware toma esta característica directamente de la configuración del BIOS del host anfitrión, mientras que VirtualBox hace solo una simulación de esa capacidad. (Bombal & Duponchelle, GNS3 Setup wizard with the GNS3 VM, 2018)

Otros motores que incluye este complemento son:

- **VPCS**: es una forma ligera de emular PC (contadores de programa) muy básicas. VPCS usa muy poca memoria y, por lo tanto, es una buena opción cuando quiere emular una PC sin una GUI y si solo necesita comandos simples como por ejemplo realizar pings para probar la conectividad en sus redes GNS3. (Bombal & Julien, Which emulator should I use?, 2017)
- **Docker**: es una buena opción cuando quiere emular un servidor o una PC que proporciona un servicio específico, como un servidor TFTP, un servidor de correo o un servidor web; y quieres hacer eso sin usar grandes cantidades de memoria.

  Docker utiliza menos memoria que QEMU o una máquina virtual en VMware/VirtualBox y se ha convertido en una forma popular hoy de crear instancias de un proceso o servicio en comparación con el método tradicional de arranque completo de VM para proporcionar un servicio individual.

  Tradicionalmente, VMware/VirtualBox o QEMU virtualiza el hardware de la PC, pero aún necesita un sistema operativo instalado para las aplicaciones. Docker lleva esto un paso más allá al virtualizar el sistema operativo para la creación de instancias livianas de múltiples procesos.

Debido a que puede crear imágenes Docker con un shell que admite múltiples herramientas, Docker se puede usar como un poderoso reemplazo de VPCS.

Docker es más complicado de configurar cuando se compara con QEMU. Sin embargo, debido a la reducción significativa en el consumo de CPU y memoria, Docker es una gran opción para los proyectos en GNS3. (Bombal & Julien, Which emulator should I use?, 2017)

Ahora, ¿cómo es posible o cual es la forma en que se puedan conectar tantos dispositivos bajo un solo software? GNS3 funciona también como un hipervisor, esta es la parte del software que genera procesos de emulación en los distintos motores cuando sea necesario. El administrador de servidor local gestiona las imágenes que están vinculadas a la dirección IP y puerto especificados dentro de las preferencias de GNS3, cuando se carga el programa enseguida se inicia una conexión con dicha IP para iniciar los servicios de emulación. Esto permite que GNS3 pueda ejecutarse en una máquina, mientras que el emulador puede ejecutarse en máquinas diferentes. (Welsh, How the GNS3 Hypervisor Manager Works?, 2013)

Cuando se crea la conexión, además de inicializar los servicios de emulación, también corre la máquina virtual de GNS3 en caso de emplearla y establece un enlace Telnet con un puerto TCP para cada consola hacia los distintos appliances; ahora, para las conexiones entre ellos se crea un túnel UDP, esto lo hace usando el rango de los puertos para UDP tunneling configurados como se muestra en la Figura 7. (Welsh, How the GNS3 Hypervisor Manager Works?, 2013)

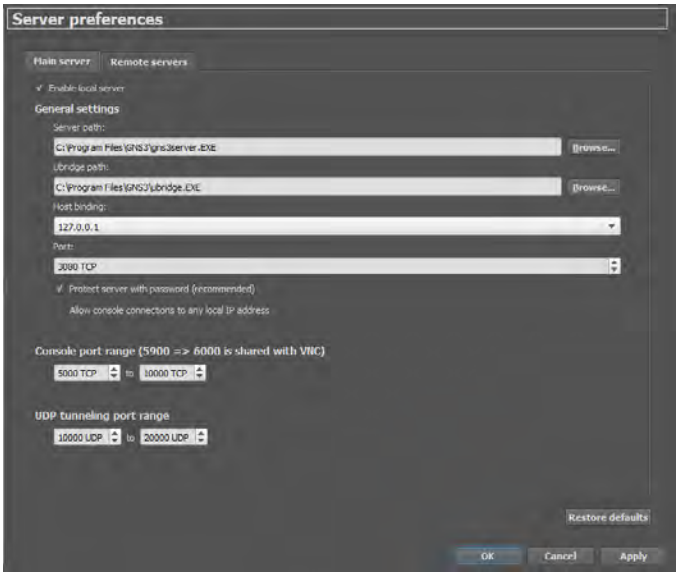

Figura 7. Vínculo con host y configuración de servidor.

Al momento de iniciar una imagen, se crea una instancia dependiendo el motor que se use, un ejemplo, si es una imagen IOS se creará una instancia de dynamips, si es la ejecución de un IOSv sería una instancia QEMU. Para cada instancia es un puerto distinto tanto para consola (TCP) y para conexión entre dispositivos (UDP tunneling). (Welsh, How the GNS3 Hypervisor Manager Works?, 2013)

Una demostración clara de esto es cuando realizamos la conexión básica entre un router y una máquina virtual. Imaginemos dos escenarios a partir de este ejemplo, supongamos que el enrutador es una imagen c7200 emulada por dynamips en el servidor local y tenemos configurados los siguientes parámetros:

- **Host binding**: 127.0.0.1
- **Port**: 3080
- **Console port range**: 8000 to 12000
- **UDP tunneling port range**: 5000 to 8000

Inicialmente, cuando arrancamos GNS3 se establece conexión (como lo muestra la Figura 8) e inicia el proceso de emulado, pero aún no se crea ninguna instancia dentro del área de trabajo. Una vez agregado y creado por consiguiente dichas instancias, se agrega una máquina virtual de

VirtualBox con sistema operativo Windows 7, la conexión virtual entre el enrutador y la VM se crea entre un túnel UDP, cada uno con distinto puerto siempre dentro del rango configurado, por ejemplo, el router con el puerto de origen (sport) 5003 y de destino (dport) 5004 y el Windows 7 virtual con 5001 de origen y 5002 de destino, ahora bien, esta conexión esta enlazada con la dirección de host local la cual es (por lo general) la IP loop 127.0.0.1, y para la visualización de la consola del enrutador se crea otra conexión por Telnet con la misma IP local, pero con los puertos TCP dentro del rango establecido, esta vez supongamos que es con el puerto 8002 para el router y 8001 para la maquina virtualizada.

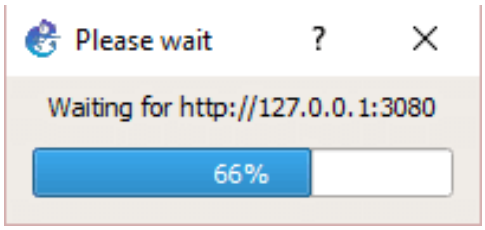

Figura 8. Estableciendo conexión entre GNS3 y el servidor local de emulación.

Ahora imaginemos un segundo escenario, y que la imagen de router en vez de ser un IOS con dynamips como motor de emulación, en su lugar sea un IOSv, recordemos que los IOSv corren bajo el motor QEMU, por lo tanto, trabajaremos con el complemento GNS3 VM en VMware®, éste primero carga la imagen al hipervisor GNS3. Los parámetros serian lo mismo salvo con un agregado: la IP será la de GNS3 VM. Siguiendo el plan de suposición imaginemos que la dirección sea la 192.168.20.100. En esta situación se repite los mismos pasos, se crea el túnel UDP con sus respectivos puertos de origen y de destino, uno a través de la IP loop local por parte de la máquina VirtualBox y por el otro lado a través de la IP local virtual configurada en GNS3 VM, pero con diferentes direcciones para la conexión de consola, la conexión enlazada al servidor local (127.0.0.1) por parte de la máquina emulada con VirtualBox, y con la dirección de GNS3 VM (192.168.20.100) por parte del enrutador emulado con QEMU, cada uno con sus puertos TCP establecidos dentro del rango configurado.

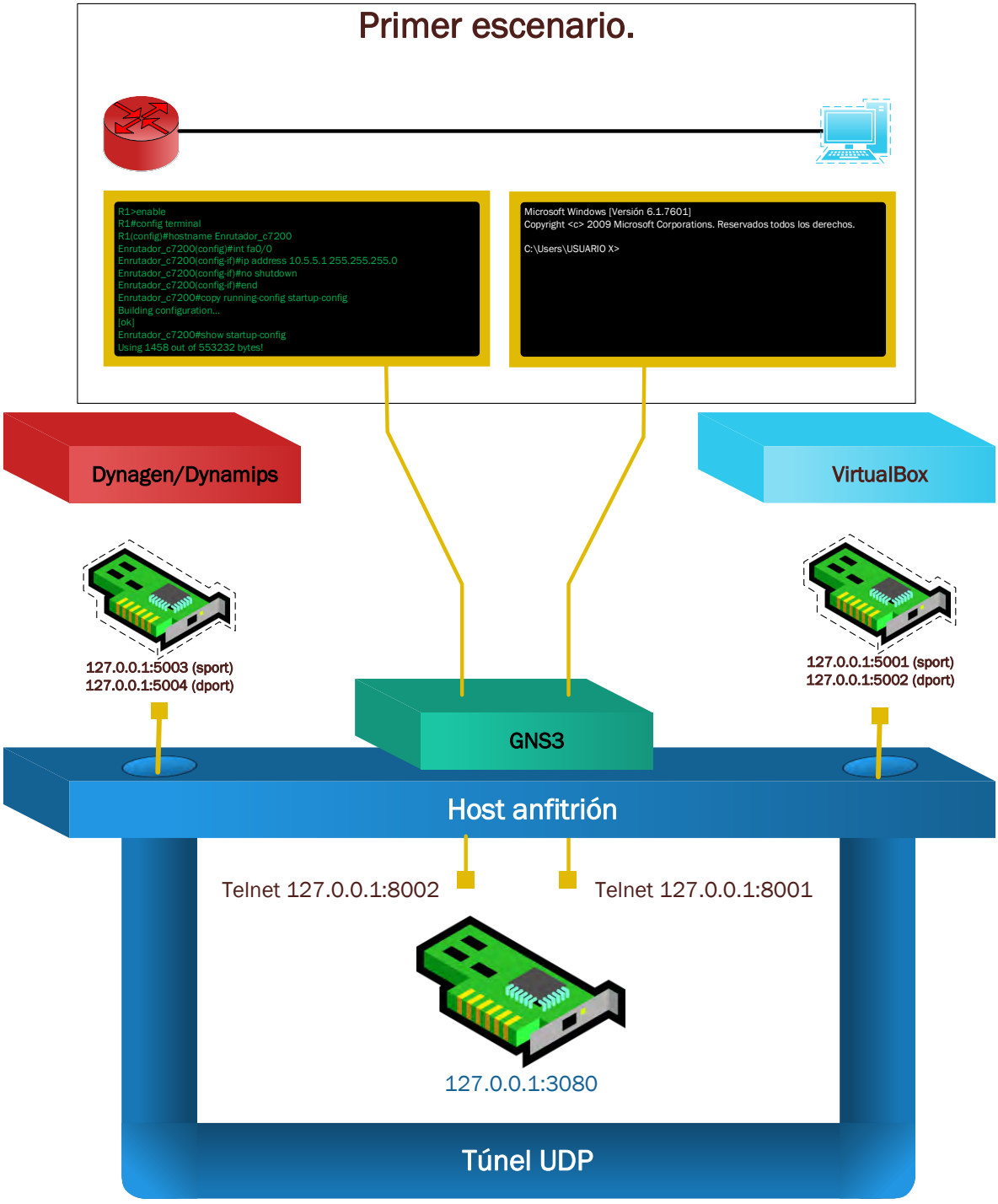

Figura 9. Primer escenario.

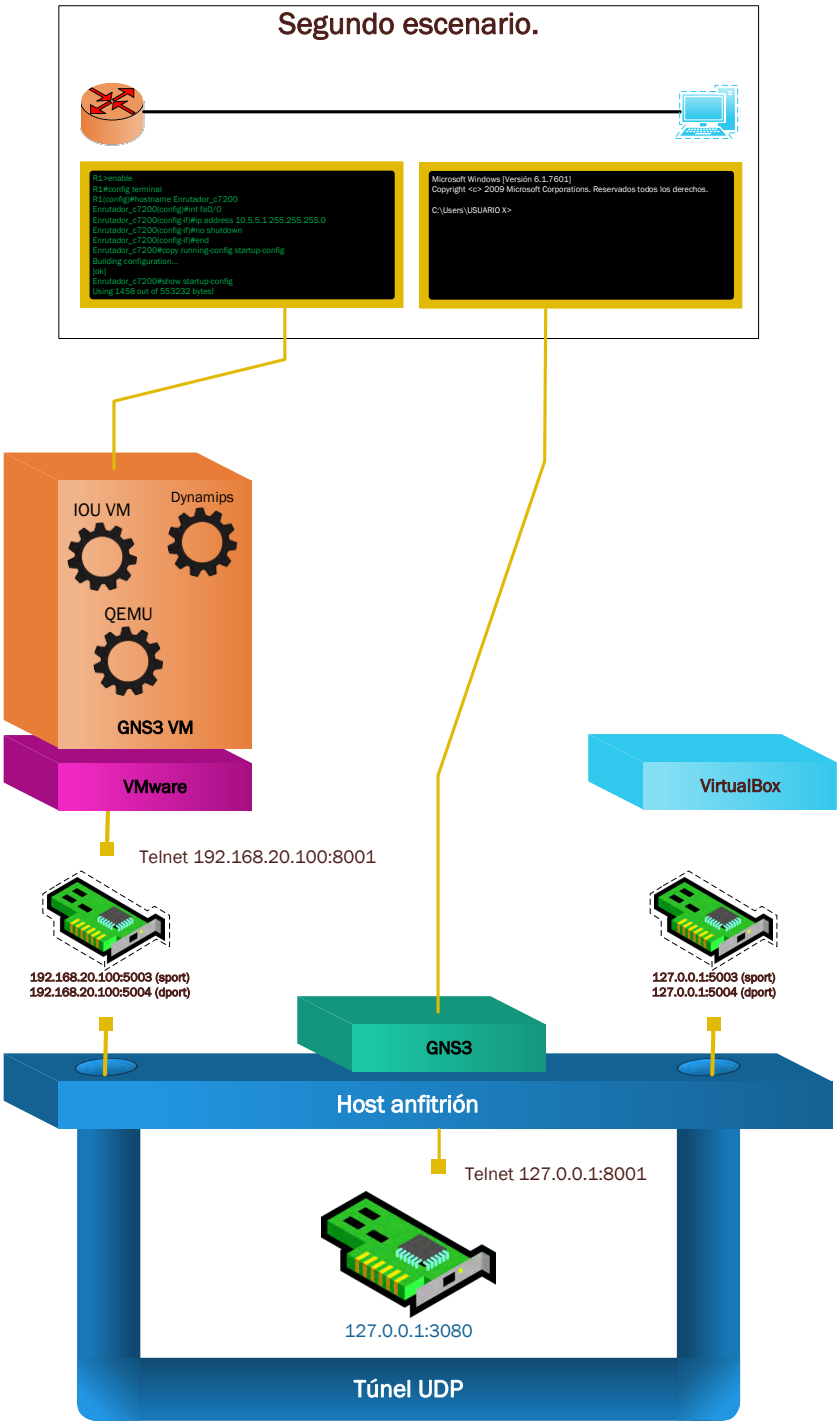

Figura 10. Segundo escenario.

CAPÍTULO III Desarrollo.

Para la realización y el desarrollo del laboratorio de seguridad virtual, se necesitó más que una simple conexión entre un enrutador virtual y una maquina emulada por VirtualBox. Se requirió de muchos dispositivos virtuales con la idea de hacer el entorno lo más realista posible; por lo tanto, se configuraron diferentes protocolos tratando de alcanzar todos los tópicos enseñados en los currículos de CCNA Exploration.

Dichas configuraciones de protocolos y servicios son hechas para garantizar una conexión básica y sin inconvenientes al momento de realizar las pruebas de seguridad y seguir con el procedimiento correcto de las variaciones que pudieran tener los diferentes tipos de ataque en una determinada prueba. Por ejemplo, si se quiere demostrar una intrusión por medio de un TCP reverso y se tiene configurado medidas de restricción estrictas, por decir, ACL's extendidas con sistemas de firewall o IPS/IDS al máximo nivel de seguridad, nos dará dificultades para la exposición de dicho tipo de ataque. Por el contrario, si se quiere demostrar una evasión a sistemas como un perimetrales de seguridad pues es necesario en cierto punto configurar las debidas medidas para tener cierto ambiente deliberadamente asegurado. Por este motivo no se configuró ninguno de estos protocolos de seguridad, pero se harán más en su debido tiempo cuando se requieran.

A modo de exposición, se mostrará los pasos requeridos para la instalación y configuración de los distintos dispositivos en GNS3 y se mostrará en anexos el proceso de integración de cada tipo de appliance y en diferentes formas, así, cada uno de estos dispositivos virtuales fueron creados para el laboratorio propuesto y repetidos en varias instancias, por lo tanto, no vale la pena y no es necesario mostrar el proceso de cada appliance puesto en el área de trabajo, ya que, seria repetir de manera engorrosa cada integración sabiendo que los pasos son iguales para todos, la razón de esto es porque son dispositivos de modelos repetidos como se verá en la descripción de laboratorio.

Instalación de GNS3 GUI.

En el anterior capítulo mencionábamos que GNS3 puede ser usado sin su máquina virtual como componente, y que en su forma más básica podemos hacer de muchas cosas con las imágenes por defecto que trae consigo y con las IOS para dynamips. En esta sección se tocará la primera parte de la instalación sin GNS3 VM y mostrando la agregación de los diferentes tipos de applaince que el servidor local soporta.

El hipervisor GNS3 fue instalado en un equipo con virtualización Intel VT-x/EPT habilitado desde BIOS para la mejora de rendimiento. Si un equipo cuenta con AMD no habrá problema ya que se puede activar su similar que es la virtualización AMD-V/RVI, pero siempre debe estar activada en cualquiera de los casos.

Dicho equipo tiene los valores de especificación óptimos para estas tareas y con la finalidad de evitar inconvenientes, la siguiente lista menciona solo las características relevantes para la ejecución del software:

- **Sistema operativo**: Windows® 10 x64
- **Procesador**: Intel Core i7 4ª generación 4702MQ Quad Core.
- **RAM**: 16 GB SODIMM 1660 MHz.
- **Almacenamiento**: 500 GB SSD + 2 TB HDD.

Se debe recordar que si se quiere probar con topologías más largas y complejas es recomendable no hacer uso del servidor local porque nos presentaría muchos errores e imposibilidades al momento de hacer uso de ciertos appliances. Para ello sirve el componente principal de GNS3 que es su máquina virtual creada para ese propósito y por sus características inherentes que nos ofrece.

Por el contrario, si haremos uso de una pequeña topología y con configuraciones básicas, se recomienda el uso del servidor local de GNS3 y de esta manera ahorrar recursos informáticos.

Con estas dos aclaraciones, procedemos a enumerar los pasos necesarios para la instalación de GNS3:

1. Primeramente, se tiene que estar registrado en la página web oficial de GNS3 para acceder y descargar tanto el programa y la máquina virtual complemento (GNS3 VM). Entre a la página oficial de GNS3 https://www.gns3.com/ y haga clic en “Free Download”.

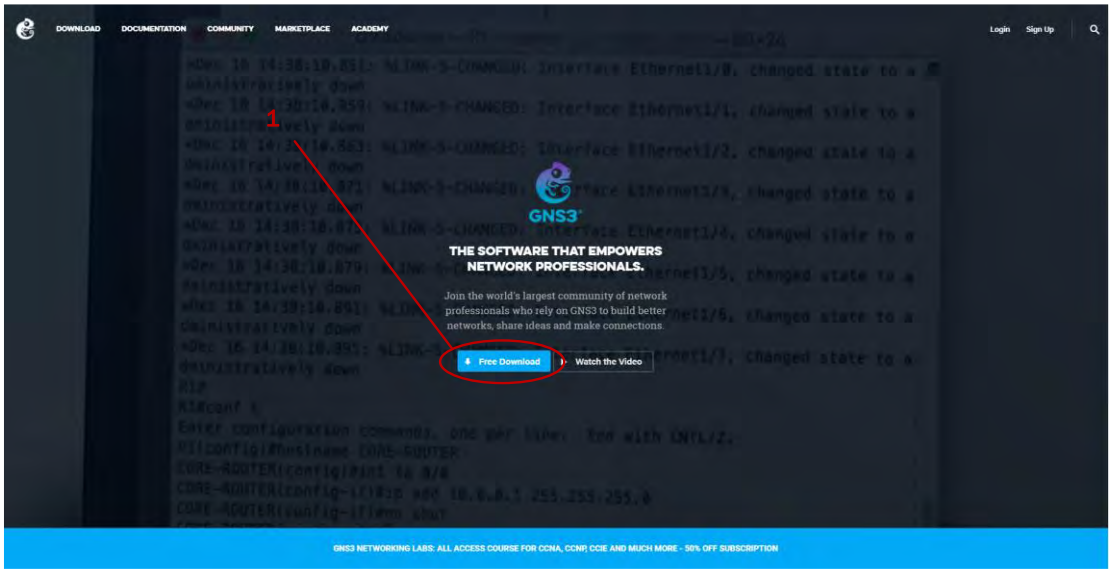

Figura 11. Página de inicio de GNS3.

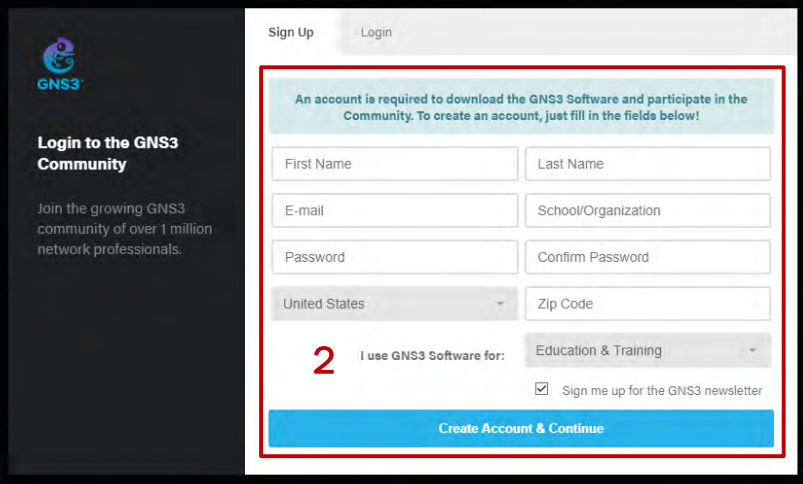

Figura 12. Solicitud de datos.

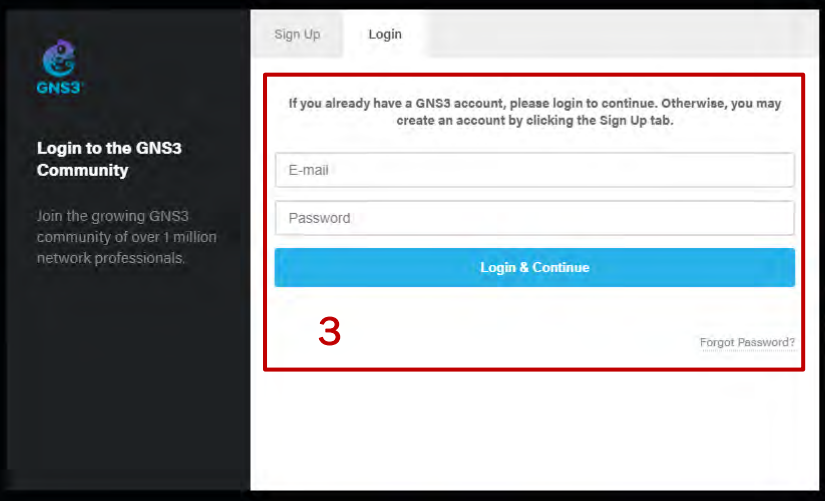

Figura 13. Inicio de sesión.

4. Una vez con la sesión iniciada nos saldrá automáticamente las opciones de sistema operativo soportados, con el número de versión y en la parte inferior el link para la descarga de GNS3 VM, pero en este caso ignoramos esa parte ya que solo se tratará de GNS3 con servidor local; en este caso elegimos Windows.

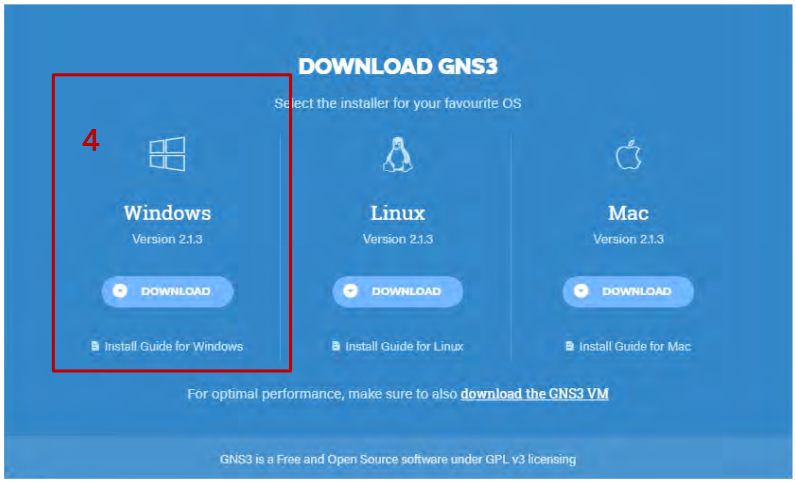

Figura 14. Sistemas operativos soportados para GNS3.

5. Después de descargar GNS3, procedemos a buscar la carpeta de descargas y ejecutamos.

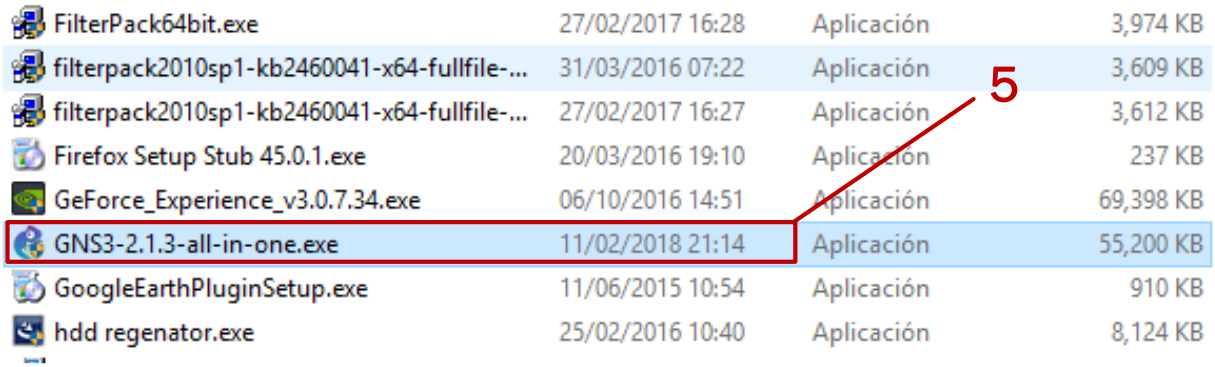

Figura 15. Ejecución de instalador.

6. Nos saldrá la ventana del Control de Acceso de Usuarios preguntándonos si queremos realizar cambios en el equipo ya que se trata de una instalación nueva; damos clic en “Sí”.

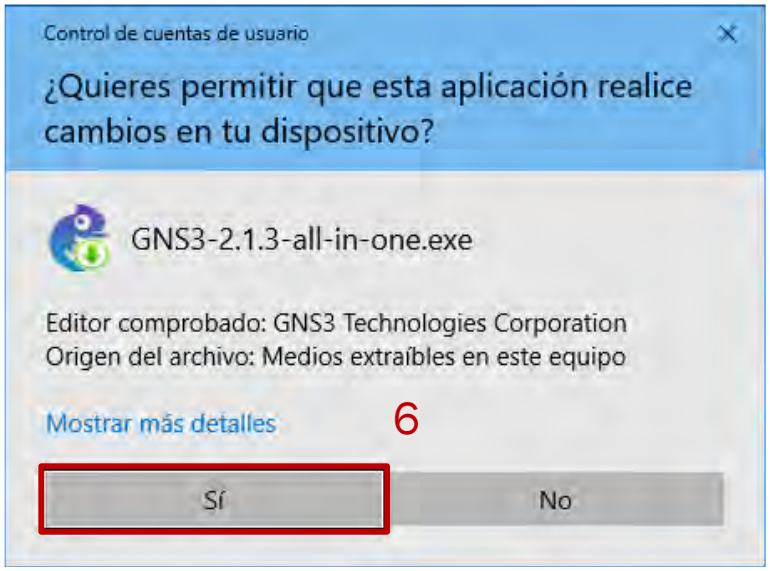

Figura 16. Control de Acceso de Usuarios.

7. Luego nos saldrá la ventana donde nos dice que nos guiará a en la instalación de GNS3 y que es recomendable que cerremos todas las aplicaciones para evitar incidentes tanto para esta acción o actualización en caso de que estemos usando una versión más vieja.

Figura 17. GNS3 setup.

8. Enseguida aparecerá el acuerdo de la Licencia Pública General de GNU la cual debemos de estar de acuerdo si queremos instalar el programa.

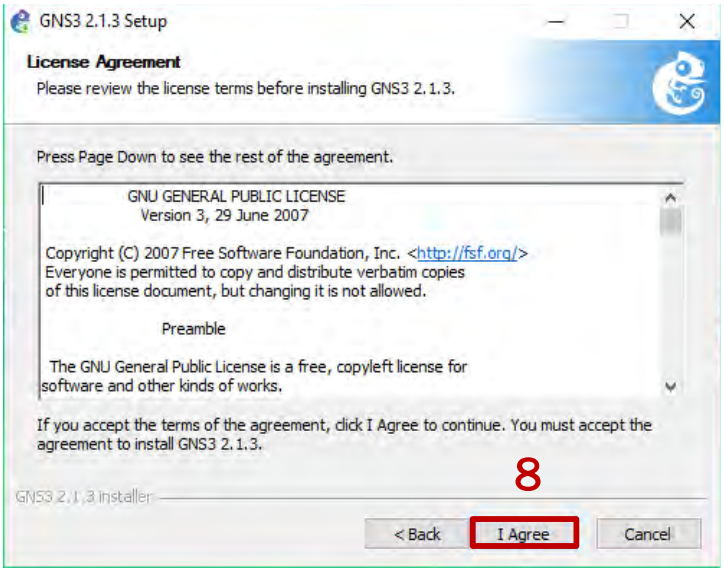

Figura 18. GNS3 GPL.

9. Nos mostrará si queremos renombrar la carpeta para los accesos directos, lo dejamos por defecto para evitar confusiones.

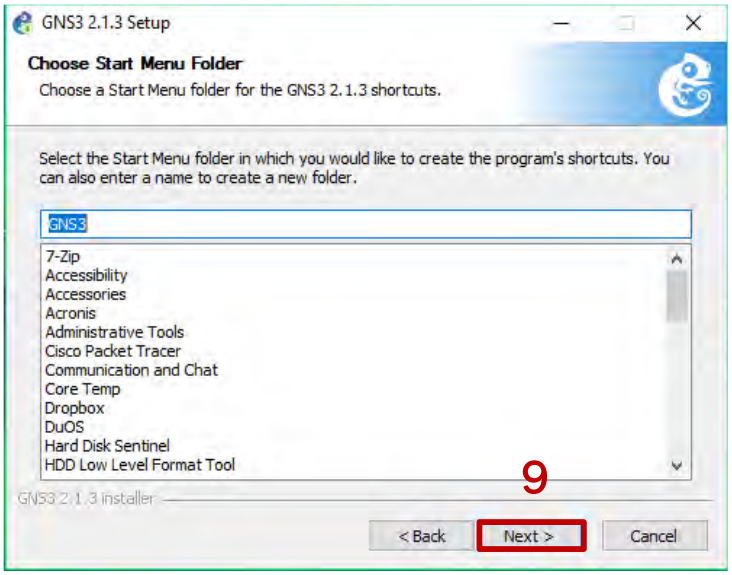

Figura 19. Nombre de carpeta para accesos directos.

10. La siguiente ventana nos expondrá las distintas dependencias que GNS3 maneja, algunas son opcionales ya que no son relevantes para ejecutar las diferentes integraciones. Hacemos clic en “Next”.

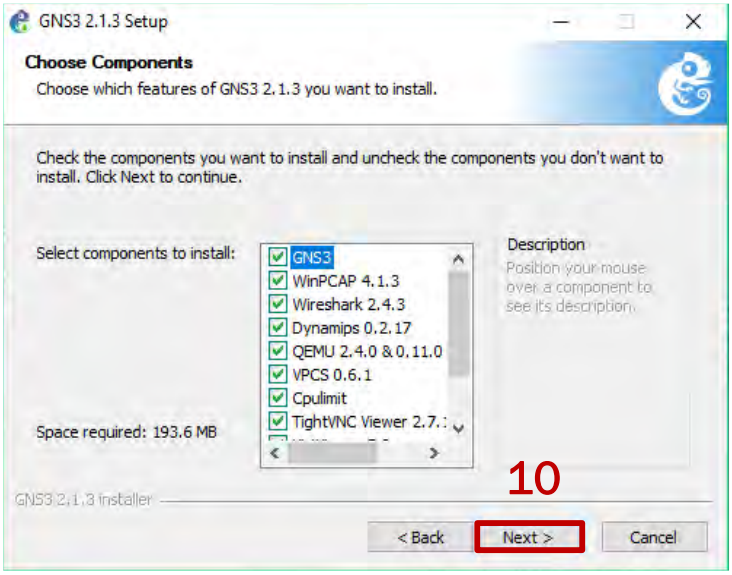

Figura 20. Dependencias de GNS3.

Dichas dependencias son: (Bombal, Duponchelle, & Ganancial, Windows Intallation, 2018)

Dependencia.	Requerido	Descripción.

GNS3	Requerido	El núcleo de GNS3. Éste es siempre requerido.
WinPCAP	Requerido	Requerido para conectar GNS3 a la red computacional. Si no se instala esta dependencia GNS3 será incapaz de comunicarse con el mundo real.
Wireshark	Recomendado	Permite capturar y ver el tráfico de red enviado entre dispositivos.
Dynamips	Requerido	Requerido para correr una instalación local de GNS3 con enrutadores Cisco. Solo se puede desmarcar si se usará única exclusivamente GNS3 VM.
QEMU 2.4.0 y 0.11.0	Requerido	Es un emulador usado para virtualizar una computadora de manera completa. La versión vieja de QEMU 0.11.0 es instalado en orden para soportar dispositivos ASA.
VPCS	Recomendado	Es un emulador muy ligero que soporta comandos básicos como ping, por decir un ejemplo.
Cpulimit	Requerido	Es utilizado para evitar que QEMU use el 100% del CPU (cuando está en ejecución).
TightVNC Viewer	Recomendado	Un cliente VNC utilizado para conectarse a las interfaces gráficas de usuario del dispositivo.
VirtViewer	Opcional	Es un cliente SPICE de Windows para control de escritorio remoto.
SolarWinds Response Time Viewer	Opcional	Software opcional para la visualización de captura de tráfico de red en un formato fácil de lectura.
Npcap	Opcional	Reemplazo moderno de WinPCAP para solucionar problemas con Windows 10 pero es menos probado que WinPCAP.

Tabla 3. Descripción de dependencias.

11. Siguientemente nos solicitará si deseamos cambiar la ruta de instalación de GNS3, ya sea que, si se tiene una partición asignada especialmente para la instalación de archivos de sistema y programas, un lugar en red o un espacio especial solo para GNS3. En este caso dejamos el valor por default y proseguimos a instalar.

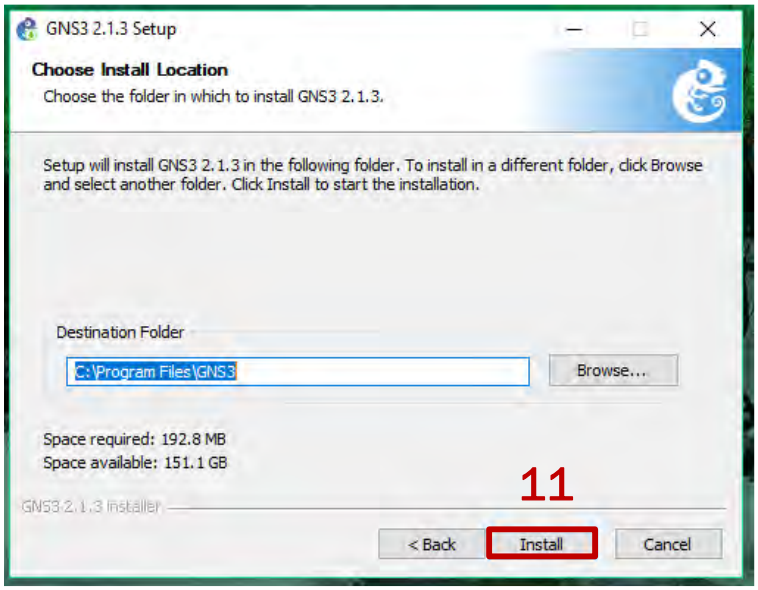

Figura 21. Directorio de instalación.

12. En este punto comenzará el paso de instalación, durante el proceso también incluirá las dependencias seleccionadas anteriormente tanto para las requeridas, recomendadas y opcionales, pero, hay un detalle en la forma de instalación, las instalaciones para las dependencias requeridas están integradas directamente por el instalador, mientras que las que son recomendadas y opcionales se realizan de forma externa, esto quiere decir que se descargan desde internet primero buscando frameworks necesarios para su instalación y

posteriormente instalándose. Dado a esto, tenga cuidado si está usando un plan de datos ya que podría haber cargos de contratación por su operadora.

13. Durante la finalización de la instalación de GNS3 nos saltará una ventana en la cual nos pregunta si queremos tener una licencia de prueba por catorce días para Solarwinds Standard Toolset, ya que su valor es de $200 USD anuales. Esta herramienta nos provee

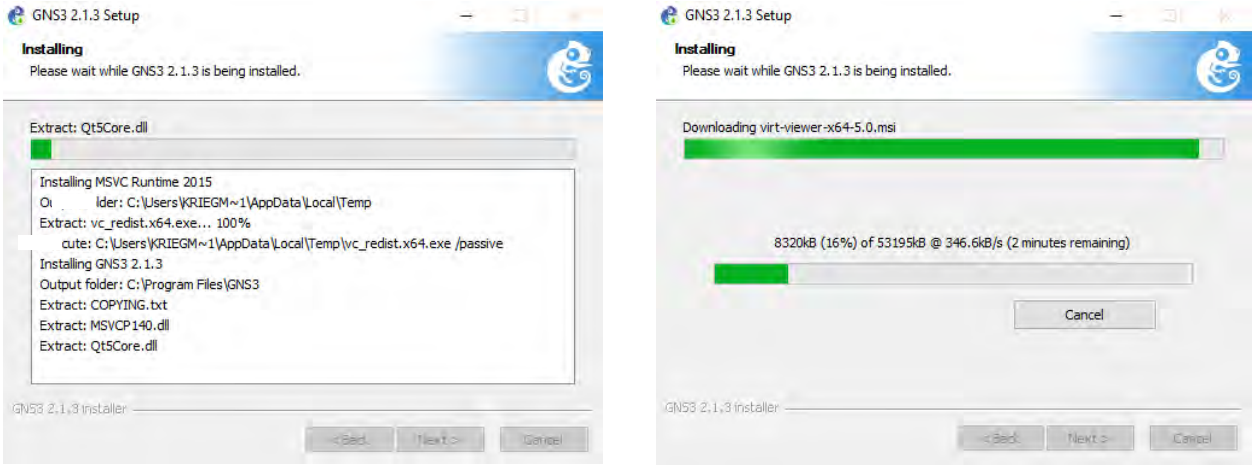

Figura 22. Instalación de GNS3 y descarga de dependencias externas.

las siguientes características para integrar a GNS3:

- Detección de redes automatizada.
- Monitoreo y alertas en tiempo real.
- Potentes capacidades de diagnóstico.
- Seguridad de red mejorada.
- Configuración y administración del registro.
- Monitoreo de direcciones IP y ámbitos DHCP.

En este caso, seleccionamos la opción negativa.

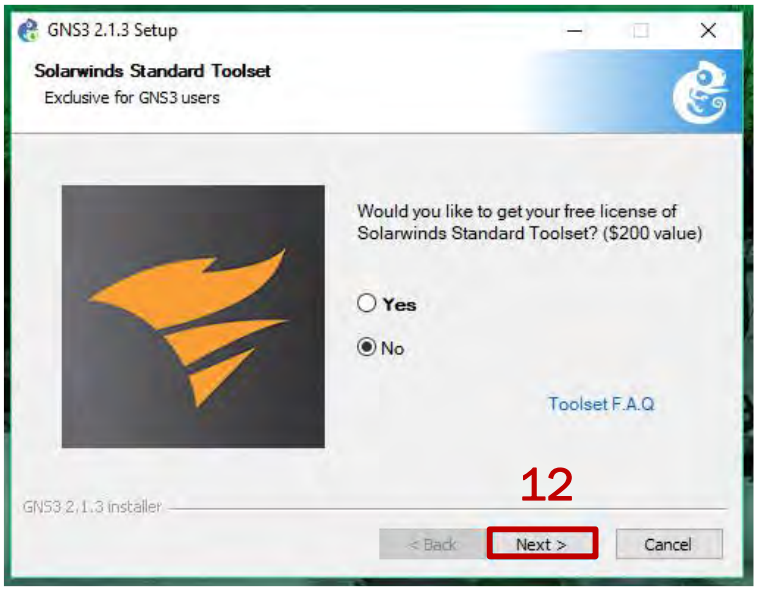

Figura 23. Oferta de licencia de Solarwinds Stantard Toolset.

14. Una vez instalados completamente GNS3 y sus dependencias damos clic en “Finish” para finalizar la instalación, se puede marcar o desmarcar la opción de iniciar GNS3 de inmediato, pero es cuestión de preferencias, en este caso lo dejamos seleccionado.

Figura 24. Finalización de instalación.

Creación de topologías con servidor local de GNS3.

Después de finalizar la instalación tenemos ya listo y en disposición del servidor local para emular las imágenes de Cisco y hacer uso de las integraciones por defecto de GNS3 como las built-in.

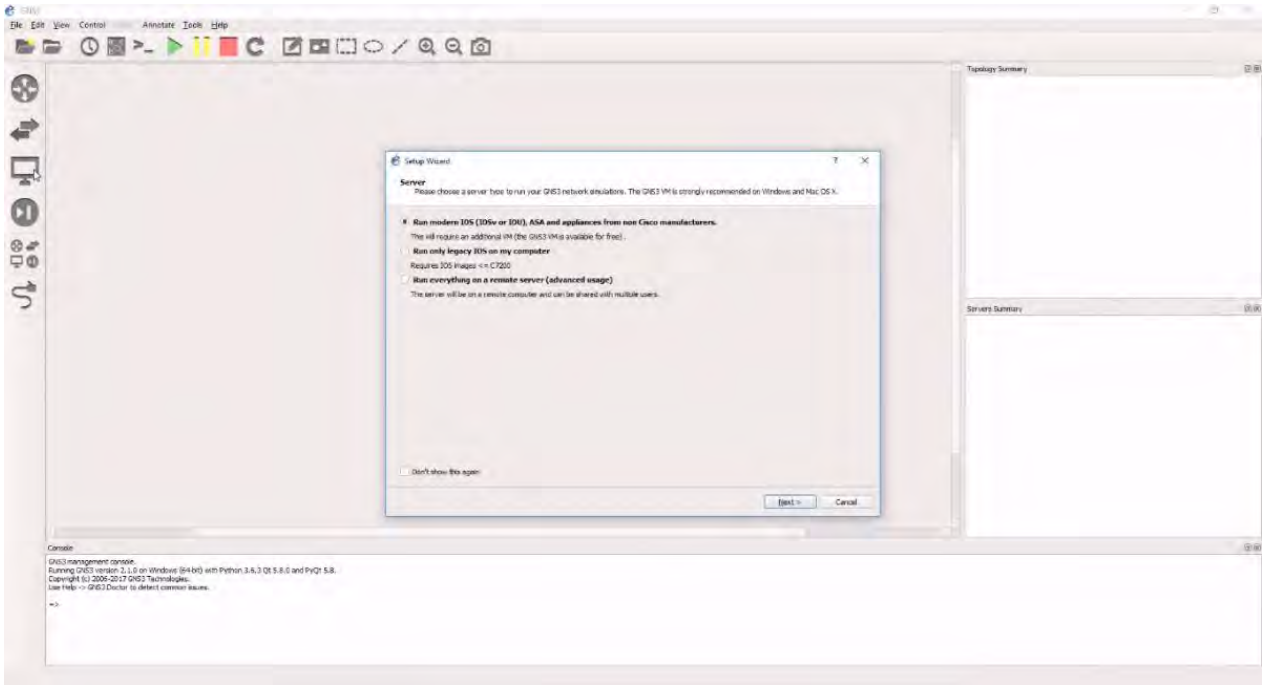

Figura 25. Pantalla de inicio de GNS3.

Aviso: Al iniciar GNS3 podríamos ver algunos mensajes de error y de advertencia, esto es debido a que algún programa de seguridad que esté ejecutándose en el sistema operativo anfitrión, ya sea un firewall o un antivirus, tenga alguna injerencia en el funcionamiento del programa en cuestión, esto se debe a que estos softwares de seguridad detectan como sospechoso el comportamiento de GNS3 por medio de sus motores heurísticos proactivos, por esta razón es "recomendable" desactivar la protección de estas herramientas de manera temporal. Lo ideal sería que se filtrara o se excluyera a GNS3 de las listas de aplicaciones sospechosas sin desactivar estas soluciones y seguidamente reiniciar el computador.

Para la instalación de appliances, diríjase a la sección de anexos.

Descripción de laboratorio.

Para el laboratorio prototipo se requirió de siete enrutadores de los cuales dos son IOSv, los cinco restantes son bajo modelo y chasis c7200 y uno de ellos actuando como enrutador/nube para la interconexión de zonas; diez conmutadores IOSvL2 las cuales cuatro son multicapa y los nueve restantes actúan como switches de capa de acceso; un conmutador IOU; tres cortafuegos pfSense las cuales una actúa como gateway/firewall doméstico y las dos restantes como IDS; y siete máquinas virtuales las cuales cuatro funcionan como servidores y tres como equipos invitados.

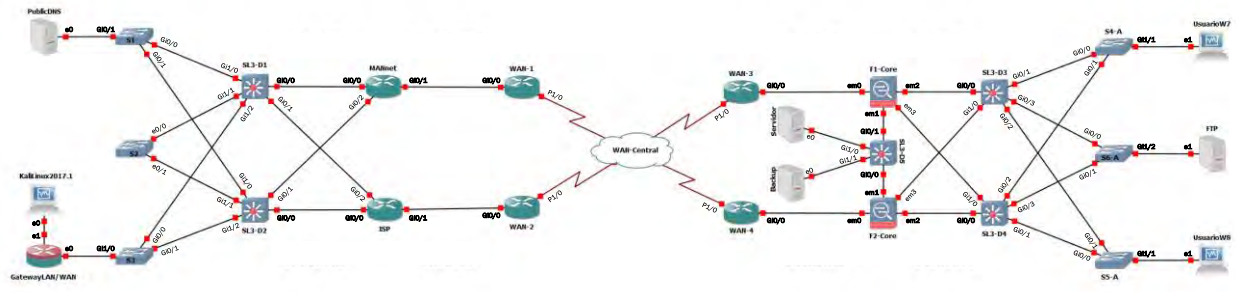

Figura 26. Laboratorio prototipo inicial

A continuación, se especificará los tipos de dispositivo con su motor de emulación para cada elemento puesto en el modelo de topología, con el fin de calcular el consumo de recursos informáticos.

- Enrutadores.
  - Dynamips (IOS c7200-adventerprisek9-mz.124-24.T5.bin)
    - WAN-1, WAN-2, WAN-3, WAN-4, WAN-Central.
  - QEMU (IOSvL3).
    - MANnet, ISP.
- Conmutadores.
  - QEMU (IOSvL2).
    - SL3-D1, SL3-D2, SL3-D3, SL3-D4, SL3-D5, S1, S3, S4-A, S5-A, S6-A.
  - IOU (IOUL2).
    - S2.
- Cortafuegos.

    - QEMU (pfSense).
        - F1-Core, F2-Core.
    - VirtualBox (pfSense),
        - GatewayLAN/WAN.
- Servidores.
    - VirtualBox.
        - PublicDNS (Debian 8), Servidor (Windows Server 2012 R2), Backup (Windows Server 2012 R2), FTP (Debian 8).
- Equipos.
    - VirtualBox.
        - Kali Linux 2017.1, Usuario W7 (Windows 7), Usuario W8 (Windows 8).

Ahora, para la mayoría de los appliances en este modelo de topología se requirió de la configuración e instalación de ciertos protocolos y servicios. La siguiente lista nos mostrará de forma ordenada dichas configuraciones aplicadas por dispositivos virtuales:

- **S1, S2, S3, S4-A, S5-A y S6-A**: VLAN y RPVST.
- **SL3-D1, SL3-D2, SL3-D3 y SL3-D4**: VLAN, 802.1Q trunking, DTP, RPVST, Inter-VLAN, HSRP, OSPF, DHCP, SSHv2 y Telnet.
- **SL3-D5**: VLAN, Inter-VLAN, 802.1Q trunking, OSPF, SSHv2 y Telnet.
- **WAN-1, WAN-2, WAN-3, WAN-4, WAN-Central, MANnet, ISP**: OSPF, SSHv2, Telnet y NTP.
- **F1-Core, F2-Core**: NAT, OSPF y DNS forwarding.
- **GatewayLAN/WAN**: NAT, DNS forwarding y DHCP.
- **Servidor y Backup**: resolución DNS, NTP, Directorio Activo, Controlador de Dominio, servicio web.
- **PublicDNS**: resolución DNS, DNS forwarding, NTP.
- **FTP**: FTP, TFTP.

Se tomó como referencia a las redes jerárquicas Top-Down de la manera más cercana posible dentro de las posibilidades para el diseño de topología lógica que representa por lo general a una

infraestructura de red con un ambiente real similar, esto es con la finalidad de representar ataques remotos; significa que el modelo en cuestión tiene por considerado lo siguiente en términos de virtualización:

- **Redundancia**: simular esta característica permite la disponibilidad en las conexiones y en las pruebas de pen-testing.
- **Seguridad**: las diferentes políticas de seguridad a nivel de acceso y de distribución expondrá de mejor forma las evasiones que se quieran probar en determinados experimentos más avanzadas.
- **Escalabilidad**: para expandir en caso necesario la topología para pruebas puntuales.
- **Facilidad de administración**: el diseño de la topología cede la gestión más fácil de cada dispositivo para una mejor visualización de ambiente de laboratorio.
- **Facilidad de mantenimiento**: en técnicas de modularidad, si un dispositivo falla rápidamente se puede revertir el incidente ya sea por medio de un snapshot, la copia de configuraciones por TFTP y/o la restauración de imágenes.
- **Rendimiento**: tomando la oportuna atención hacia un ambiente de red adecuado para las distintas pruebas, cobra sentido cuando se demanda una alta carga de datos más si es de manera remota, por lo tanto, para evitar cualquier problema los enlaces entre cada capa son 1000BASE-TX y para el grupo de conexión entre los enrutadores WAN y el enrutador-nube central son bajo interfaces de fibra óptica virtuales SONET.
- **Capas de jerarquía**: para tener una buena representación de esta característica inherente al diseño, se dividió en dos zonas (sin contar la zona WAN), cada uno con su dominio y capa correspondiente, simulando así dos infraestructuras independientes.
    - **Capa de acceso**: S1, S2, S3, S4-A, S5-A y S6-A.
    - **Capa de distribución**: SL3-D1, SL3-D2, SL3-D3, SL3-D4 y SL3-D5.
    - **Capa de núcleo**: MANnet, ISP, F1-Core y F2-Core.

El direccionamiento fue configurado con la misma finalidad de representar un entorno aproximado a uno real, por esa misma razón se hizo uso de CIDR con VLSM y presuponiendo que las redes son parte de dos organizaciones totalmente distintas, contando también con la zona WAN que simula la sección de interconexión entre las dos zonas principales; por eso mismo, se hizo un

pequeño análisis para el cálculo del número total de IP dentro de un escenario hipotético, sin dejar de lado futuros elementos que nos podrían servir en otras pruebas más adelante. La siguiente tabla nos muestra cómo se conforma el direccionamiento del laboratorio propuesto:

<table>
<tr><th colspan="3">Zona my-telecom.net</th><th colspan="3">Zona lab-sec.com</th></tr>
<tr><td colspan="3">Superred: 10.30.0.0/17</td><td colspan="3">Superred: 192.168.0.0/17</td></tr>
<tr><td>VLAN40</td><td>Clientes</td><td>10.30.0.0/18</td><td>VLAN100</td><td>DataCenter</td><td>192.168.0.0/18</td></tr>
<tr><td>VLAN20</td><td>Extras</td><td>10.30.64.0/26</td><td>VLAN10</td><td>Administrativa</td><td>192.168.64.0/28</td></tr>
<tr><td>VLAN10</td><td>Administrativa</td><td>10.30.64.64/28</td><td colspan="3">Superred: 92.68.9.0/24</td></tr>
<tr><td colspan="3" rowspan="4"></td><td>VLAN30</td><td>Servidores</td><td>92.68.9.0/24</td></tr>
<tr><td colspan="3">Superred: 172.16.0.0/21</td></tr>
<tr><td>VLAN80</td><td>Empleados</td><td>172.16.0.0/22</td></tr>
<tr><td>VLAN90</td><td>Jefes</td><td>172.16.4.0/23</td></tr>
<tr><td colspan="2">Enlace 1 principal (SL3-D1 a MANnet)</td><td>10.30.64.80/30</td><td colspan="2">Enlace 1 principal (SL3-D3 a F1-Core)</td><td>172.16.6.0/30</td></tr>
<tr><td colspan="2">Enlace 2 principal (SL3-D2 a ISP)</td><td>10.30.64.84/30</td><td colspan="2">Enlace 2 principal (SL3-D4 a F2-Core)</td><td>172.16.6.4/30</td></tr>
<tr><td colspan="2">Enlace 1 respaldo (SL3-D1 a ISP)</td><td>10.30.64.88/30</td><td colspan="2">Enlace 1 respaldo (SL3-D3 a F2-Core)</td><td>172.16.6.8/30</td></tr>
</table>

Enlace 2 de respaldo (SL3-D2 a MANnet)	10.30.64.92/30	**Enlace 2 de respaldo (SL3-D4 a F1-Core)**	172.16.6.12/30
		Superred: 185.0.0.0/11	
		Enlace F1-Core a SL3-D5	185.20.30.0/30
		Enlace F2-Core a SL3-D5	185.10.20.0/30
Zona WAN my-telecom.net		**Zona WAN lab-sec.com**	
Superred: 120.30.64.0/20		**Superred**: 140.50.48.0/20	
Enlace MANnet a WAN-1	120.30.64.0/30	**Enlace F1-Core a WAN-3**	140.50.60.0/30
Enlace ISP a WAN-2	120.30.72.0/30	**Enlace F2-Core a WAN-4**	140.50.61.0/30
Conexión a WAN-Central			
Superred: 0.0.0.0/0			
Enlace a WAN-1	100.150.200.0/30		
Enlace a WAN-2	200.150.100.0/30		
Enlace a WAN-3	30.40.50.0/30		
Enlace a WAN-4	40.50.60.0/30		

Tabla 4. Direccionamiento de laboratorio prototipo inicial.

No obstante, a todo esto, no descartemos que este diseño podría ser remplazado por uno más específico dependiendo del tipo de prueba que se vaya a requerir, esto puede significar cambios tanto en las configuraciones de protocolos y servicios, en el esquema de topología y hasta el direccionamiento IP.

CAPÍTULO IV Resultados y conclusiones

"La seguridad informática no es magia, es ciencia".

Chema Alonso.

Al paso del tiempo las tecnologías seguramente evolucionarán y, por lo tanto, lo que está "detrás del telón" de esas tecnologías también lo harán, no por ello estas implementaciones sean actualmente obsoletas si no que ofrecen un compendio para el seguimiento oportuno de esos cambios. Esto, además, dará a entender que lo más importante en las empresas es "componer lo básico", es decir, detectar y aplicar correctivos necesarios sin muchas pretensiones, las empresas que verdaderamente toman en cuenta este factor no necesitan de eso.

No existe tal cosa como límites de seguridad, por tanto, no existen aplicaciones cien por ciento seguras; sin embargo, no por ello descartar su importancia ya que cada solución está destinada para la resolución de problemas puntuales mas no de todo. De tal modo que para tener una buena enseñanza se debe de comprender que actualmente como mencionaba Linus Torvalds en una entrevista en 2008: "El tiempo de las soluciones sencillas a problemas sencillos hace años que pasó en la tecnología y seguridad". Por consiguiente, la complejidad de la gestión de la seguridad es muy alta y el individuo que quiera tomarse muy en serio y ser organizado.

Existen diferentes modos para experimentar con las tecnologías de la información y comunicación, lo más imprescindible es saber cómo se comportan los distintos dispositivos en diferentes entornos. Todo se vuelve significativo cuando se trata en el ámbito de seguridad ya que al final nos permitirá aprender las maneras de contrarrestar las vulnerabilidades y, además, de cómo funcionan los ataques de manera empírica y que mejor que de una forma segura y controlada.

En sí, el programa que es objeto de exposición no tuvo percances en el uso con las diferentes configuraciones, pero, a decir verdad, no se han probado por completo todas las posibilidades con la aplicación y con los appliances. Esto se debe a que solo se aplicaron los tópicos enseñados por CCNA Exploration en cuestión de redes como se mencionaba en el capítulo de desarrollo. Sería

una buena idea aprovechar las cualidades de este programa y de la propuesta para poder en un futuro ejercer temas más avanzados y usar varios tipos de appliances.

Las ventajas de la virtualización de red nos dan muchas facilidades de uso y de experimentación de forma que no gastemos nuestros recursos económicos, pero esto no significa que sea lo mejor de todo, ya que, es muy importante reconocer el aspecto físico de los diferentes equipos que emulamos; sería una pena, un desperdicio y a la vez contraproducente, en este caso, saber del funcionamiento y de la configuración de protocolos, tecnologías y servicios, y no saber al menos la configuración del cableado cruzado por decir un ejemplo; no seamos ese tipo de profesional. Por lo tanto, no debemos descartar por completo el uso de laboratorios con dispositivos físicos porque al final en nuestra vida laboral las utilizaremos.

Tenemos con esto, una gran oportunidad como carrera de ingeniería en redes de explotar las distintas combinaciones de laboratorios tanto virtuales y físicos, dando así una puerta de posibilidades a los nuevos integrantes. De esta manera podemos ver este potencial con dos tipos de perspectiva:

1. Apertura del espacio de tiempo para trabajos grupales para laboratorios de red.
2. Creación de ambientes para el laboratorio de seguridad informática.

Las dos son válidas para la realización y la expansión de la carrera en cuestión de asignaturas, dando así, el dinamismo necesario para el aprendizaje de cada uno.

Una implementación en la nube sería también una alternativa para no gastar nuestros recursos informáticos y aprovecharlos de otra manera, pero existe un detalle, el costo de contratación de este tipo de servicios depende mucho de la empresa prestadora y la mayoría cobran por hora.

Para finalizar, este plan pretende dar una nueva escala y dinamismo a la experimentación de los diferentes tipos de tecnologías, servicios y protocolos que hay en el mundo de la computación y al mismo tiempo alcanzar la rama de seguridad que hoy en día está siendo objeto de interés de forma masiva y no sería justo abrir de una u otro modo un espacio para éste mismo.

Referencias

Almehmadi, A., & El-Khatib, K. (07 de mayo de 2015). On the Possibility of Insider Threat Prevention Using Intent-Based Access Control (IBAC). Oshawa, Ontario, Canadá.

Bishop, M. (2005). The Basic Components. En M. Bishop, *Introduction to COMPUTER SECURITY* (págs. 1-4). Boston: Addison-Wesley.

Bombal, D. (12 de julio de 2017). *Switching and GNS3.* Obtenido de GNS3 Documentation: https://docs.gns3.com/1aQSkL4KyIh-3j-UCeuukj4Wg1VJ7uI-vwcewaUHbjbU/

Bombal, D., & Duponchelle, J. (04 de enero de 2018). *Getting Started with GNS3.* Obtenido de GNS3 Documentation: https://docs.gns3.com/1PvtRW5eAb8RJZ11maEYD9_aLY8kkdhgaMB0wPCz8a38/

Bombal, D., & Duponchelle, J. (25 de enero de 2018). *GNS3 Setup wizard with the GNS3 VM.* Obtenido de GNS3 Documentation: https://docs.gns3.com/1wdfvS-OlFfOf7HWZoSXMbG58C4pMSy7vKJFiKKVResc/

Bombal, D., & Julien, D. (06 de febrero de 2017). *Which emulator should I use?* Obtenido de GNS3 Documentation: https://docs.gns3.com/1o4IX8nXISl5gb4BwoSFrUht3MeTjkzHM1TCeWAe669g/index.html

Bombal, D., Duponchelle, J., & Ganancial, R. (02 de febrero de 2018). *Windows Intallation.* Obtenido de GNS3 Documentation: https://docs.gns3.com/11YYG4NQlPSl31YwvVvBS9RAsOLSYv0Ocy-uG2K8ytIY/

Ciobanu, C. (15 de abril de 2015). *What functions IOU not support?* Obtenido de GNS3 Discussions: https://www.gns3.com/discussions/what-functions-iou-not-support

Cisco Systems. (29 de septiembre de 2015). *Cisco IOS XRv 9000 Router Data Sheet.* Obtenido de Cisco Systems: https://www.cisco.com/c/en/us/products/collateral/routers/asr-9000-series-aggregation-services-routers/datasheet-c78-734034.html

Cisco Systems. (09 de agosto de 2017). *Cisco Adaptive Security Virtual Appliance (ASAv) Data Sheet.* Obtenido de Cisco Systems: https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/datasheet-c78-733399.html

Cisco Systems. (20 de octubre de 2017). *Cisco Adaptive Security Virtual Appliance (ASAv) Quick Start Guide, 9.4, Chapter: Introduction to the Cisco ASAv.* Obtenido de Cisco Systems: https://www.cisco.com/c/en/us/td/docs/security/asa/asa94/asav/quick-start/asav-quick/intro-asav.html

Cisco Systems. (08 de enero de 2018). *Chapter: NX-OSv 9000: NX-OSv 9000 Software Functionality.* Obtenido de Cisco Systems: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/nx-osv/configuration/guide/b_NX-OSv_9000/b_NX-OSv_chapter_01.html#reference_BAD5B5587C6B45AAB2FA462759DCCBD0

Duponchelle, J. (05 de diciembre de 2016). *What's new in GNS3 1.4.* Obtenido de GNS3 Documentation: https://docs.gns3.com/1E8V7wcENH7FV99N8y6rgMbtJFrUVyfwvq06cRpIa8NI/index.html

Duponchelle, J. (17 de diciembre de 2017). *Cisco IOS images for Dynamips.* Obtenido de GNS3 Documentation: https://docs.gns3.com/1-kBrTplBltp9P3P-AigoMzlDO-ISyL1h3bYpOl5Q8mQ/

González Pérez, P., Sánchez Garcés, G., & Soriano de la Cámara, J. M. (2015). Introducción a Kali Linux. En P. González Pérez, G. Sánchez Garcés, J. M. Soriano de la Cámara, & J. Ramón Jiménez (Ed.), *Pentesting con Kali 2.0* (pág. 13). Madrid, Móstoles, España: 0xWORD Computing S.L.

Grossmann, J., & Saraiva, F. (12 de marzo de 2016). *GitHub GNS3/dynamips.* Obtenido de GitHub Inc: https://github.com/GNS3/dynamips/blob/master/README.hypervisor

Hassan, N. A., & Hijazi, R. (2017). What Is Digital Privacy? En N. A. Hassan, & R. Hijanzi, *Digital Privacy and Security Using Windows: A Practical Guide* (pág. 6). New York: Apress.

IBM. (27 de febrero de 2014). *Componentes de la alta disponibilidad*. Obtenido de IBM Knowledge Center: https://www.ibm.com/support/knowledgecenter/es/ssw_ibm_i_72/rzarj/rzarjhacomponents.htm

Jain, A. (17 de junio de 2013). *Unifying identity management and access control*. Obtenido de SourceSecurity.com: Making the world a safer place: https://www.sourcesecurity.com/news/articles/co-2415-ga.9535.html

Polanco, M. (06 de marzo de 2013). *¿Y usted ya está evaluando la resiliencia de su infraestructura?* Obtenido de Magazcitum: El magazine para los profesionales de la seguridad de TI: http://www.magazcitum.com.mx/?p=2105

Reyes Krafft, A., Solís, C., Torres, H., Gabriela, R., Vera Vallejo, L., Reyes, A., . . . Puyol Montero, J. (18 de noviembre de 2016). *LAS BRECHAS DE SEGURIDAD*. Obtenido de Lex Informática: Derecho informático y propiedad intelectual / Protección real en el Entorno Digital: http://www.lexinformatica.co/2016/11/18/las-brechas-de-seguridad/

Stamp, M. (2011). INFORMATION SECURITY Principles and Practice. En M. Stamp, *INFORMATION SECURITY Principles and Practice* (págs. 2-3, 6, 265, 274-276, 278, 279, 281, 285-292). New Jersey: WILEY.

The Cisco Learning Network Store. (04 de octubre de 2016). *Virtual Internet Routing Lab: Features.* Obtenido de Cisco: The Cisco Learning Network Store: https://learningnetworkstore.cisco.com/virlfaq/features

The Cisco Learning Network Store. (25 de enero de 2018). *Cisco Virtual Internet Routing Lab Personal Edition (VIRL PE) 20 Nodes.* Obtenido de Cisco: The Cisco Learning Network Store: https://learningnetworkstore.cisco.com/virtual-internet-routing-lab-virl/cisco-personal-edition-pe-20-nodes-virl-20

Ulbrich, C. E., & Della Valle, S. (2004). La negligencia de las empresas. En C. E. Ulbrich, & S. Della Valle, *Universidad Hacker* (pág. 19). São Paulo: Digerati Comunicación y Tecnología Ltda.

Waschke, M. (2017). How Does Computer Security Work? En M. Waschke, *Personal Cybersecurity: How to Avoid and Recover from Cybercrime* (pág. 73). New York: Apress.

Waschke, M. (2017). What's Biting Us? En M. Waschke, *Personal Cybersecurity: How to Avoid and Recover from Cybercrime* (págs. 1, 5-25). New York: Apress.

Welsh, C. (20 de febrero de 2013). *Dynamips/GNS3 Idle-PC explained. Finally!* Obtenido de RedNectar's Blog: https://rednectar.net/2013/02/24/dynamipsgns3-idle-pc-explained-finally/

Welsh, C. (06 de julio de 2013). *How the GNS3 Hypervisor Manager Works?* Obtenido de RedNectar's Blog: https://rednectar.net/2013/07/06/how-the-gns3-hypervisor-manager-works/

Anexos

Integración de built-in en GNS3.

Si ya no tenemos percances con el inicio de GNS3 seguimos con la creación de la primera topología con appliances que tiene por defecto.

1. Primeramente, cerramos la ventana de “Setup Wizard” cuando abrimos el programa por primera vez, esta sirve para la guía automatizada de instalación de imágenes tanto en servidor local o en GNS3 VM.

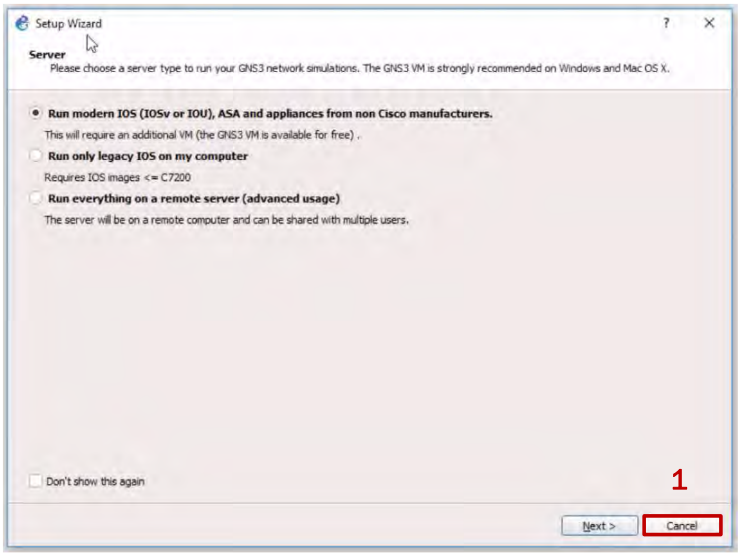

Figura 27. Cancelación de integración guiada.

2. Seguidamente vamos a la pestaña “File” y seleccionamos “New blank project” para crear un nuevo proyecto y topologías consiguientemente.

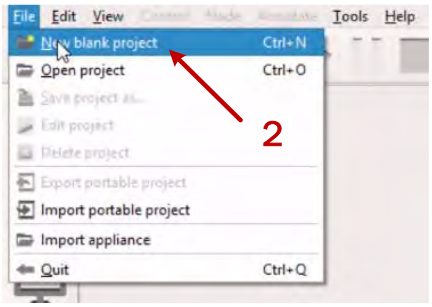

Figura 28. Creando un nuevo proyecto.

3. Nos aparecerá una nueva ventana la cual nos solicitará el nombre de proyecto que le queramos dar y la ruta donde se guardará, ésta última lo dejamos por defecto. Cuando tengamos un proyecto creado los botones “Open a project from disk” y “Recent projects” nos permitirá abrir trabajos que tengamos guardado en disco y abrir los recientes con las que hayamos empleado. Presionamos “Ok” para crearlo.

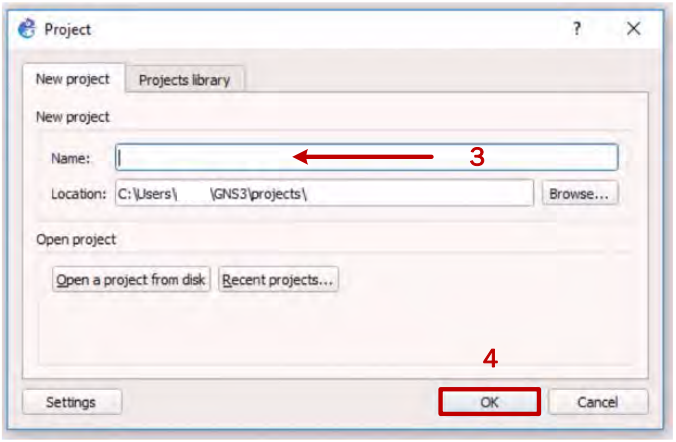

Figura 29. Definiendo nombre y ruta de proyecto.

4. Una vez creado nuestro primer proyecto veremos que nuestra área de trabajo se encuentra en blanco, y del lado izquierdo se encuentran las categorías de dispositivos de red, y en cada uno estarán listadas las diferentes appliances que tengamos instalados. Por el momento GNS3 tiene instalados sus dispositivos por default, estas se tratan de las built-ins.

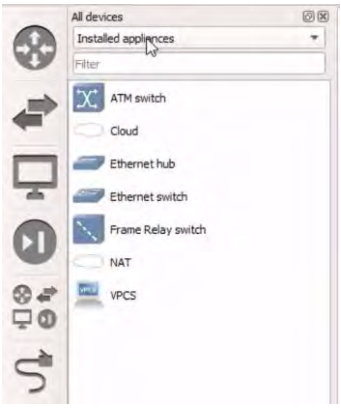

Figura 30. Appliances por defecto.

5. Arrastramos un ethernet switch y dos VPCS para crear una topología básica con el objetivo de dar una demostración. Seleccionamos el último símbolo que es de conexión entre dispositivos; seleccionamos la tarjeta de red virtual correspondiente y conectamos.

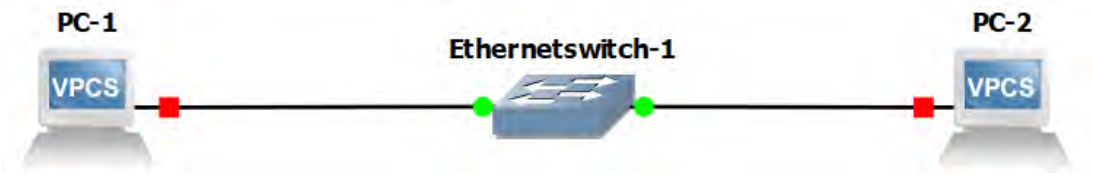

Figura 31. Topología con built-in de GNS3.

6. Corremos los tres dispositivos al mismo tiempo con el ícono y damos pie a configurar los VPCS. Para suspenderlos con haga uso del ícono , para detener el proceso de emulación con el icono , y para recargar o reiniciarlos con el ícono .

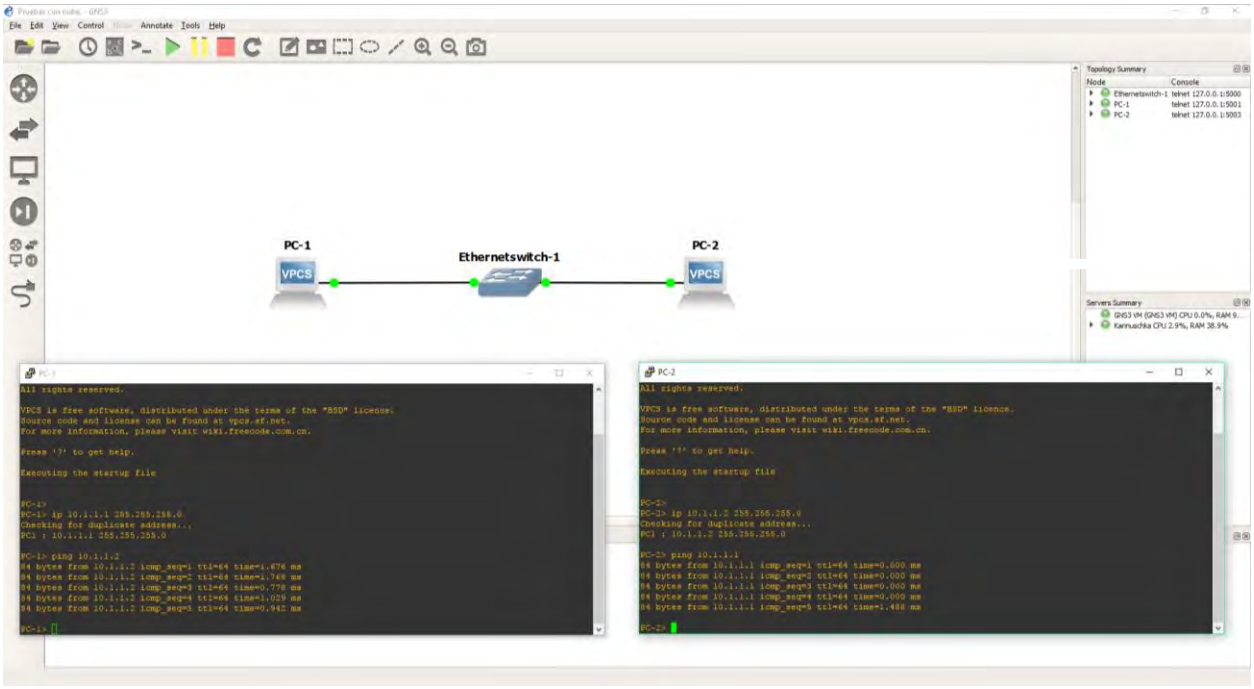

Figura 32. Conexión exitosa.

Integración de appliances Cisco IOS con dynamips.

Una vez sabiendo los pasos necesarios para la integración de un built-in de GNS3, podemos trabajar con topologías básicas y crear nuevos proyectos. Ahora, podemos con más facilidad unir un appliance de cualquier tipo y fabricante, pero esta vez veremos cómo instalar un IOS de Cisco.

Cuando iniciamos con la creación de un proyecto vimos que para colocar un dispositivo de GNS3 solo bastaba con arrastrar el appliance para agregarlo al área de trabajo, en este caso es un poco diferente ya que, si lo realizamos de esta forma, nos pedirá directamente el binario ya expandido, es decir, en formato “.image”. Por este motivo las instrucciones serán un poco más largas, pero más completas.

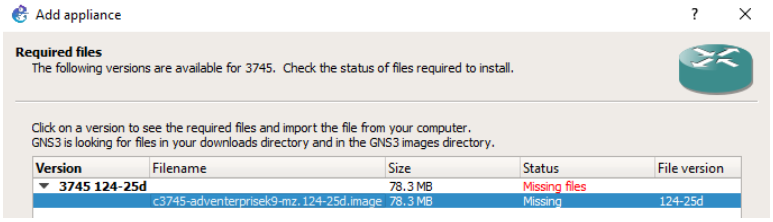

Figura 33. Solicitud directa de binario descomprimido.

1. Seleccionamos la pestaña “Edit” y luego a “Preferences”, con esto podemos editar las preferencias del servidor local tales como cambiar de tema, cambiar rutas de proyectos, editar comandos de inicio análisis de red etc., entre ellas está la de agregar diferentes appliances.

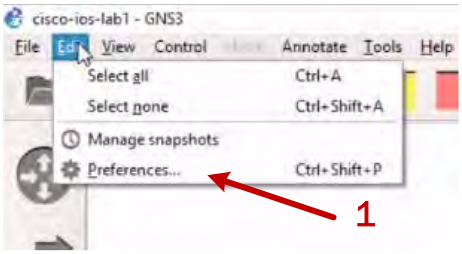

Figura 34. Editar las preferencias de GNS3.

2. Inmediatamente nos saltará la ventana de preferencias y nos dirigimos directamente a la lista de “IOS routers” bajo la sección de dynamips y observamos que nuestra lista está vacía ya que no hemos agregado ningún appliances de Cisco y de ningún otro fabricante. Damos clic en “New” para integrar el dispositivo virtual al área.

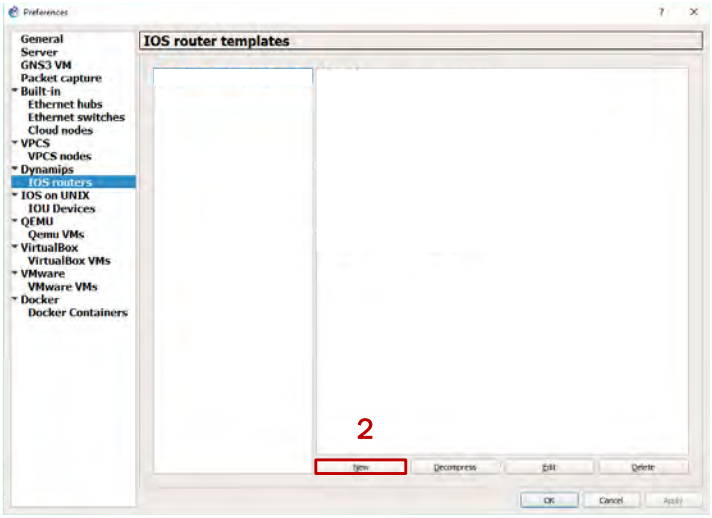

Figura 35. Añadiendo nuevo appliance.

3. Continuamente, nos saldrá una ventana indicándonos si queremos agregar una imagen existente o una nueva, en este caso seleccionamos en “New image”. Después de elegir esa opción, damos clic en “Browse” para buscar nuestro binario que queramos y que esté soportado o recomendado por GNS3 y dynamips.

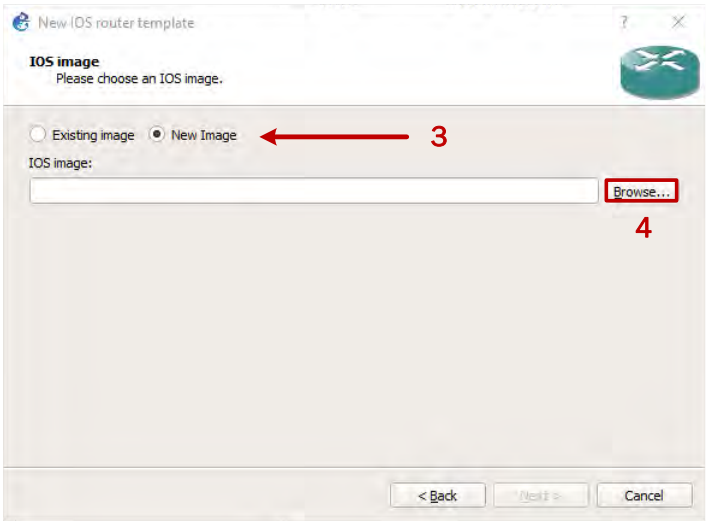

Figura 36. Busca del binario.

Aviso: Recordemos que para adquirir estos binarios es necesario tener permisos suficientes para poseer de ellos y evitar cuestiones legales.

4. Buscamos en el directorio el binario correspondiente, lo seleccionamos y damos clic en “Abrir”. En nuestro caso será un “c3725-adventerprise-mz.124-15.T14.bin”.

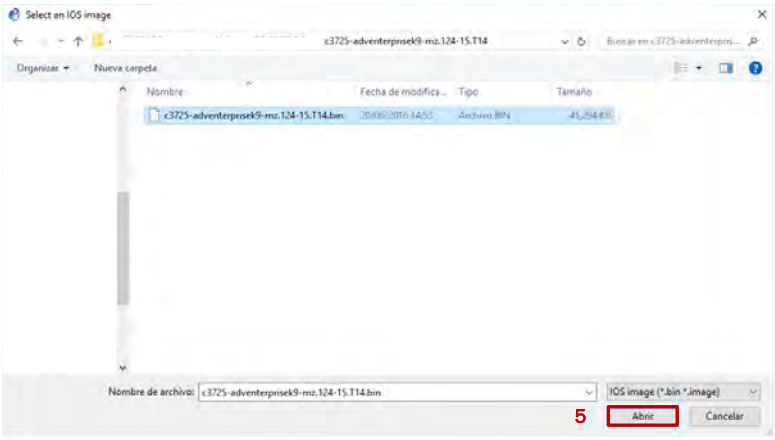

Figura 37. Selección de binario.

5. Ya seleccionado y abierto, continuamos con la expansión del binario. GNS3 nos preguntará si queremos descomprimir esta imagen IOS, por lo tanto, damos clic en “Yes”.

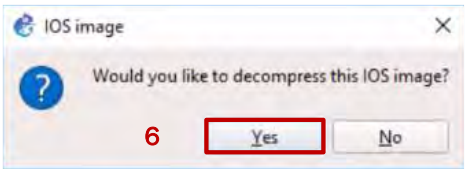

Figura 38. Solicitud de descomprensión de binario.

El programa automáticamente nos descomprimirá el binario como se muestra en la siguiente figura.

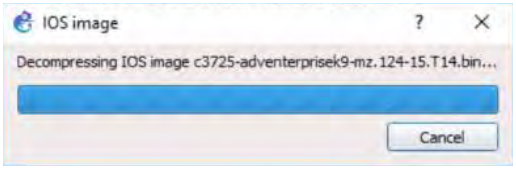

Figura 39. Descomprimiendo binario.

6. Luego de descomprimir el binario nos quedara con el formato “.image”. Damos clic en “Next” para proseguir con la integración.

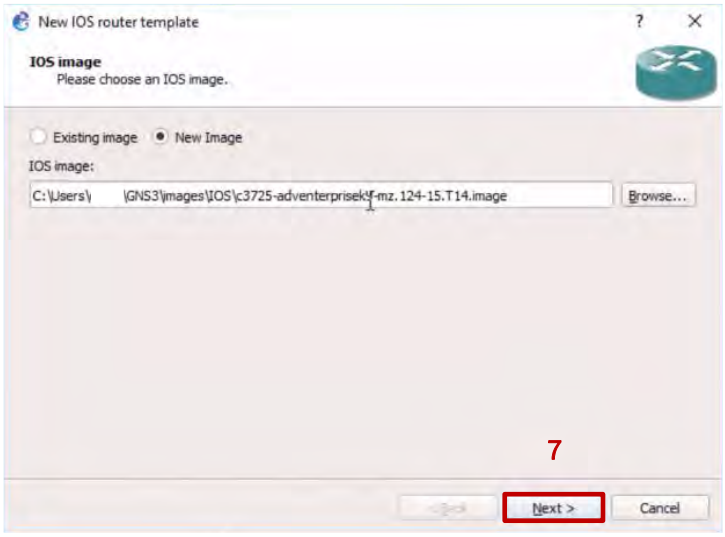

Figura 40. Binario descomprimido.

7. Nos saldrá la opción de cambiar de nombre al nuevo appliance, también nos ofrecerá la opción de plataforma y de chasis, esto quiere decir que dynamips emulará también las características de hardware del modelo elegido, así mismo, nos dará la libertad de elegir si queremos integrarle el módulo de etherswitch, si deseamos hacerlo solo basta marcar la casilla “This is an etherswitch router” y con ello tener capacidades básicas de conmutación. En nuestro caso lo dejamos por defecto y damos clic en “Next” para continuar.

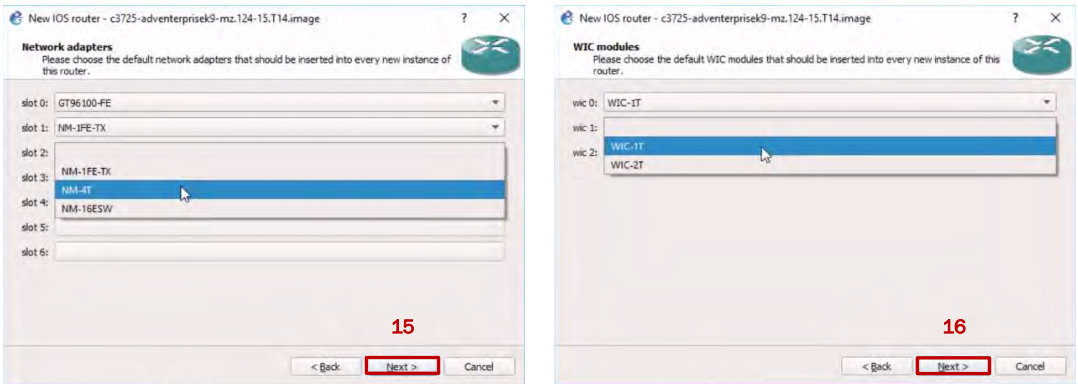

Figura 41. Configurando appliance.

8. Es importante revisar el mínimo de RAM requerido por el appliance para que dynamips pueda ejecutar la imagen. Para ello damos clic en el enlace “Check for minimum and maximum RAM requirement”.

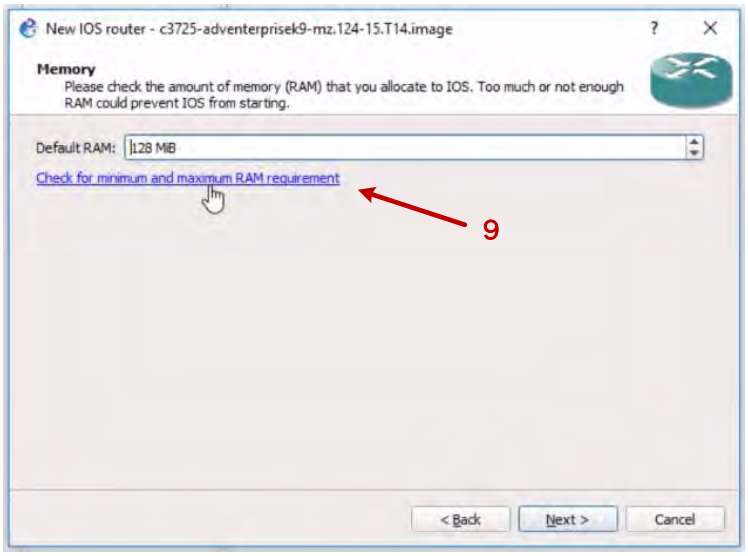

Figura 42. Revisión de mínimo de RAM.

9. Nos abrirá nuestro navegador y nos redirigirá hacia una extensión de Cisco dedicada a la búsqueda de los mínimos requerimientos para cierto binario. El enlace en sí nos guiará a la siguiente dirección http://cfn.cloudapps.cisco.com/ITDIT/CFN/jsp/SearchBySoftware.jsp. En esta página seleccionaremos la opción “Image Name” de este modo buscaremos dichas especificaciones con base al nombre del binario, por consiguiente, una vez seleccionado la opción copiamos el nombre de nuestro binario y procedemos a buscar.

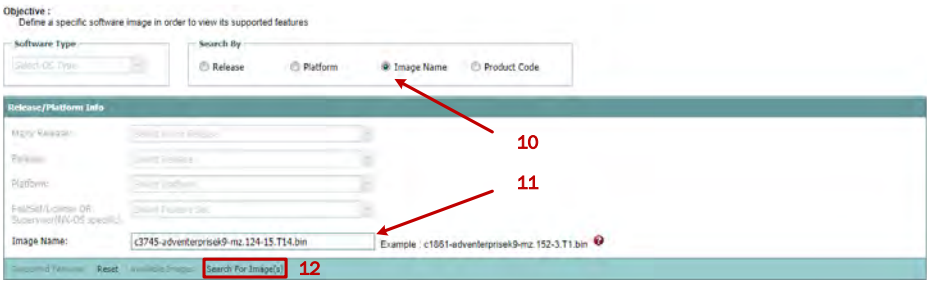

Figura 43. Buscando especificaciones.

10. Nos enlistará una serie de viarios binarios con el mismo nombre, pero con diferente finalidad cada uno, en nuestro caso se trata de la primera opción ya que corresponde con la nomenclatura, es decir, el binario es diseñado para servicios avanzados empresariales.

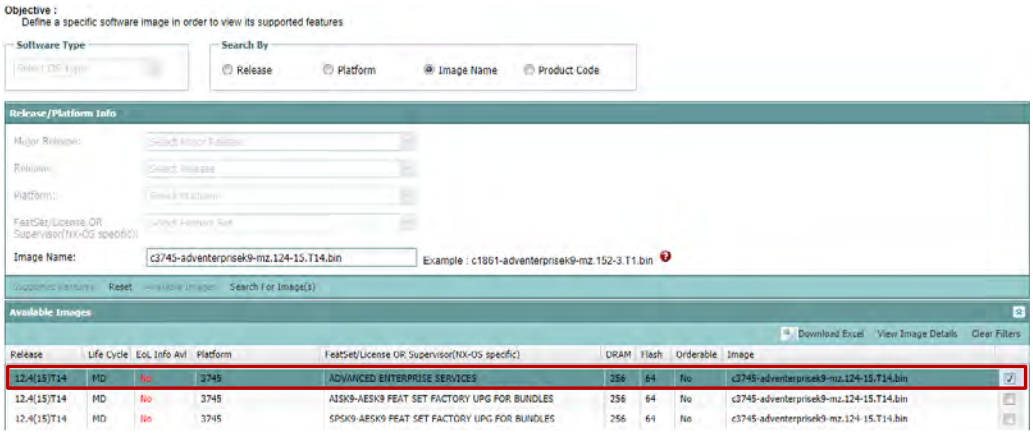

Figura 44. Especificaciones para appliance.

11. Como podemos ver en la figura anterior, nos indica que nuestro appliance junto con la imagen funciona con un mínimo de 256 MiB de RAM, de esta manera corregimos el detalle de memoria mínima en el programa. A continuación, damos clic en “Next” para seguir con el proceso.

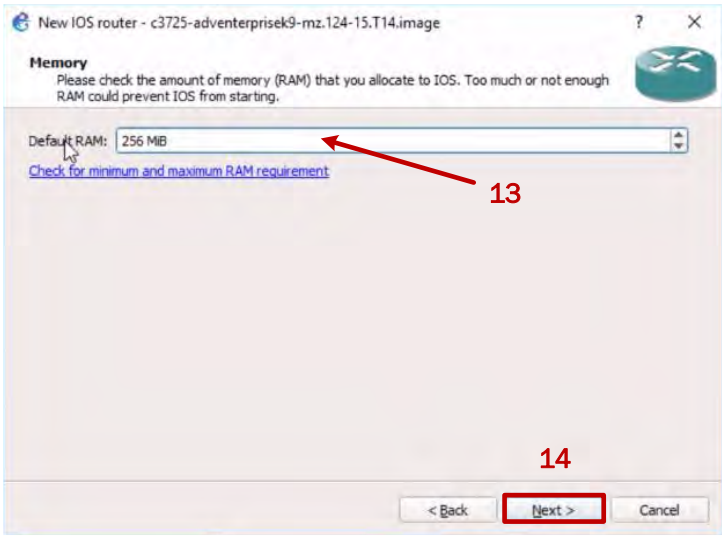

Figura 45. Modificando mínimo de RAM para appliance.

12. La siguiente ventana nos pedirá que configuremos los adaptadores de red que deseemos añadirle por cada slot virtual.

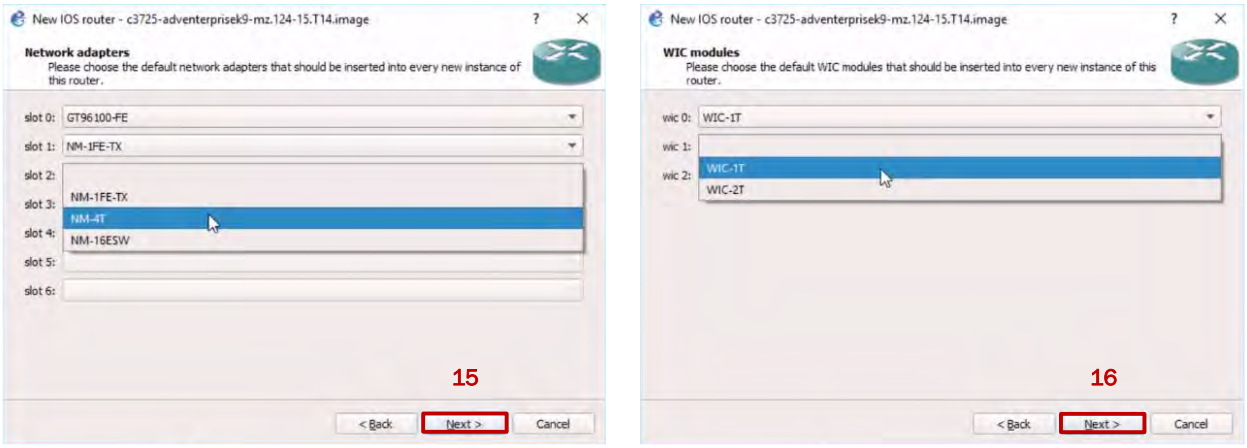

Figura 46. Añadiendo adaptadores de red.

13. Enseguida configuraremos la opción más importante de todos, se trata del valor para el Idle-PC que en el capítulo anterior explicamos para que funciona y cuál es su relevancia. Para calcular dicho valor, damos clic en “Idle-PC finder”, seguidamente damos clic en “Finish” para finalizar la integración.

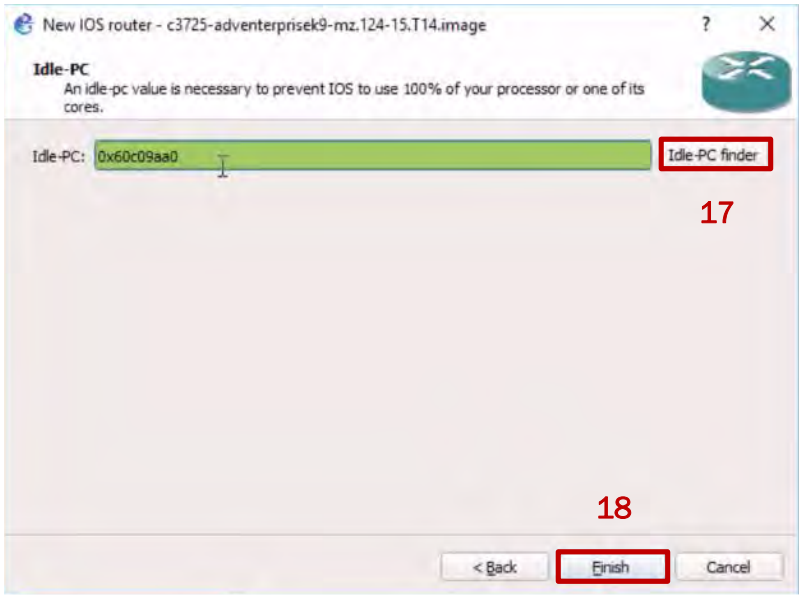

Figura 47. Finalizando integración de appliance.

Ahora, podemos combinar appliances de Cisco con los built-in de GNS3 para crear topologías un poco más completas, por ejemplo, podemos conectar un built-in ethernet switch con un appliance de Cisco emulado por dynamips como se muestra en la siguiente figura.

Figura 48. Combinación de dispositivos.

Tenemos en la lista de appliances disponibles a un enrutador con una imagen de servicios avanzados como sistema operativo de arranque y con plataforma y chasis del modelo de serie c3725 listo para ser emulado cuantas veces sea, arrastramos hacia el área de trabajo conectamos y configuramos. Una vez configurados probamos conectividad.

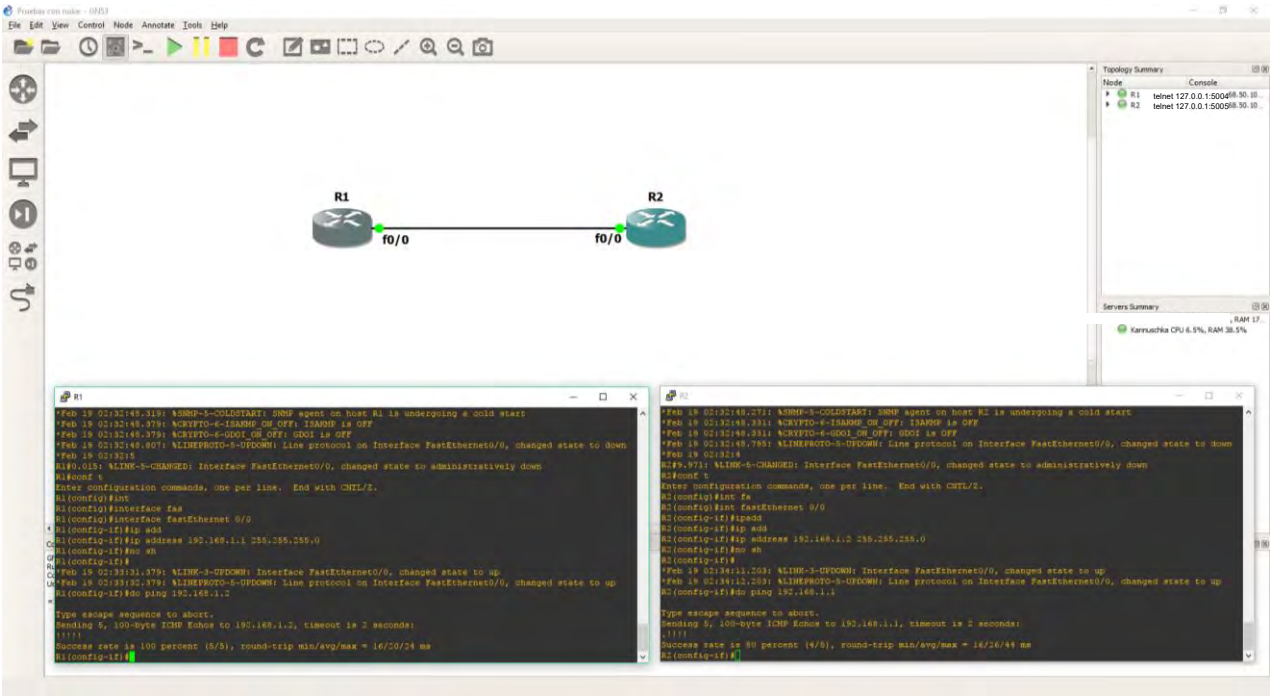

Figura 49. Conexión exitosa.

Integración de máquinas virtuales de Oracle VM VirtualBox.

Adicional a los ejemplos anteriores, GNS3 ofrece la posibilidad de colocar equipos virtuales con VirtualBox, con esto podemos realizar pruebas más completas y realistas junto con las demás integraciones que hemos visto.

Para poder hacer uso de ellas necesitamos primero haber instalado el programa Oracle VM VirtualBox, algo que no se mostrará en este documento porque se trata de un tema fuera del contexto principal. Pero lo que si se expondrá es la manera de suplir dichas máquinas virtuales en GNS3; los pasos son los siguientes:

1. En nuestro proyecto creado, abrimos la sección de appliances y damos clic en el símbolo  la cual es para los distintos tipos de equipos virtuales tanto de VirtualBox, VMware y QEMU. Seguidamente damos clic en “New appliance template” que está en la parte inferior de la lista. De inmediato nos saldrá una ventana en la cual nos pide que tipo de dispositivo queremos añadir al área de trabajo, seleccionamos “Add a VirtualBox virtual machine” y damos clic en “Ok”.

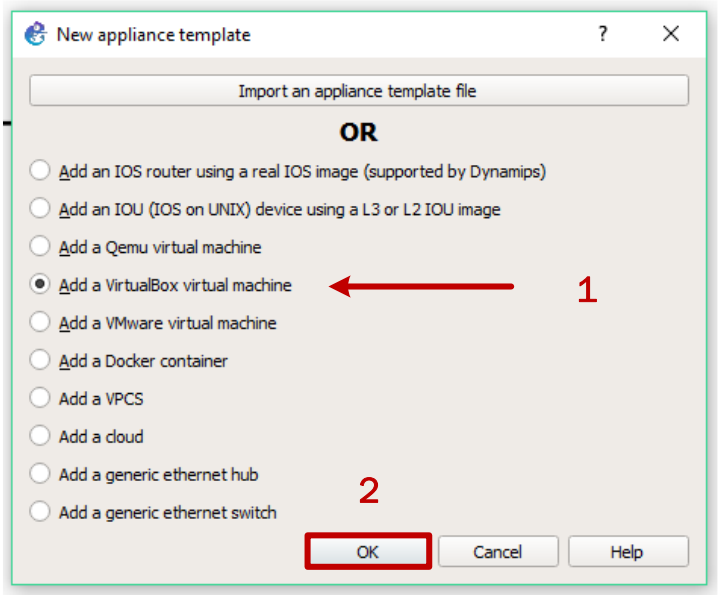

Figura 50. Opciones de tipo de appliance.

2. Nos mostrará una ventana y en ella nos pregunta si queremos correr esta máquina virtual en un equipo remoto o directamente en la computadora local, en este caso no tenemos hasta el momento configurado un servidor remoto, por lo cual, la primera opción esta desactivada y la segunda esta seleccionada automáticamente por defecto. Damos clic en “Next” para continuar.

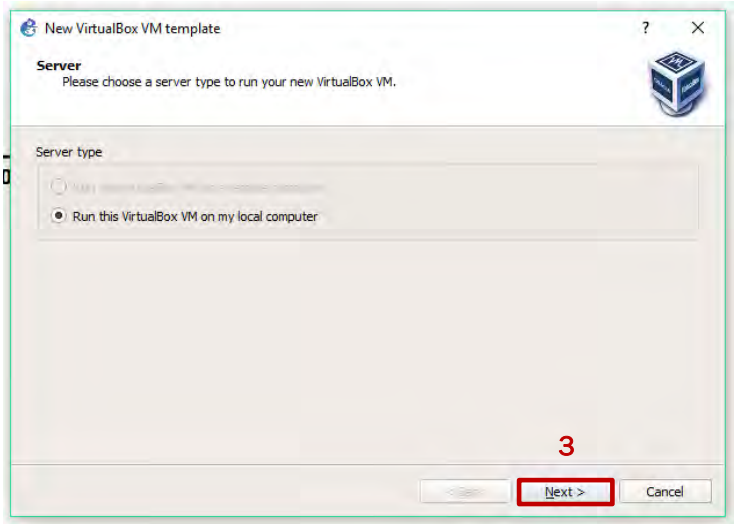

Figura 51. Ejecución en computadora local.

3. Lo que realizará GNS3 es que se conectará a VirtualBox para buscar y enlistar las computadoras virtuales que tengamos disponibles en ese momento.

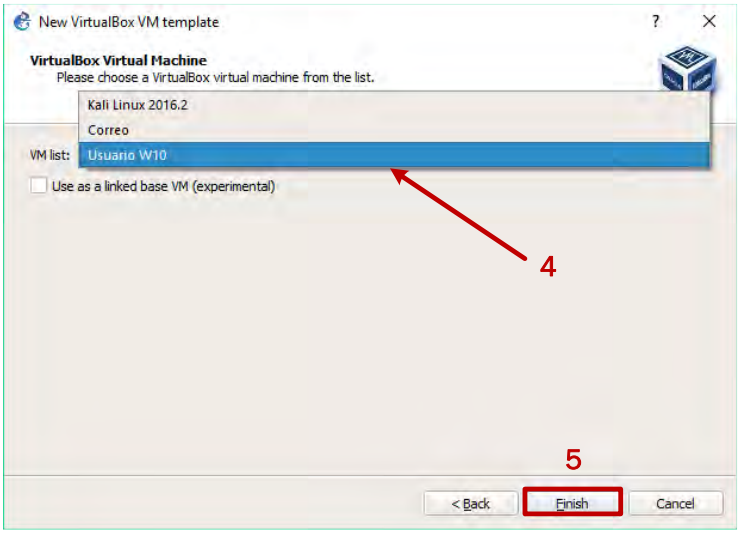

Figura 52. Selección de máquina virtual.

Es muy importante señalar que debemos de tener el equipo en modo apagado para que el proceso de integración funcione. Seleccionamos el equipo virtual y damos clic en "Finish" para finalizar la integración a GNS3.

4. Cuando finalizamos nos botará la lista de máquinas de VirtualBox agregadas recientemente, y si queremos editar sus preferencias como número y tipos de adaptadores de red, memoria RAM, nombre de host, ícono, categoría etc., damos clic en "Edit".

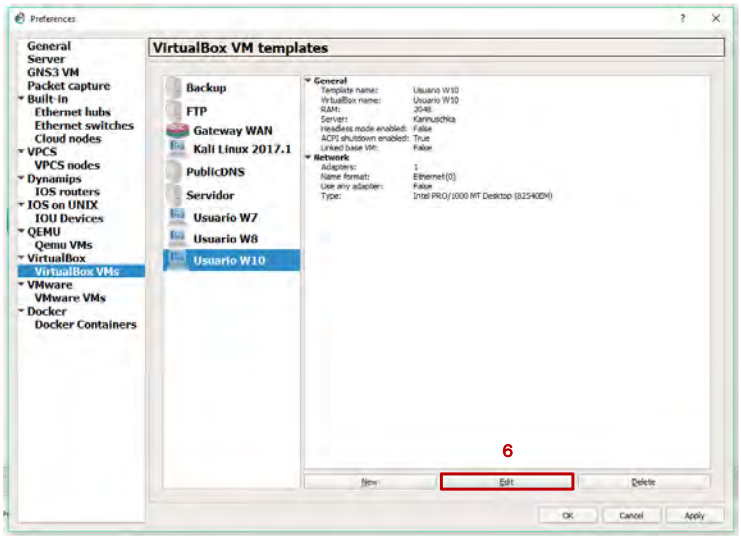

Figura 53. Editar preferencias máquina virtual.

Una vez editado la configuración de la máquina VirtualBox damos clic en "Ok" y de nuevo en preferencias para cerrar y completar la integración.

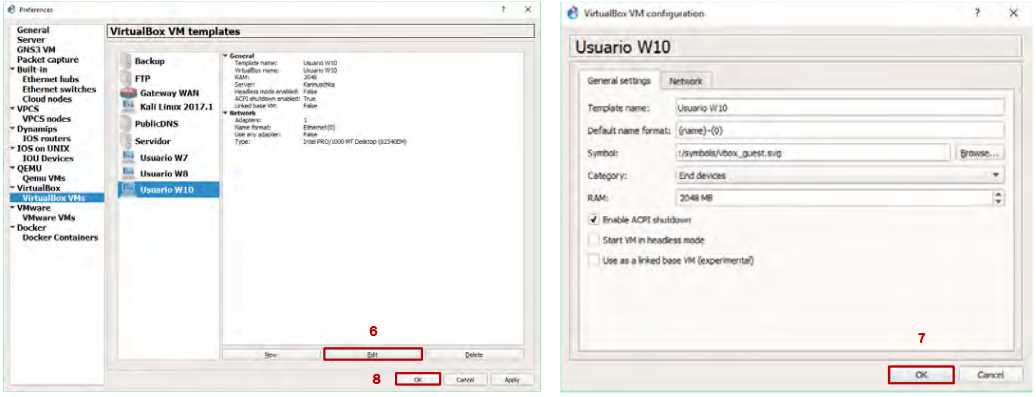

Figura 54. Completando integración.

5. Construimos nuestra pequeña topología con los appliances anteriores configurados y los conectamos a las máquinas virtuales. El ejemplo nos queda de la siguiente forma.

Figura 55. Topología de ejemplo con servidor local.

6. Configuramos y probamos conectividad.

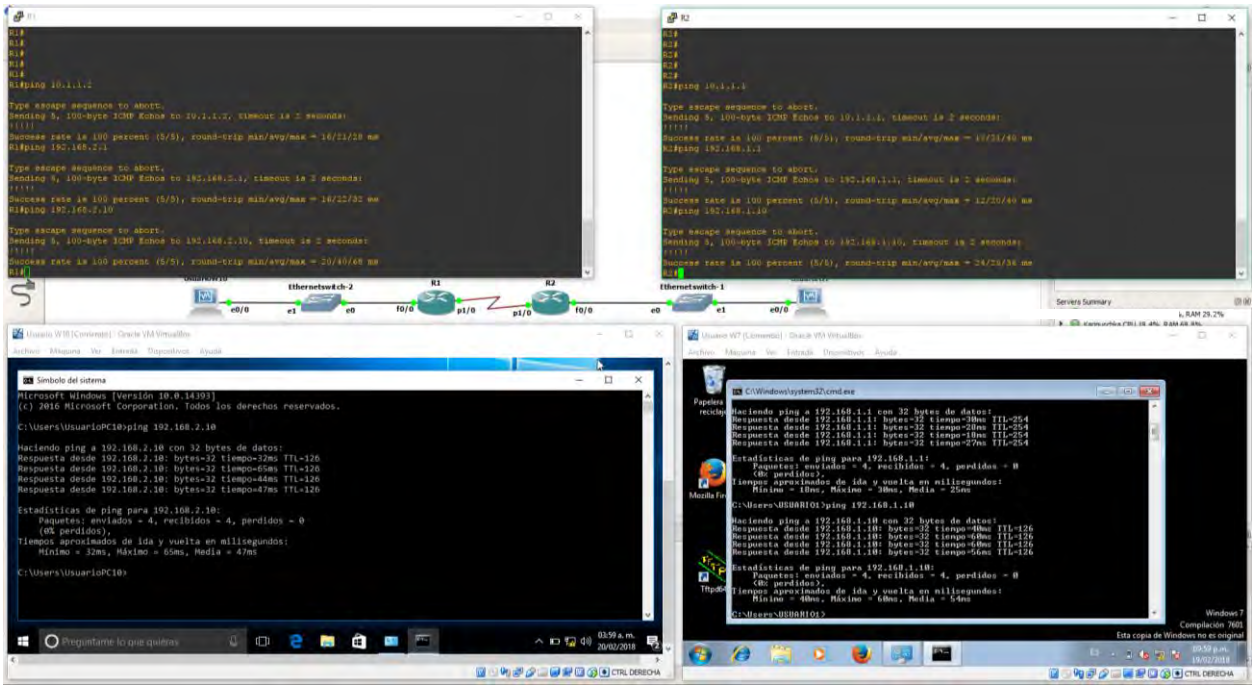

Figura 56. Conexión exitosa.

Integración de GNS3 VM.

Como se mencionaba reiteradas veces, GNS3 cuenta con un complemento el cual se vuelve meramente principal y necesario si queremos trabajar con topologías más largas y avanzadas, esto sucede así porque GNS3 VM da portabilidad a nuestros proyectos, más opciones de soporte de emulación y más soporte para nuevos tipos appliances tal como sucede con los IOSv.

La portabilidad a nuestros trabajos es porque en este sandbox almacena nuestras instancias que hemos colocado anteriormente y poderlos respaldar mediante varias formas como el copiado directo desde GNS3 VM o su exportación en un archivo OVA.

También mencionábamos que se recomienda VMware® sobre Oracle VM VirtualBox por el motivo de la virtualización anidada, por lo cual, se necesita de hacer uso de este hipervisor. Reiteramos que VMware® cuenta con varias versiones y la gran mayoría son de paga; si se da uso del sistema operativo OS X haga utilización de la versión Fusion, ahora si está en una plataforma de Microsoft Windows™ se recomienda la versión Workstation Pro. En caso de no contar con el presupuesto y decide usar la versión Workstation Player la cual es gratuita, pero antes necesitará de la instalación adicional de VMware VIX para que GNS3 VM funcione de manera correcta.

Sabiendo esto, mencionaremos los pasos para integrar GNS3 VM, no se mostrará los pasos de instalación de VMware® para no salirse del tópico principal.

1. Nos dirigimos al siguiente portal https://github.com/GNS3/gns3-gui/releases.

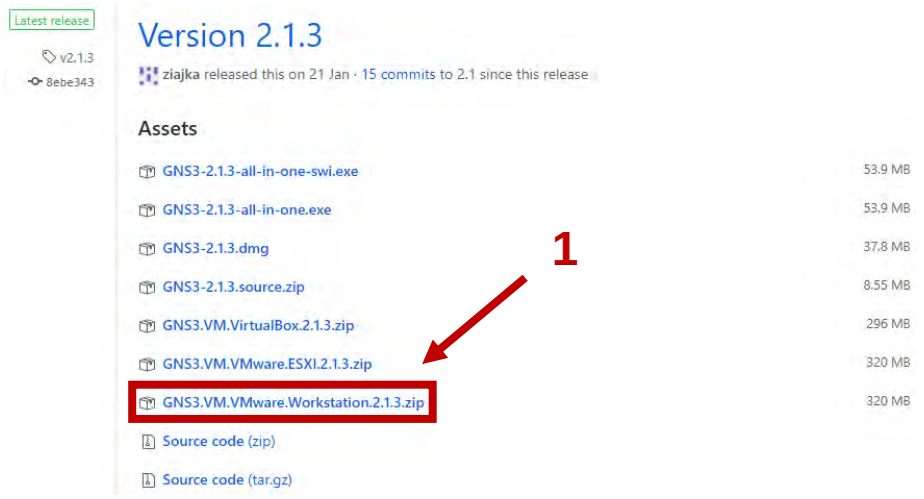

Figura 57. Versión estable y reciente de GNS3 VM.

Buscamos la versión más reciente, estable y compilado para nuestro tipo de hipervisor como se muestra en la figura 56; puede darse el caso que la versión en cuestión sea una beta y nos de problemas para trabajar, por tanto, no se recomienda dichas versiones.

Es muy importante marcar que la versión de GNS3 VM debe ser la misma que GNS3 para tener un funcionamiento óptimo.

2. Una vez descargado, disponemos a buscar en nuestro equipo, el directorio en donde se alojó GNS3 VM, veremos que se trata de un archivo compreso en formato y extensión ".zip", para poder descomprimirlo necesitaremos de programas como WinRAR o 7zip. Hacemos clic derecho y seleccionamos "Extraer aquí".

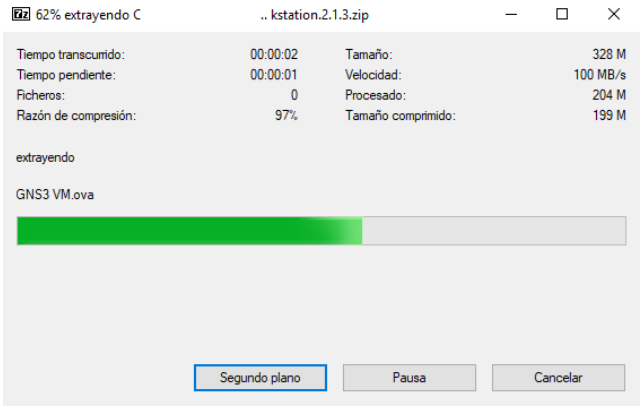

Figura 58. Extracción de archivo.

3. Veremos que se trata de un Archivo Abierto para Virtualización (OVF); ejecutamos nuestro VMware® (en nuestra situación utilizamos VMware Workstation Pro); damos clic en "File" y luego en "Open" o con la opción Ctrl + O, para poder importar el archivo al hipervisor.

Figura 59. Abrir directorio.

4. De inmediato nos abrirá una ventana para buscar nuestro directorio en donde alojamos nuestro GNS3 VM recién descargado. Damos clic en “Abrir”.

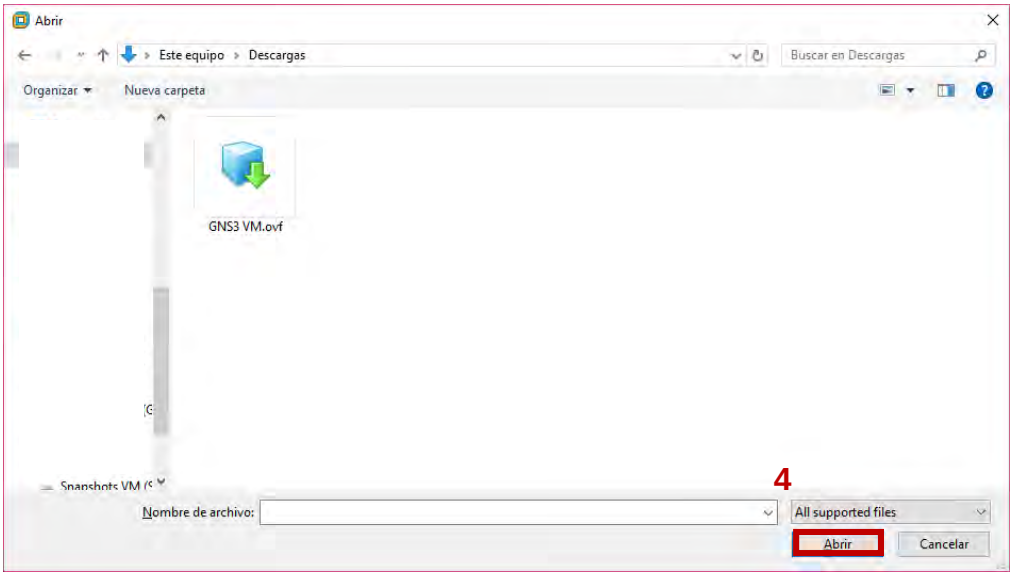

Figura 60. Abrir archivo.

5. Nos aparecerá dentro del programa una pequeña ventana en donde nos solicitará el nombre de la máquina virtual y la ruta en donde se estarán los archivos para virtualización. Es importante hacer mención que debe dejar esos valores por defecto porque GNS3 los toma directamente para detectar el nuevo tipo de servidor local. Damos clic en “Import” para iniciar el proceso de importación de GNS3 VM a VMware®.

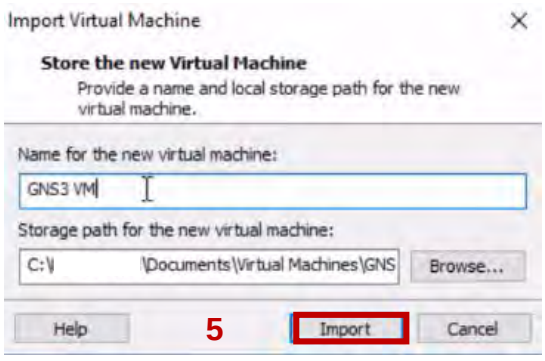

Figura 61. Configuración de nombre y ruta de GNS3 VM.

6. Se empezará la importación.

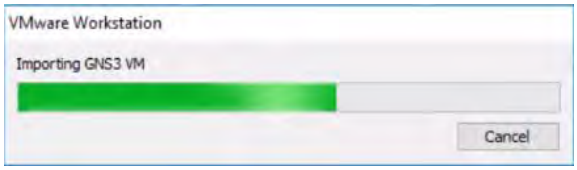

Figura 62. Importando GNS3 VM.

7. Siguientemente nos quedará de esta forma.

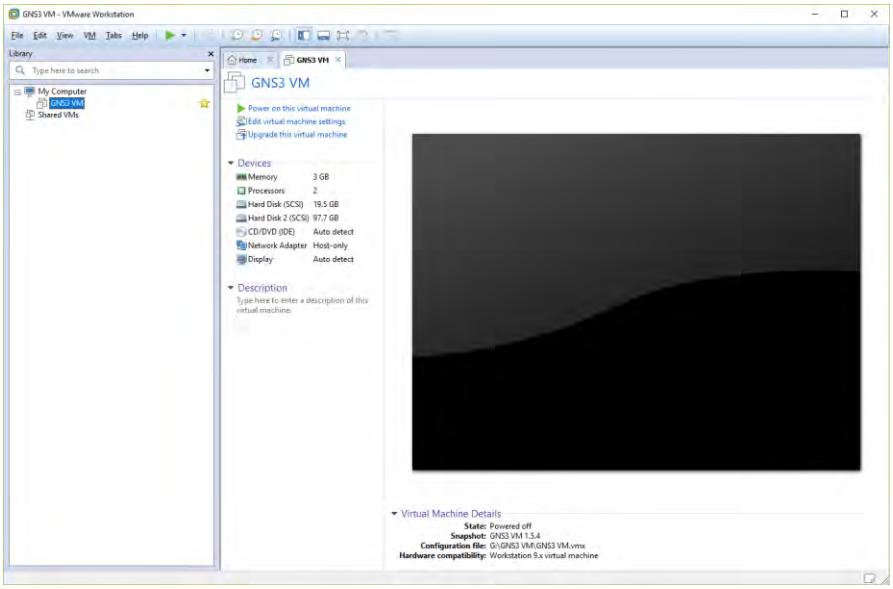

Figura 63. GNS3 VM en VMware®.

Podemos editar sus preferencias dependiendo el nivel de recursos informáticos que se obtenga.

8. Abrimos GNS3 y creamos un proyecto; nos dirigimos a editar las preferencias del programa, entre las listas de opciones esta la sección de GNS3 VM, en ese mismo segmento está la opción de marcar la casilla para la activación del componente; marcamos, damos en “Refresh” para que GNS3 detecte la máquina, en caso de no detectar reiniciamos el programa; después podemos editar la cantidad de memoria RAM, número de CPU virtuales y acciones después de cerrar GNS3. Posteriormente damos en “Apply” y en “Ok” para aplicar las configuraciones.

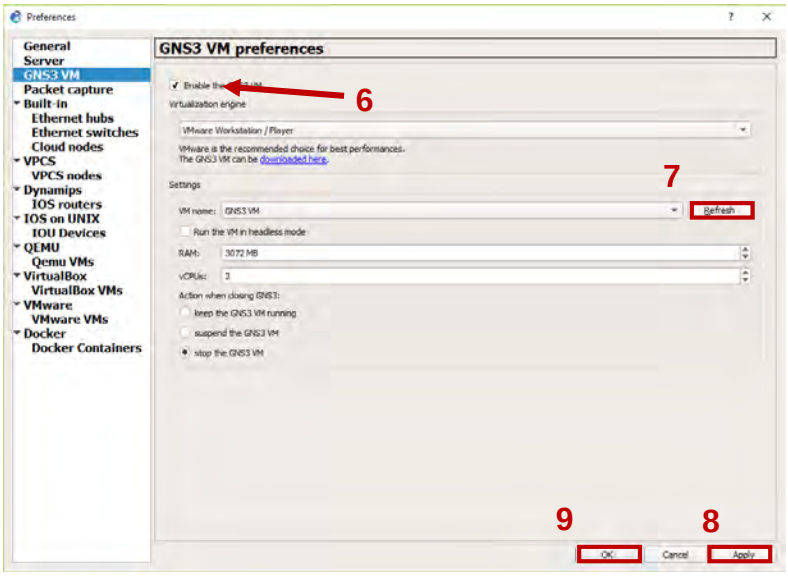

Figura 64. Edición de preferencias para GNS3 VM.

9. Enseguida se conectará hacia el host local y del lado derecho, específicamente en "Servers Summary" nos indicará que GNS3 VM está cargado y enlazado.

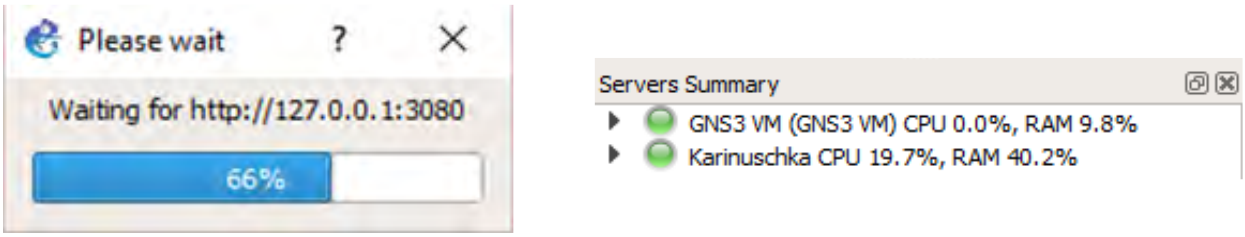

Figura 65. Integración exitosa de GNS3 VM.

Mientras se carga se iniciará la máquina virtual de GNS3 en VMware®. Su interfaz es como se muestra en la siguiente figura.

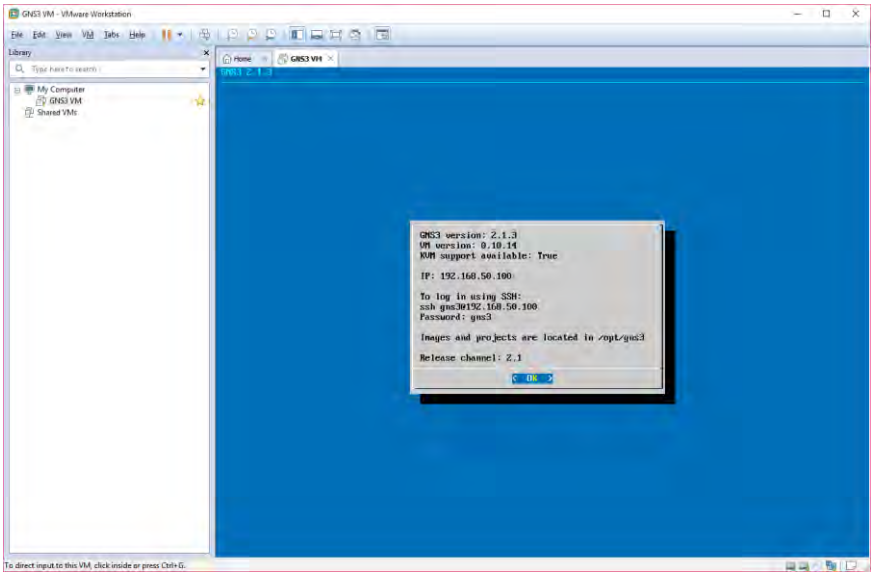

Figura 66. GNS3 VM.

Es importante recalcar de nuevo que es prescindible de activar tecnologías de virtualización como Intel VT-x/EPT o AMD-V/RVI en el BIOS para poder usar este componente.

De esta forma, ya tenemos la posibilidad de integrar más appliances disponibles por la Marketplace de GNS3 tales como imágenes QEMU, IOU y Docker, y crear así topologías más extensas y complejas.

Integración de appliances Cisco IOSv con QEMU.

Expuesto lo anterior, podemos hacer uso de las imágenes de Cisco VIRL en GNS3 por medio de su componente virtual. De esta manera podemos emplear configuraciones para protocolos y servicios más avanzados, particularmente para switching.

Ahora, cada vez que ejecutamos el programa se contactará con GNS3 VM para iniciarlo, además, cuando queramos arrastrar al área de trabajo distintos dispositivos virtuales que originalmente corren sin el componente, nos preguntará que tipo se servidor local usaremos para correrlo, si a nuestro host local o a GNS3 VM, tal como se aprecia en la figura 66.

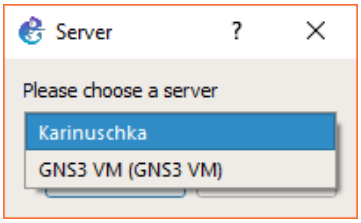

Figura 67. Opciones de servidor.

En este ejemplo vamos a mostrar los pasos para la integración de un IOSv al hipervisor de GNS3:

1. Creamos proyecto y damos clic en ícono  y nos listará los appliances que tenemos disponible; seleccionamos la opción de “Cisco IOSv” y arrastramos hacia el área de trabajo.

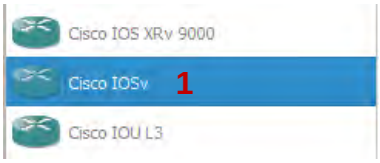

Figura 68. Appliance Cisco IOSvL2.

2. Nos saltará de inmediato la ventana de atributos del appliance.

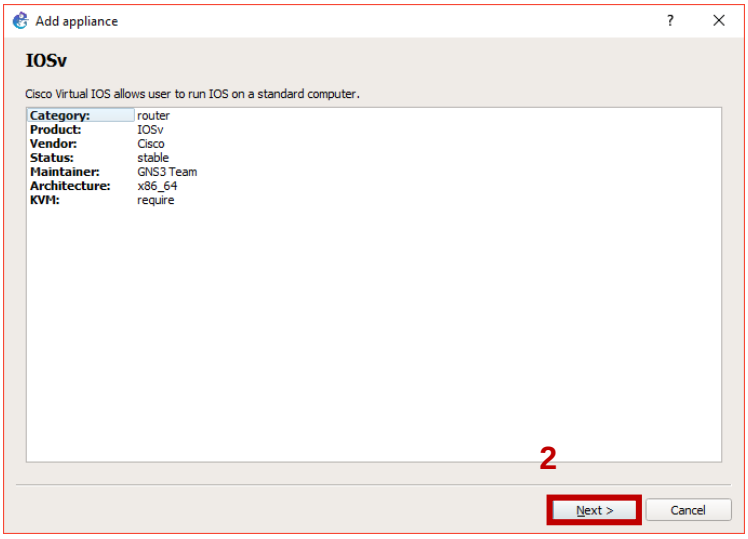

Figura 69. Atributos del appliance.

Damos clic en “Next” para continuar.

3. Como se trata de un appliance que se ejecutará con QEMU, las opciones de servidor solo estarán activadas para ser puestas en GNS3 VM. Damos clic en “Next” para continuar.

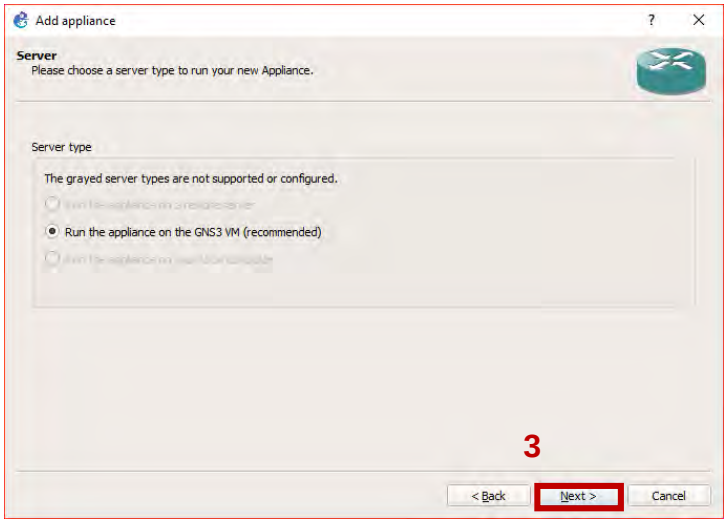

Figura 70. Tipos de servidor disponible.

4. Se enlazará de nuevo a GNS3 VM para comprobar los requisitos de virtualización anidada y después nos dirá que los requerimientos están en orden. Damos clic en “Next”.

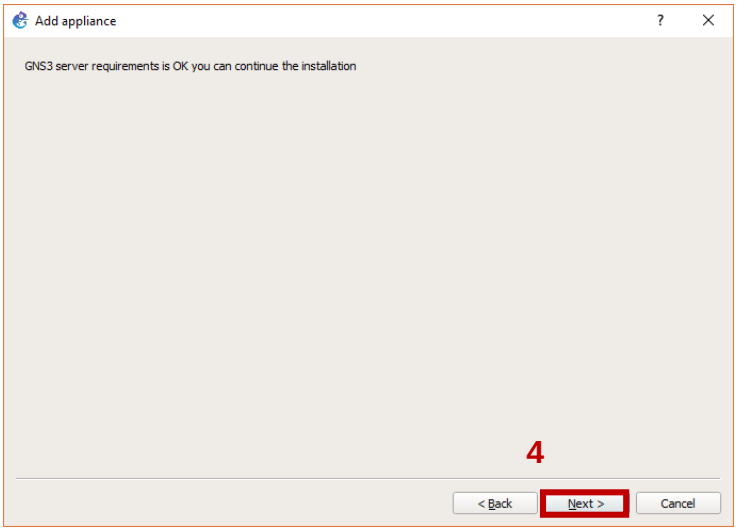

Figura 71. Requerimientos en orden.

5. Ahora, la ventana consecutiva nos expondrá los archivos que necesitamos para poder subir y emular las imágenes en GNS3 VM. Primeramente, seleccionamos "IOSv_startup_config.img"; damos clic en "Download" para descargar.

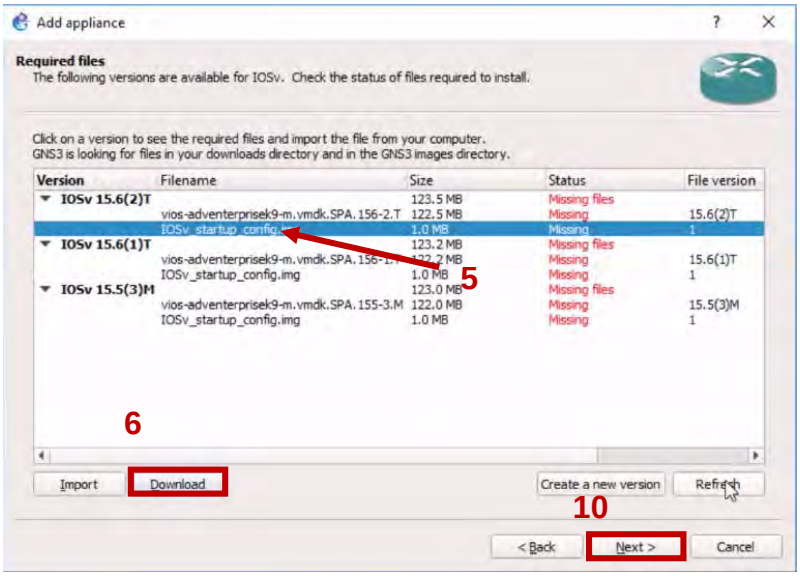

Figura 72. Archivos requeridos.

6. Se iniciará y abrirá el navegador que tengamos de preferencia y nos redirigirá a https://sourceforge.net/projects/gns-3/files/Qemu%20Appliances/IOSv_startup_config.img/download y se iniciará la descarga en cinco segundos.

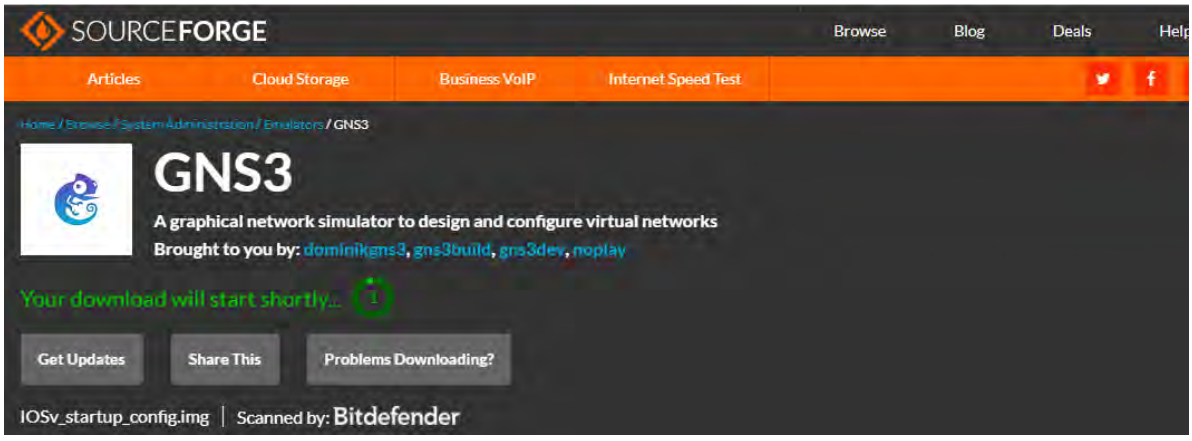

Figura 73. Descargando archivo.

7. Regresamos hacia la ventana de GNS3 y hacemos clic en “Import”.

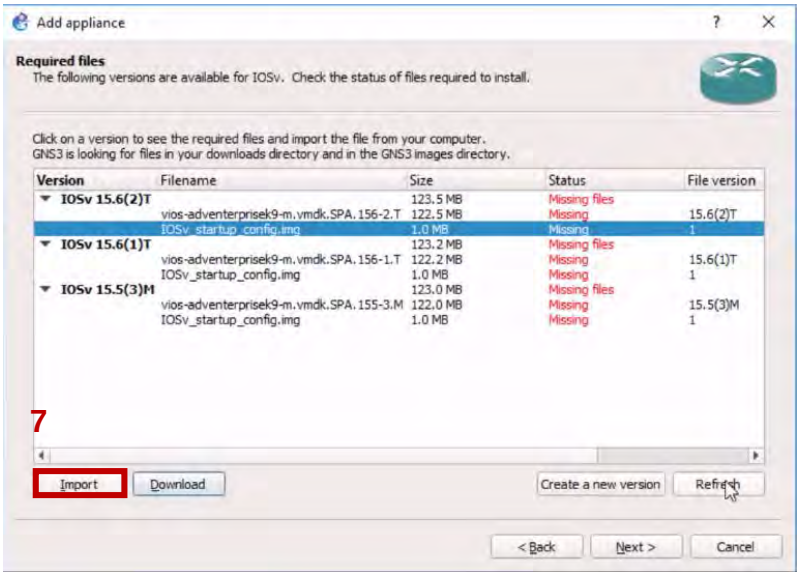

Figura 74. Archivos requeridos.

8. Seguidamente se nos abrirá la ventana de explorador para buscar y seleccionar nuestro archivo imagen. Este archivo funciona como controlador y nos permitirá precargar e iniciar el appliance. Damos clic en “Abrir”.

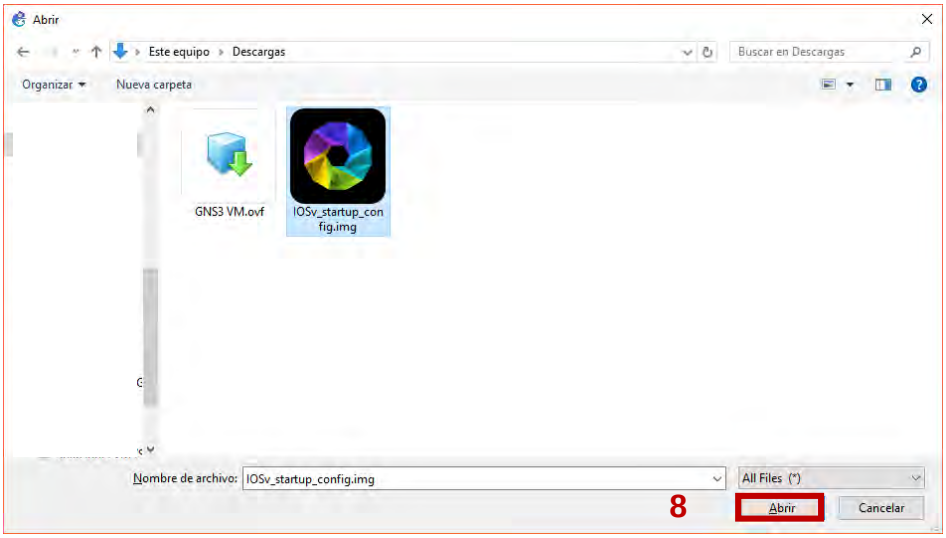

Figura 75. Abrir archivo.

9. Opcionalmente damos clic en “Refresh” para asegurarnos si el programa reconoce la importación. Una vez reconocido, nos dirá la leyenda “Found” en color verde; a continuación, seleccionamos nuestra imagen principal y de nuevo en “Download” para descargar el IOSv.

Aviso: Recordemos que para adquirir los diferentes IOSv, es necesario tener una suscripción anual de $199 USD para poseer de ellos y evitar cuestiones legales.

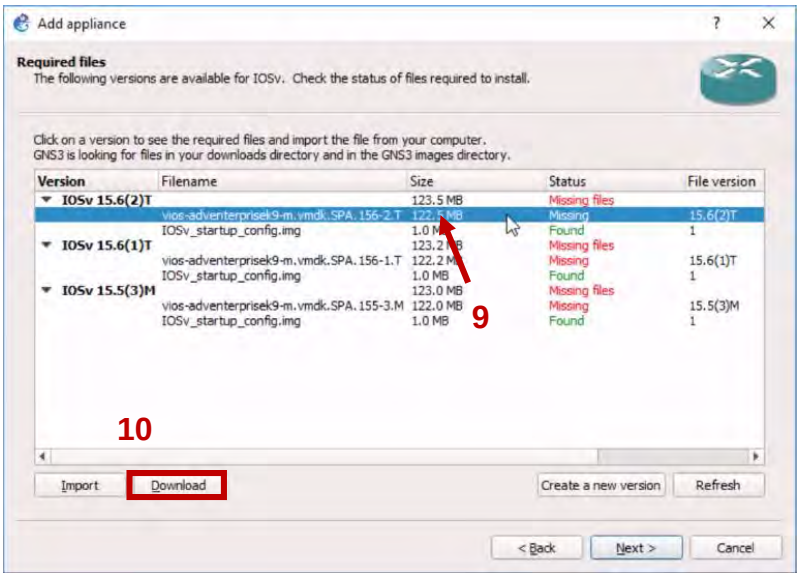

Figura 76. Seleccionando archivo principal.

10. Nos redirigirá de nuevo pero ahora hacia https://sso.cisco.com/autho/forms/CDClogin.html, el cual es la página de inicio de Cisco Systems®.

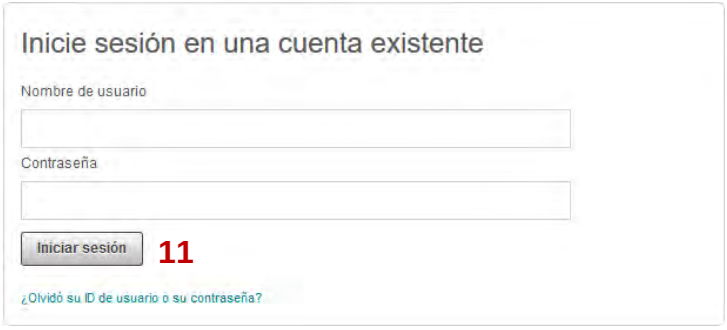

Figura 77. Inicio de sesión de Cisco Systems®.

Advertencia: Se recomienda usar Mozilla Firefox o Google Chrome para poder navegar sin problemas en la página de Cisco Systems® por motivos de seguridad y usabilidad, ya que, en navegadores diferentes suelen tener problemas hasta de visualización.

11. Iniciamos sesión y nos dirigimos hacia "Mi Cuenta", veremos que nos aparece la suscripción de VIRL. Daremos clic en "Download VIRL".

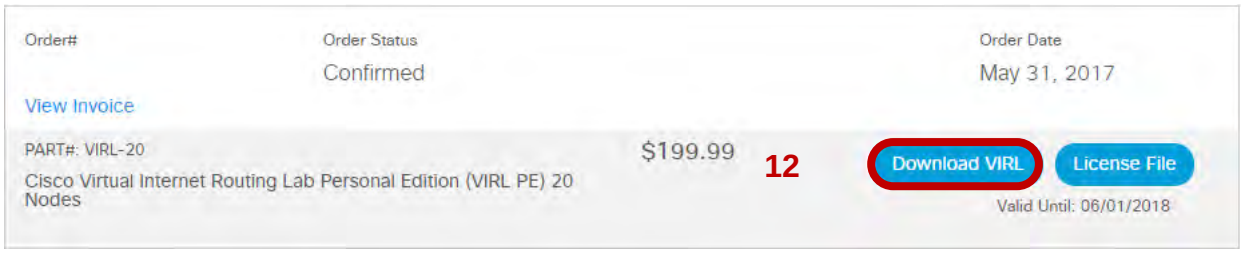

Figura 78. Suscripción de VIRL.

12. Nos redirigirá a la página de versiones de descarga de VIRL incluyendo los veinte nodos disponibles; buscamos la versión de IOSv que necesitamos y descargamos. En esta demostración elegimos la "vios-adventerprisek9-m.vmdk.SPA.156-2.T"

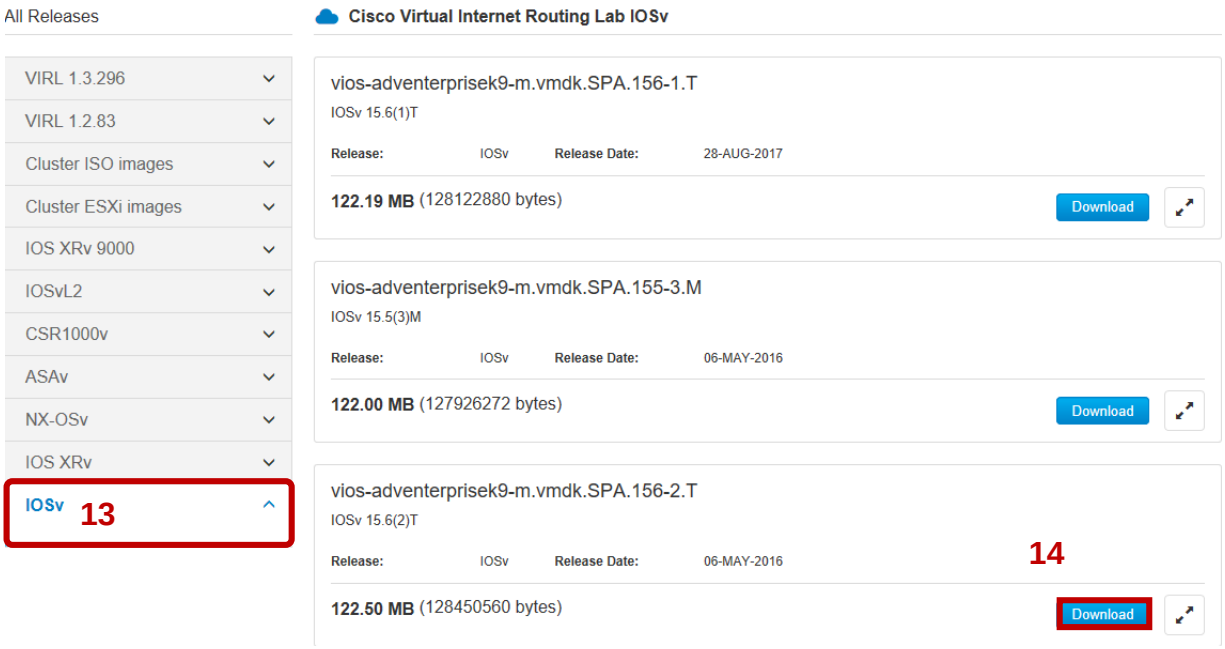

Figura 79. Versiones y nodos de VIRL

13. Ya descargado y almacenado en el disco duro, regresamos a la ventana anterior de GNS3 y pulsamos en “Import” nuevamente para traer la imagen al programa.

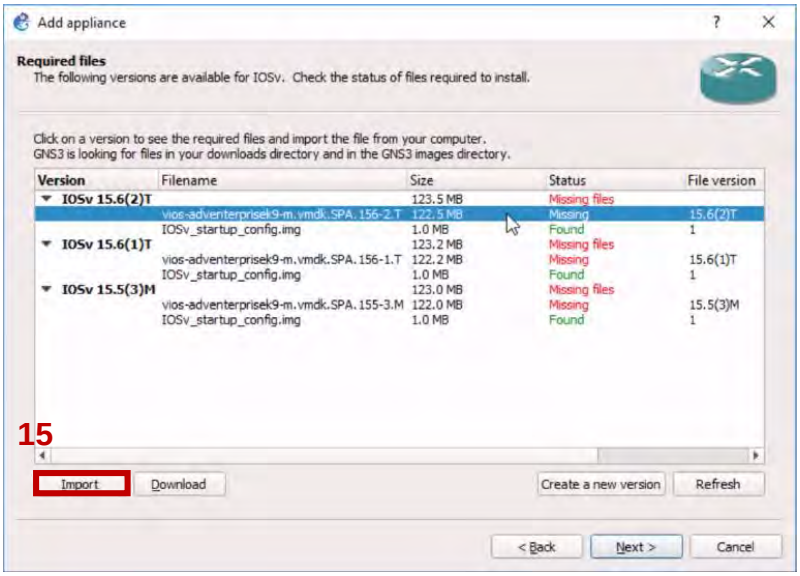

Figura 80. Importación de IOSv.

14. Se abrirá la ventana de explorador de nuevo; buscamos y seleccionamos nuestro IOSv.

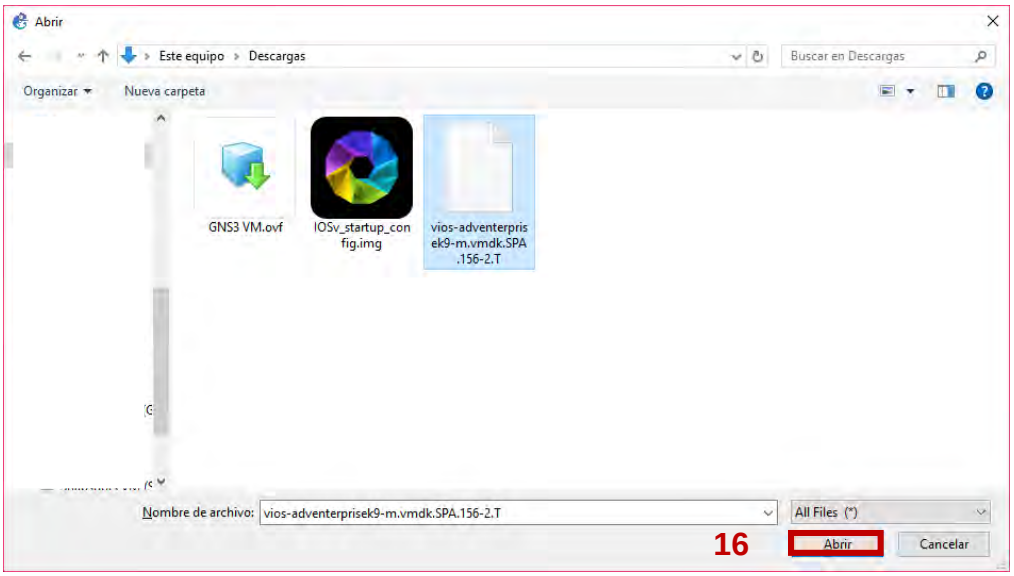

Figura 81. Selección de IOSv.

15. Cuando importamos nos debería reconocerlo el programa y con la leyenda “Found” en color verde, si no nos aparece de esa forma, damos clic en “Refresh” para actualizar el estado. Damos clic en “Next” para continuar.

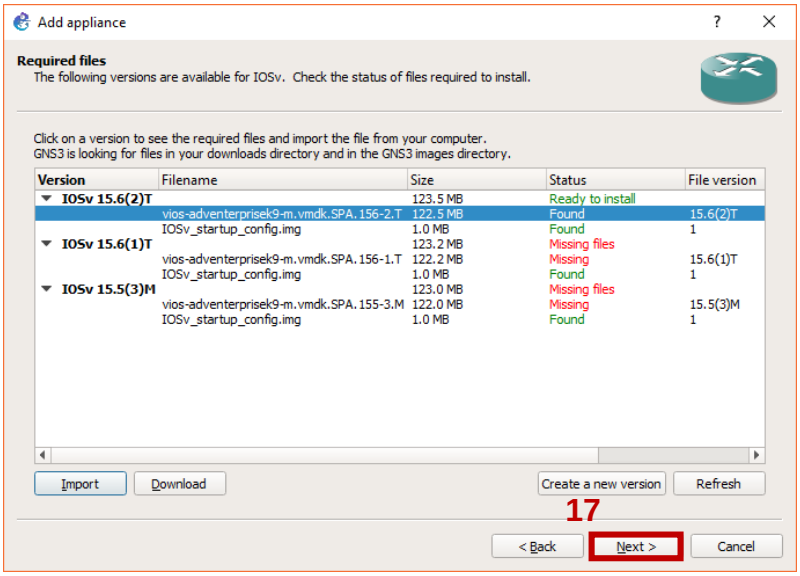

Figura 82. Importaciones exitosas.

16. Nos aparecerá una pequeña caja de diálogo que nos preguntará si queremos instalar el appliance; damos clic en “Yes”.

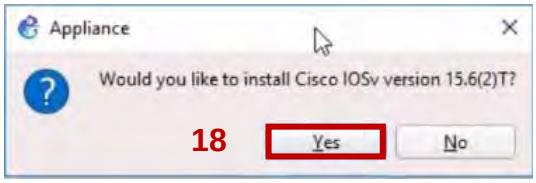

Figura 83. Caja de diálogo.

17. Nos indicará en cuadros verdes que el appliance se está subiendo a GNS3 VM del lado superior derecho del programa, como se muestra en la figura siguiente.

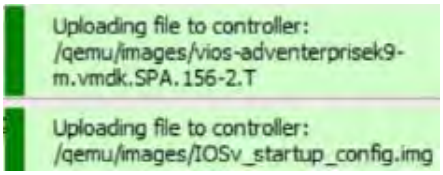

Figura 84. Subiendo archivos a GNS3 VM.

Al mismo tiempo, la siguiente ventana nos mostrará las opciones de arquitectura para el motor de emulación QEMU el cual se trata de un binario ejecutable dentro de GNS3 VM, en este caso dejamos los valores por defecto y damos clic en “Next”.

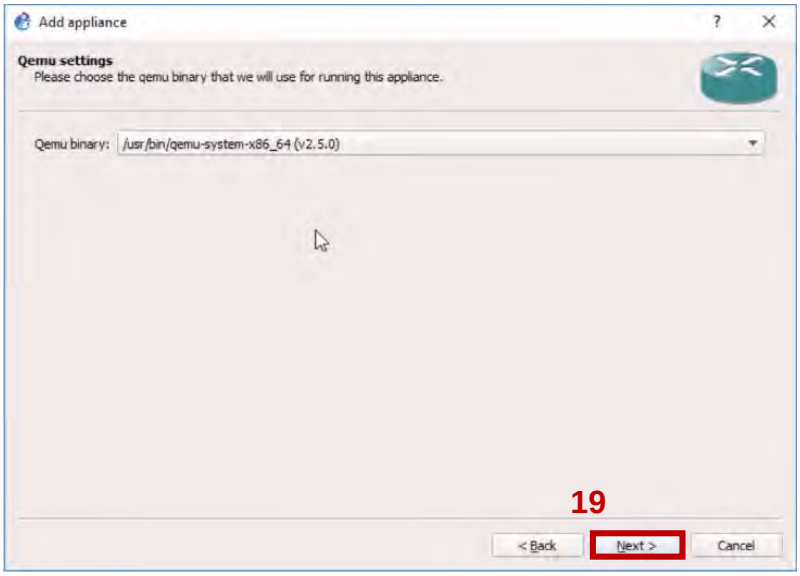

Figura 85. Arquitecturas para emulación con QEMU.

18. Siguientemente nos aparecerá un resumen, damos clic en “Next” para continuar.

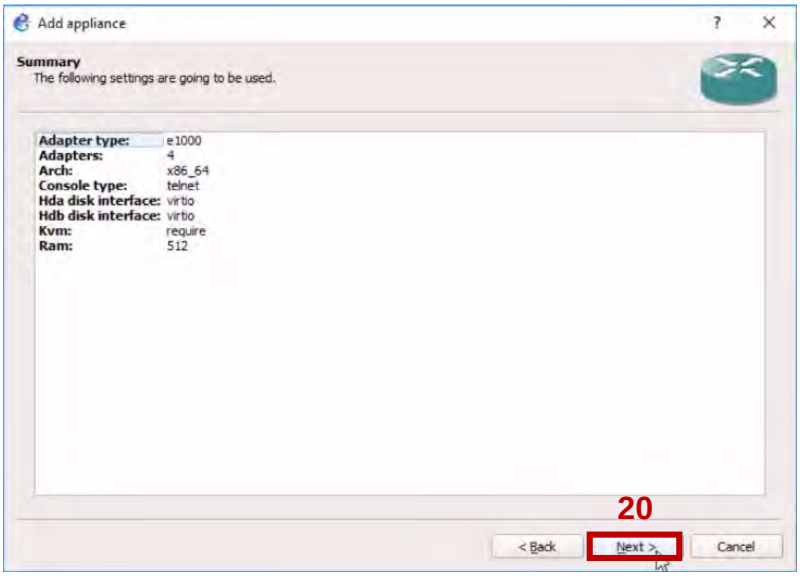

Figura 86. Sumario de atributos del appliance.

19. Nos dirá enseguida que nuestro appliance se encontrará en la categoría de enrutadores. Damos en “Finish” para finalizar la integración.

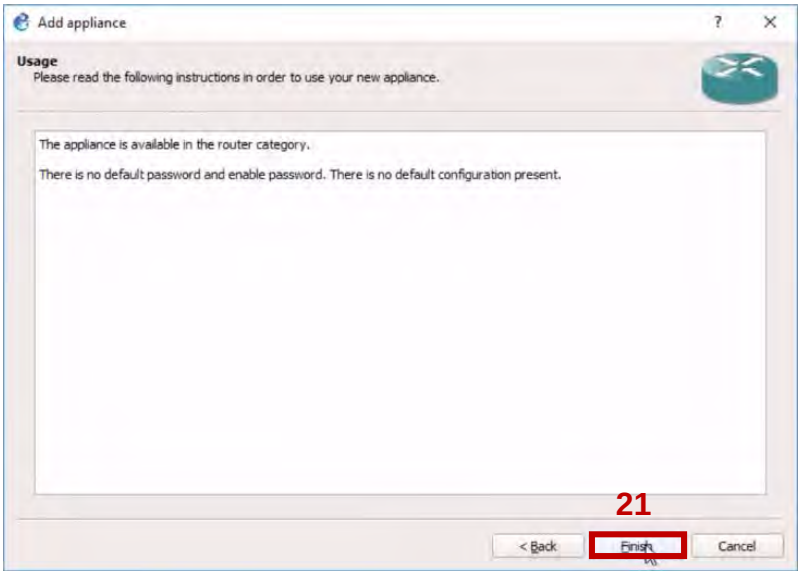

Figura 87. Indicación de categoría de appliance.

20. El siguiente cuadro de diálogo nos señalará que la instalación del appliance está completada, hacemos clic en “Ok”.

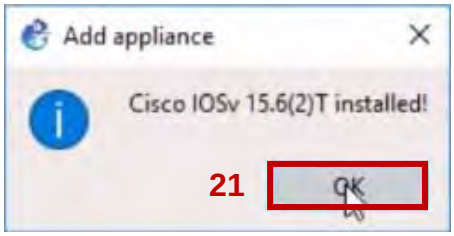

Figura 88. Integración finalizada.

21. Podemos ahora arrastrar nuestro nuevo appliance y crear varias instancias hacia el área de trabajo y combinarlos con cualquier tipo de appliance. En la imagen inferior podemos ver cuatro tipos de dispositivos:
    - R1 y R2: emulado con dynamips.
    - CiscoIOSv15.6(2)T-1 y CiscoIOSv15.6(2)T-2: emulados con QEMU.

- Ethernetswitch-1, Ethernetswitch-2 y PC-1: built-in ejecutados por GNS3.
- UsuarioW7: emulado con Oracle VM VirtualBox.

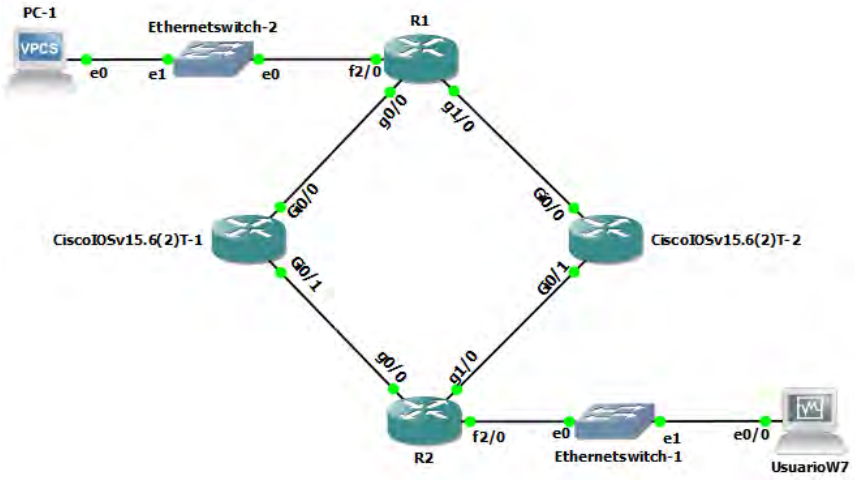

Figura 89. Varios tipos de appliances en el área de trabajo.

22. Probamos conectividad.

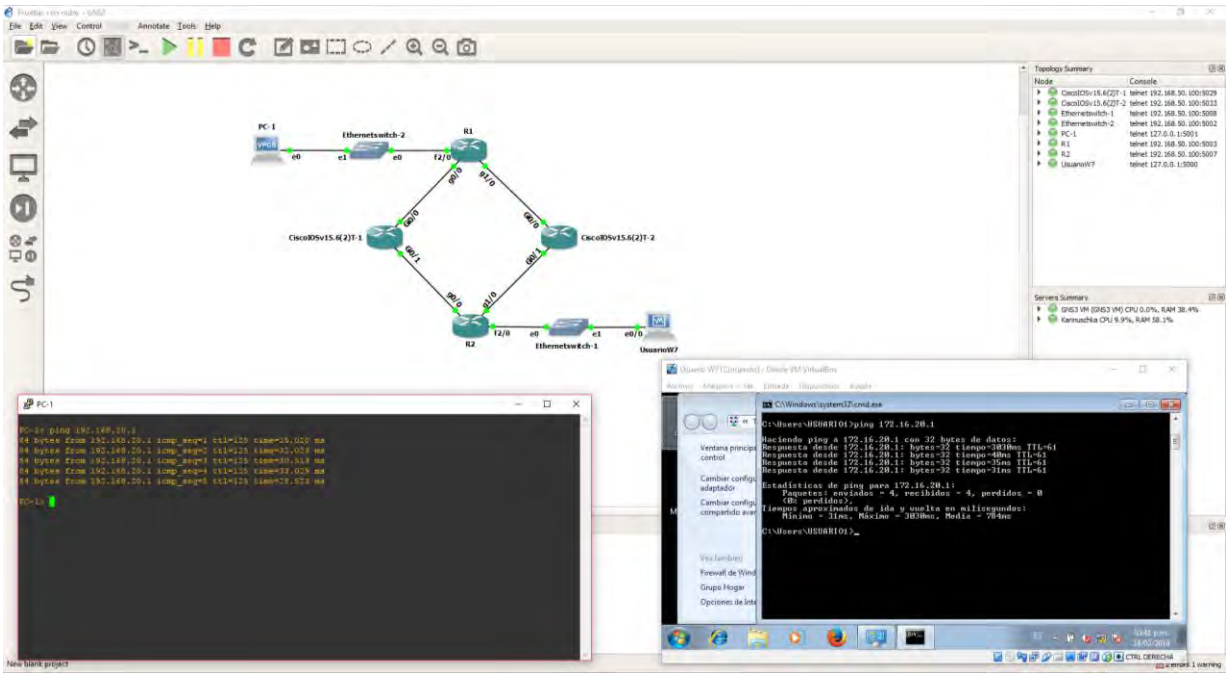

Figura 90. Conexión exitosa.

Por último, es prioritario aclarar que los requerimientos pueden variar dependiendo el tipo de dispositivo, especialmente los que son emulados con este motor. Ejemplos claros serían la integración de un IOSvL2, de un pfSense o de un Kali Linux.

Integración de appliances Cisco IOU.

Otra de las ventajas que ofrece GNS3 VM es la integración de enrutadores y conmutadores de bajo consumo de recursos informáticos. Al igual que la integración de los IOSv y otras appliances para QEMU, los IOU son subidos, alojados y ejecutados en GNS3 VM.

Los pasos para la integración de un appliance Cisco IOU son los siguientes:

1. Creamos un nuevo proyecto, y arrastramos nuestro Cisco IOU, en este ejemplo será para un elemento de capa dos. Nos aparecerá las características del appliance; damos clic en “Next”.

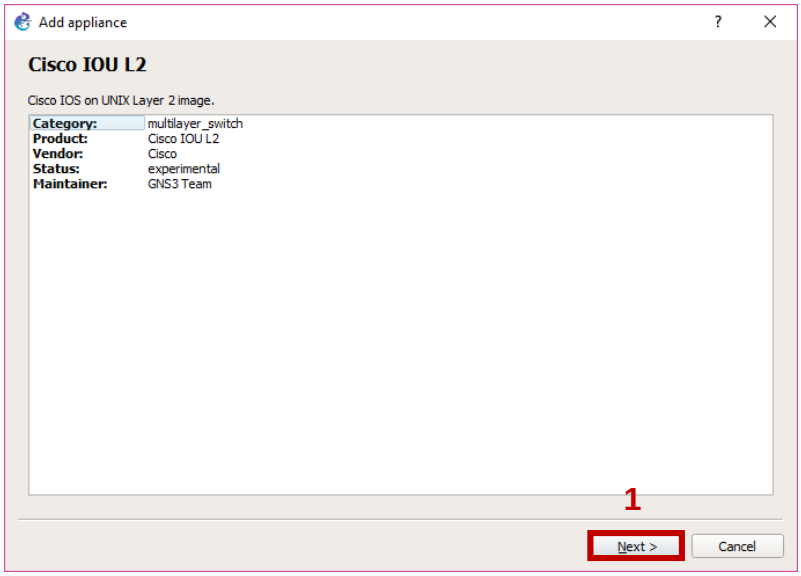

Figura 91. Características de IOU.

2. Como se trata de un appliance Cisco IOU, las opciones de servidor solo estarán activadas para ser puestas en GNS3 VM. Damos clic en “Next” para continuar.

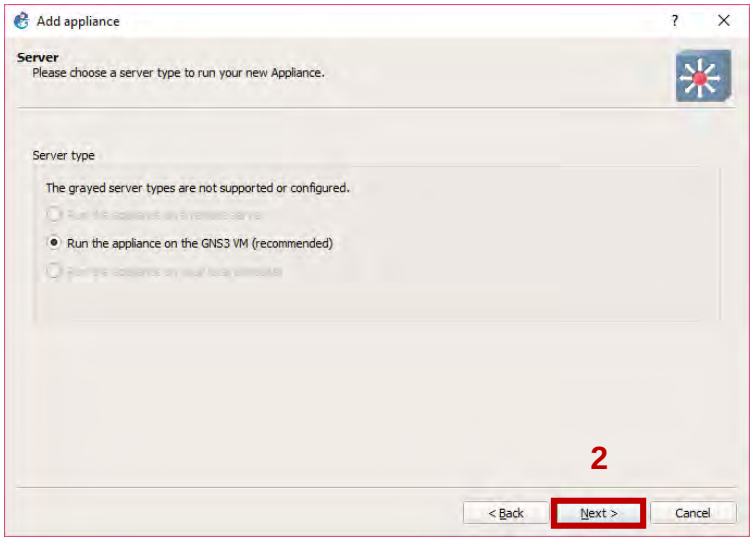

Figura 92. Servidor GNS3 VM como opción por defecto.

3. Nos indicará las imágenes recomendadas que podemos correr, apretamos “Import” para abrir nuestro explorador de archivos y buscar el binario, una vez encontrado los seleccionamos y nos aparecerá la leyenda “Found” en verde, en caso contrario damos en “Refresh” para actualizar. Damos “Next” para continuar.

Aviso: Recordemos que para adquirir los diferentes IOU, es necesario tener permisos suficientes para poseer de ellos y evitar cuestiones legales.

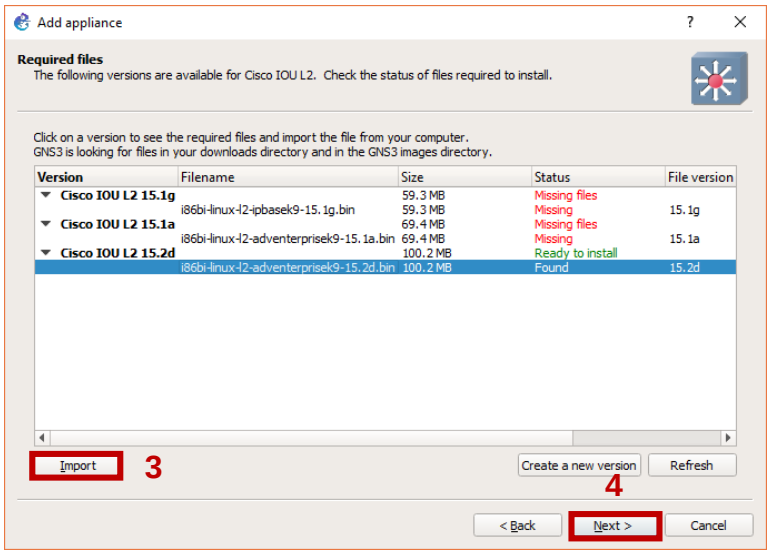

Figura 93. IOUL2 reconocido.

4. Nos preguntará si queremos instalar el appliance, seleccionamos “Yes” para proceder.

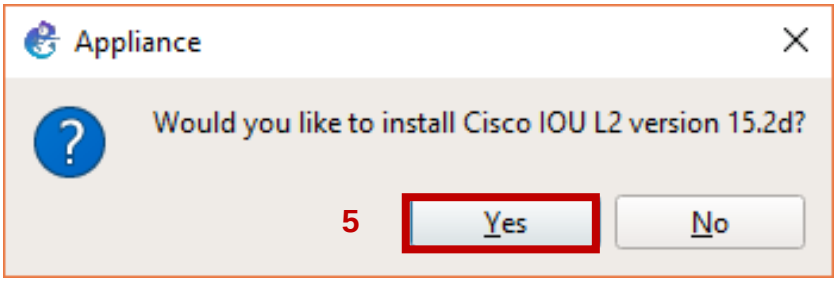

Figura 94. Caja de diálogo.

5. Nos mostrara el sumario del appliance. Damos clic en “Next”.

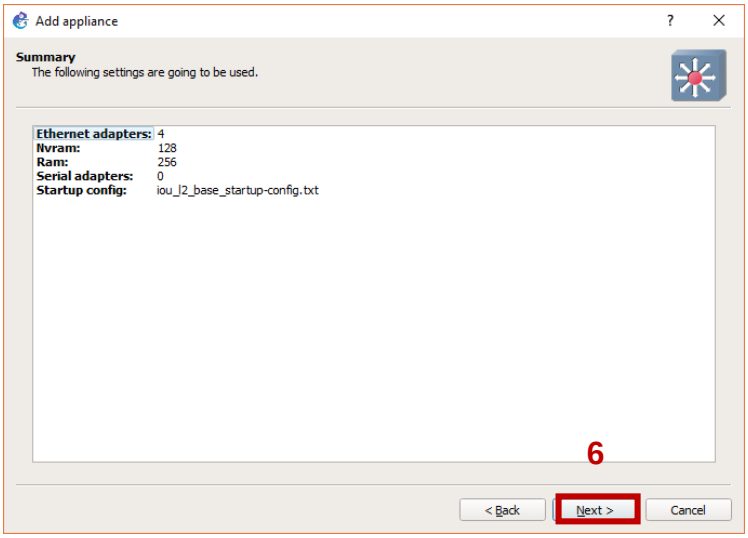

Figura 95. Sumario de appliance.

6. Nos dirá que nuestro appliance estará en la categoría de conmutadores. Damos en “Finish” para finalizar.

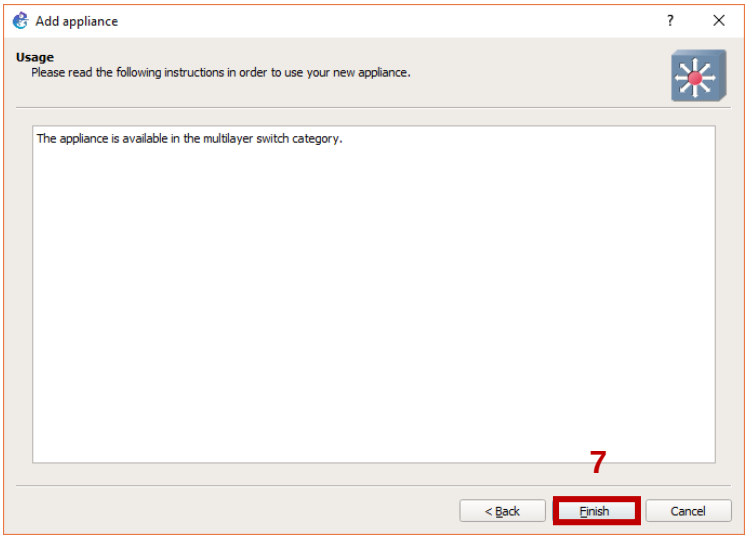

Figura 96. Categoría de appliance.

7. Tendremos otro diálogo en donde los dice que el dispositivo ya ha sido instalado. Hacemos clic en “Ok”.

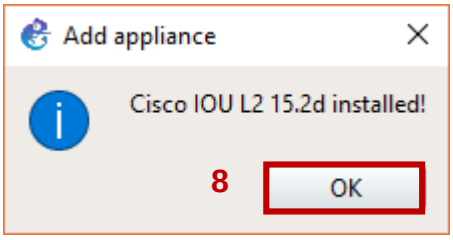

Figura 97. Appliance instalado.

A partir de este punto la integración de este tipo de appliance se vuelve un poco diferente, la razón es que necesitamos de un archivo de licencia que nos permitirá su uso en GNS3, este archivo se trata de un ejecutable escrito en Python.

Vamos a necesitar del programa llamado WinSCP instalado para poder subir el fichero y ejecutarlo para generar dicha licencia. Este programa usa el protocolo SFTP empleando SSH para subir archivos. Por lo tanto, continuando con la integración, seguimos con los pasos:

8. Iniciamos WinSCP y se nos abrirá una pantalla de inicio de sesión para conectarnos a GNS3 VM, sus credenciales por defecto son:
    - Usuario: gns3.

- Contraseña: gns3.

Presionamos “Conectar” para establecer enlace.

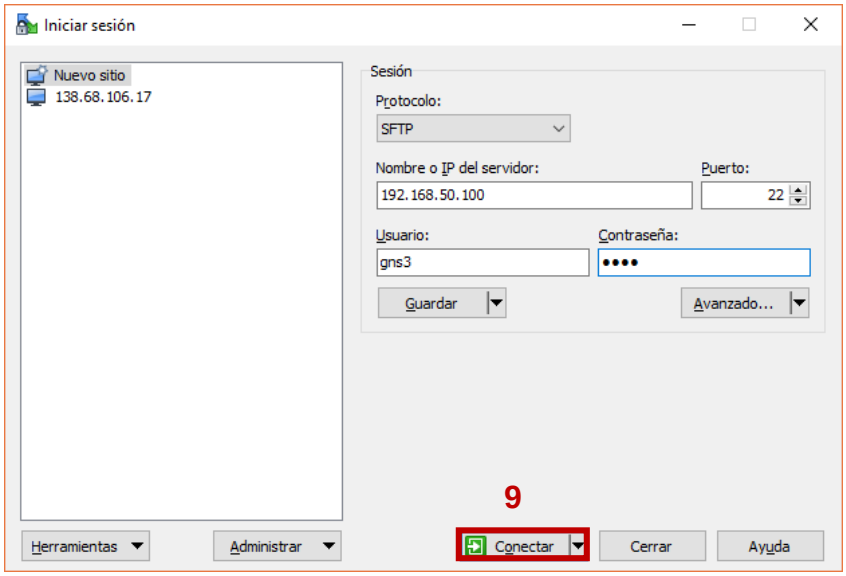

Figura 98. Conectando con GNS3 VM.

9. Inmediatamente, se nos creará la conexión y nos mostrará la estructura de archivos de GNS3 VM del lado derecho y de nuestro equipo local del lado izquierdo. Localizamos nuestro archivo “.py”, lo copiamos y lo pegamos en la máquina virtual.

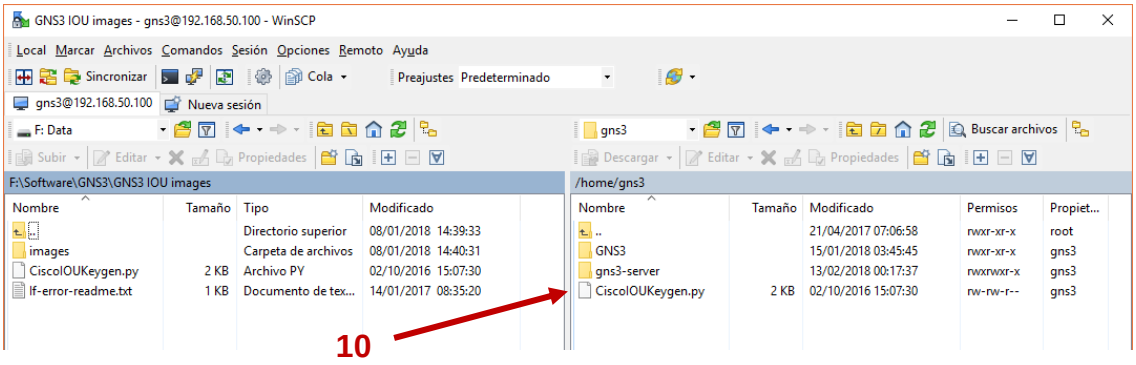

Figura 99. Archivo generador de licencia.

10. Dentro de GNS3 VM, presionamos “Ok”.

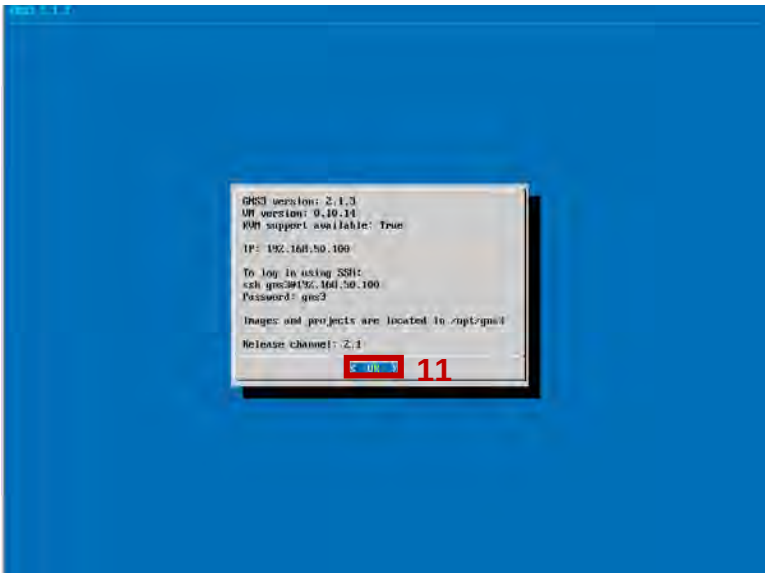

Figura 100. Pantalla principal de GNS3 VM.

11. Seleccionamos la opción de “Shell” para abrir la línea de comandos.

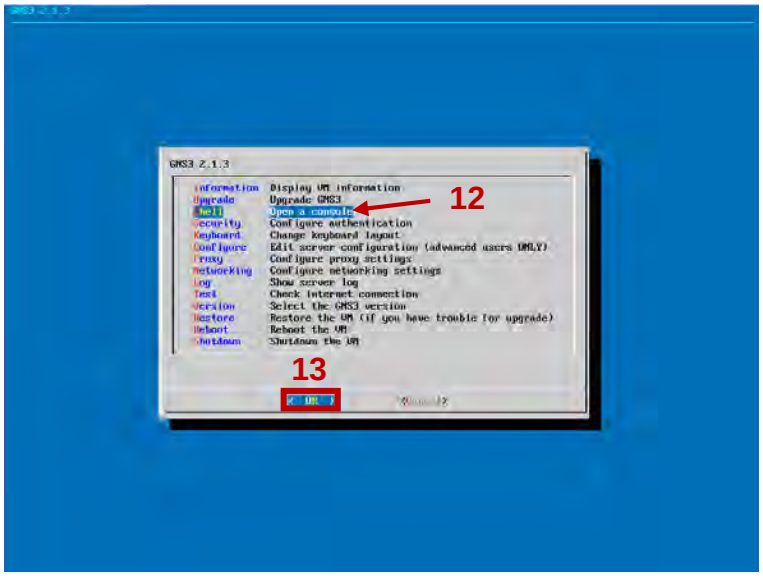

Figura 101. Opciones de GNS3 VM.

12. Nos aparecerá la consola de GNS3 VM y lo primero que debemos realizar es elevar los permisos de administración, por tanto, pasamos a super-usuario root para poder usar los comandos necesarios. Buscamos en el directorio el archivo y ejecutamos.

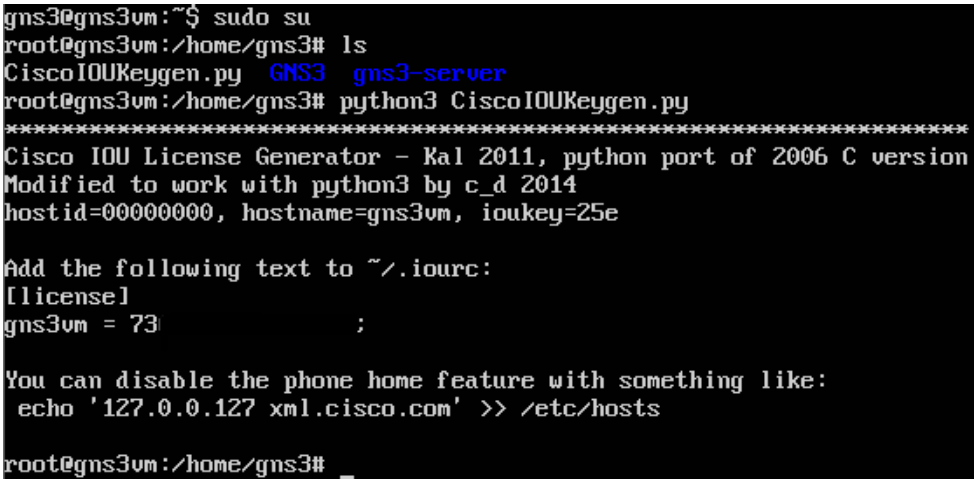

Figura 102. Ejecución de generador de licencias para Cisco IOU.

Vemos que se nos genera una licencia (que por seguridad está parcialmente oculto).

13. Nos manda una instrucción de crear un archivo de texto con los datos generados. Creamos en archivo de texto como en la siguiente figura y cerramos sesión en WinSCP.

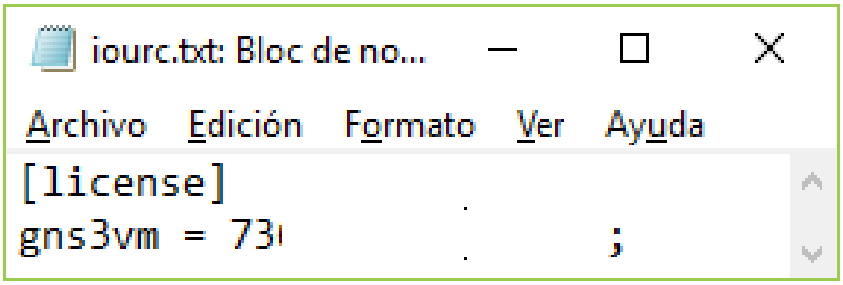

Figura 103. Licencia en archivo de texto.

14. Regresamos a las preferencias de GNS3 y editamos la categoría de “IOS on Unix” y hcemos clic en “Browse” para buscar la licencia.

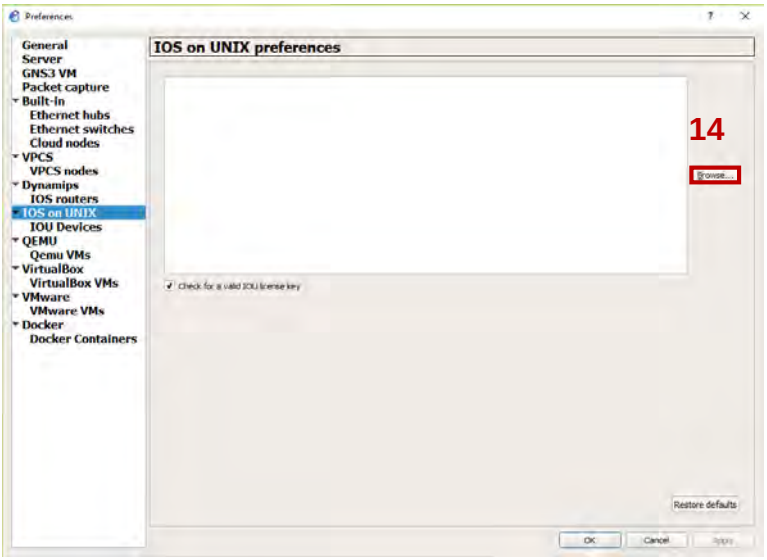

Figura 104. Edición de preferencias de IOU.

15. Nos aparecerá nuestro explorador para seleccionar nuestra licencia. Una vez seleccionada nos aparecerá de nuevo la información de licencia y damos en “Apply” y en “Ok”.

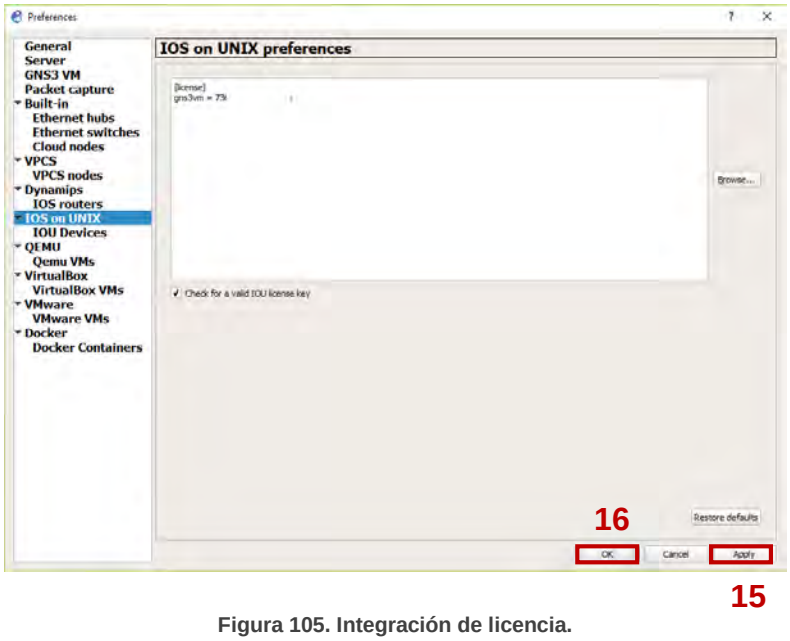

Figura 105. Integración de licencia.

16. De esta forma podemos, iniciar y trabajar con estos appliances tanta de capa dos y de capa tres. Podemos combinar dispositivos como se muestra en la figura inferior.

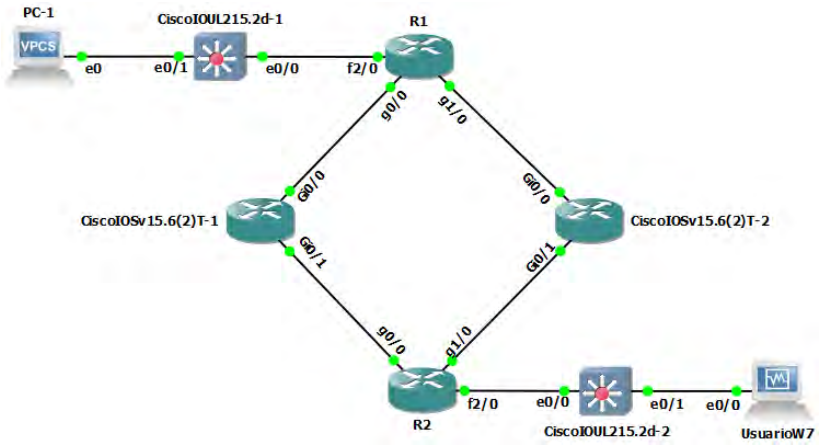

Figura 106. Topología con diversos appliances.

17. Configuramos dispositivos y probamos conexión.

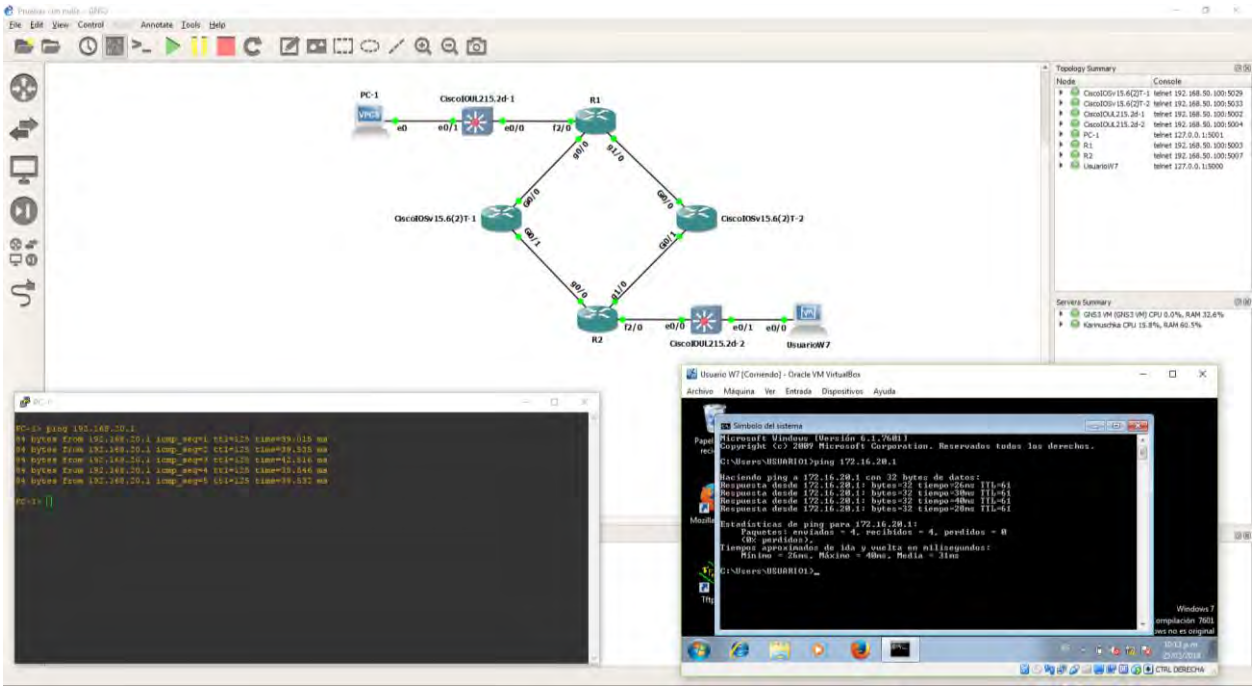

Figura 107. Conexión exitosa.

Integración de appliances Docker.

Uno de los tipos de appliance más interesantes son los Docker, ya que podemos montar servicios, plataformas, protocolos etc., de manera dedicada, portable y ligera. GNS3 cuenta en su Marketplace muchos de este tipo de integración, es así que veremos otra forma de realizar

una unión con GNS3, usaremos la plataforma de Ubuntu para realizar la demostración. Los pasos son los siguientes:

1. Vamos a la Marketplace de GNS3 en la categoría de "Appliances" (https://www.gns3.com/marketplace/appliances/), buscamos "Ubuntu Docker Guest" y descargamos.

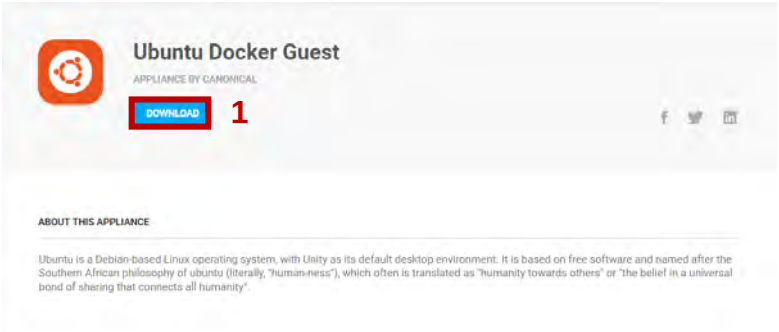

Figura 108. Descargando appliance.

2. Abrimos el programa, se cargará GNS3 VM e iniciamos el proceso de importación. Damos clic en "File" y en "Import appliance". Seguidamente se nos abrirá el explorador y buscamos el archivo con extensión ".gns3a".

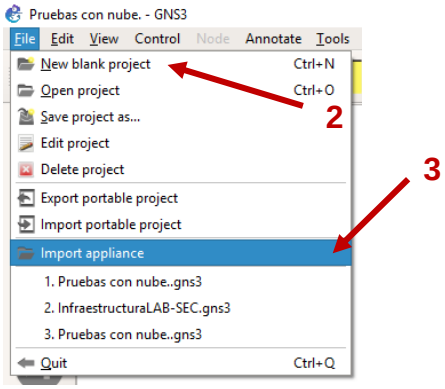

Figura 109. Importando appliance.

3. Seleccionamos el archivo e inmediatamente nos expondrá el sumario de características del dispositivo que estamos importando. Damos clic en "Next".

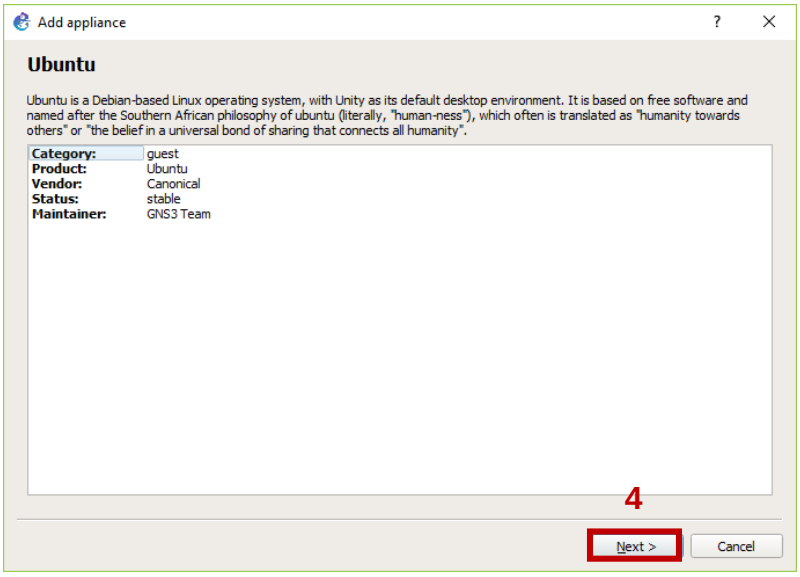

Figura 110. Características de appliance.

4. Nos dirá en dónde queremos subirlo y ejecutarlo, pero al tratarse de un appliance Docker, solo la opción de GNS3 VM está disponible. Damos clic en “Next”.

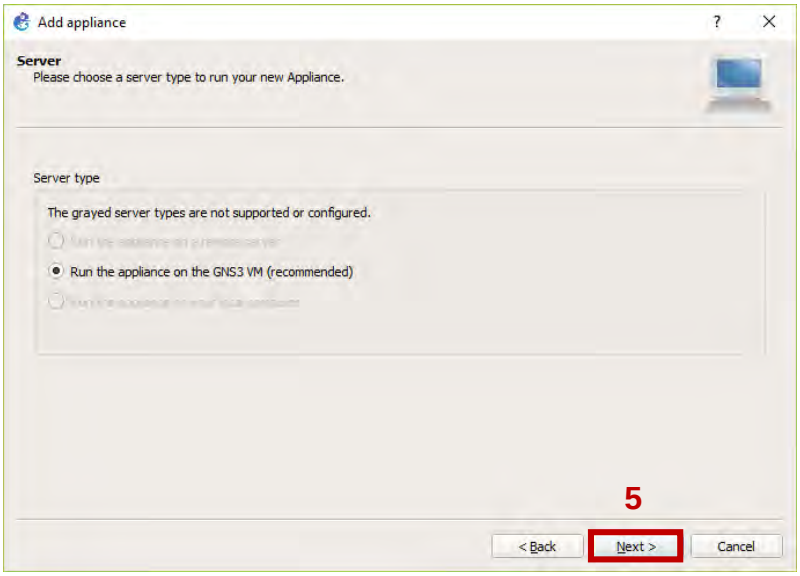

Figura 111. Opciones de servidor.

5. La siguiente ventana se trata de otro sumario, pero de especificaciones del appliance. Damos clic en “Next”.

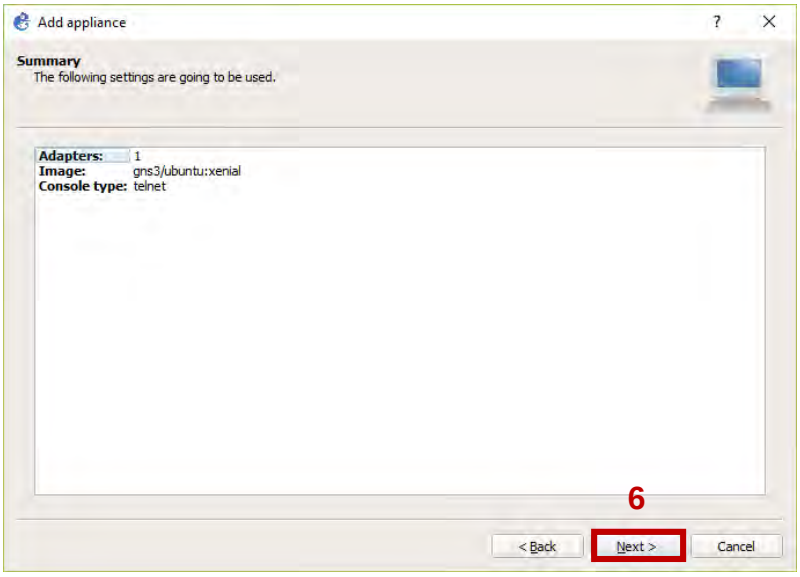

Figura 112. Especificaciones de appliance.

6. Nos dirá que el dispositivo estará en la categoría de “Guest”. Presionamos en el botón “Finish” para finalizar.

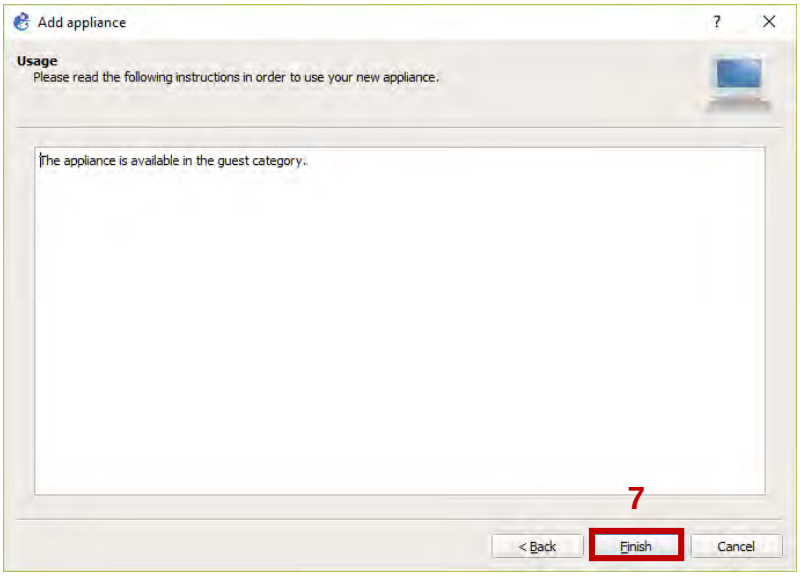

Figura 113. Indicación de categoría de appliance.

7. Se nos mostrará la barra de proceso de instalación y al finalizar se nos indicara que se ha instalado correctamente. Damos clic en “Ok”.

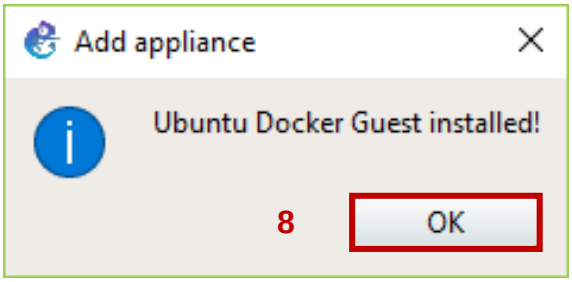

Figura 114. Appliance Docker instalado.

8. Cuando arrastramos e insertamos nuestro appliance, comenzará a descargar los repositorios necesarios para trabajar como se muestra en la siguiente imagen.

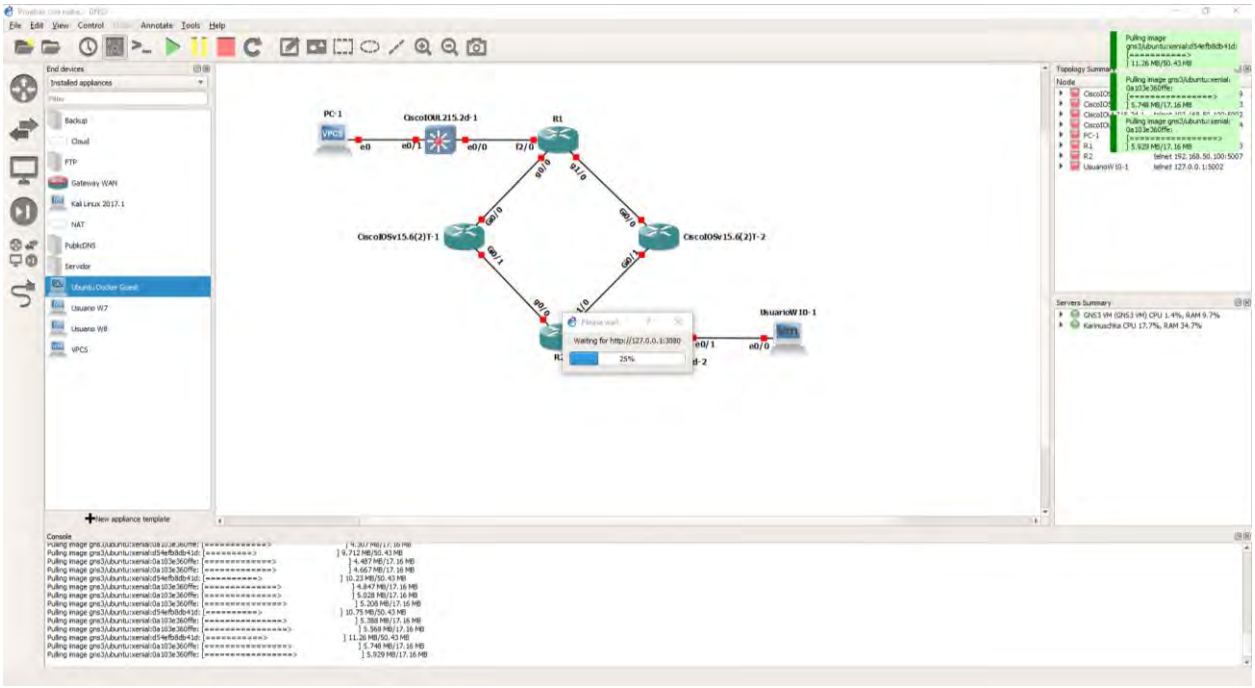

Figura 115. Descarga de repositorios.

Para lograr esto, primero tenemos que activar las conexiones NAT o puente en VMware® y configurar los adaptadores en GNS3 VM de manera que haya conexión hacia los servidores.

9. Una vez integrado el appliance, conectamos con distintos tipos de dispositivos y configuramos.

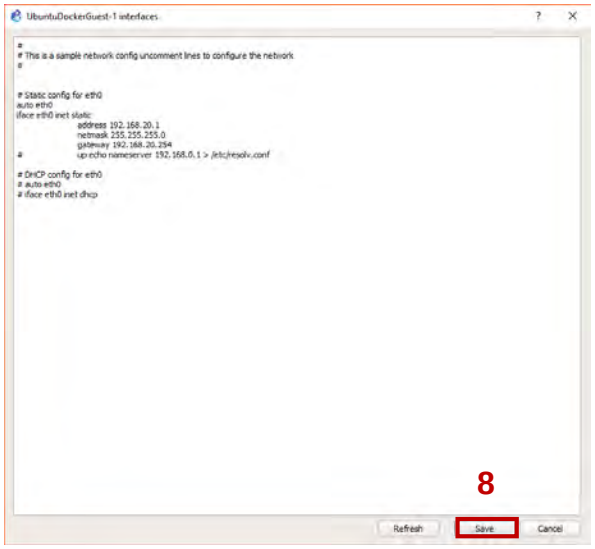

Figura 116. Configuración de adaptador de Ubuntu Docker.

10. Probamos conectividad.

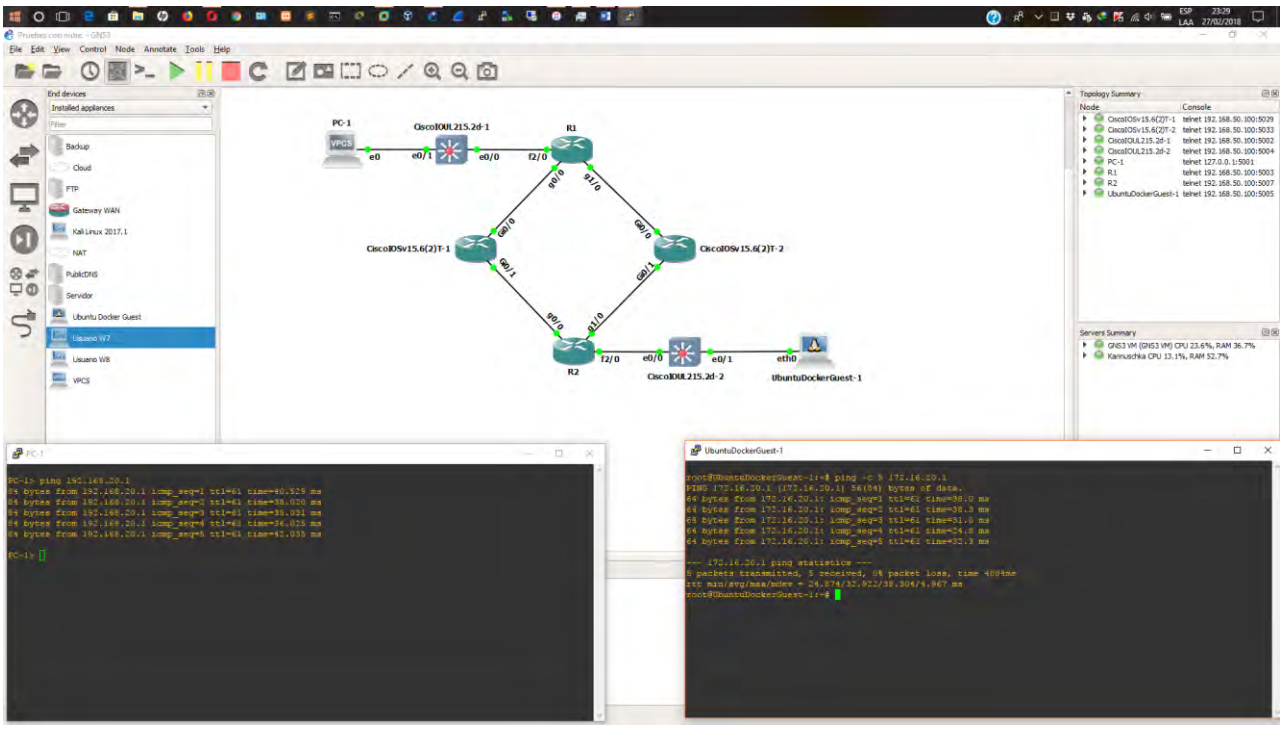

Figura 117. Conexión exitosa.