SEGURIDAD DE CABLEADO Y DATACENTER

Unidad 2

Seguridad de almacenamiento en el datacenter

ESCUELA DE CONSTRUCCIÓN E INGENIERÍA

Director: Marcelo Lucero Yáñez

ELABORACIÓN

Experto disciplinar: Eder Morán Heredia

Diseñadora instruccional: Luisa García Ospina

Editora instruccional: Emilia De la Cruz Barrés

VALIDACIÓN

Experto disciplinar: Gabriel Urra Varas

Jefa de Diseño Instruccional: Alejandra San Juan Reyes

EQUIPO DE DESARROLLO

Welearn

AÑO

2022

Tabla de contenidos

Aprendizaje esperado

Aplicar técnicas de diseño de red de datacenter basado en seguridad lógica, considerando procesos de implementación de una red segura de acceso de datos.

Fuente: Freepik. (s/f)

Introducción

¿Cómo se establece dentro de la seguridad física el control de acceso en un datacenter?

En la actualidad, el sistema informático y el constante cambio tecnológico junto a la gran demanda que supone el uso de las redes, inciden en la necesidad de la revisión de la infraestructura de los datacenter actuales, no solo a nivel computacional sino también a través de la red.

La búsqueda de alternativas para el tráfico de la red que se usa hasta ahora, el uso de Ethernet o InfiniBand provocaba que la red no fuese lo suficientemente flexible ni escalable para adaptarse a las necesidades que requiere un datacenter actual.

El uso de tecnología óptica como medio de conexión y distribución de los datos, pudiendo ofrecer un mayor ancho de banda a una baja latencia, genera que se obtenga un mejor rendimiento, además de un ahorro de energía.

Actualmente, una gestión adecuada y eficiente de los recursos físicos que componen un datacenter, han devenido en la búsqueda de un uso óptimo de los componentes físicos tales como la red, almacenamiento de datos, y los servidores computacionales. Estas plataformas permiten orquestar de forma heterogénea los recursos de un datacenter con el fin de ofrecer a terceros una infraestructura Cloud donde alojar servicios, y, este espacio se le conoce por virtual datacenter.

En principio, las gestiones en los datacenter requieren de una evaluación y estudio para determinar el consumo de energía y la eficiente utilización de esta. La eficiencia eléctrica en un centro de datos toma real preponderancia cuando, debido a la proyección y administración, se pierden cantidades considerables de energía que, a su vez, se ven reflejadas en costos innecesarios.

1. Criterios de Seguridad para Acceso y Gestión de un Datacenter

Actualmente, los datacenter se pueden sostener sobre tres estructuras paralelas: Tecnología de la información (TI), alimentación energética y refrigeración. Las tres infraestructuras tienen que relacionarse, ajustarse y optimizarse para lograr el funcionamiento perfecto del centro de datos.

- La tecnología de la información (TI) está compuesta por tres categorías, el primero son los servidores, los conmutadores de red y el espacio de almacenamiento y, es donde se instalan las funciones principales de los datacenter tales como la variedad de software, virtualizaciones, bases de datos, sistemas operativos y nubes.

- La energía eléctrica proviene principalmente de la red y esta alimenta los equipos de TI por medio de generadores, transformadores, sistemas de alimentación ininterrumpidas (UPS), barras de bus y conmutadores de transferencia automática (ATS)

- Gran parte de la energía que consumen los equipos de TI se pierde en forma de calor, de tal manera que ese calor debe ser manejado o evacuado. El objetivo es mantener la temperatura de los equipos los rangos para su funcionamiento en los datacenter. El sistema de refrigeración está compuesto por aire refrigeración por inmersión, acondicionadores de aire (CRAC *computer room air conditioning*) y unidades de manipulación de aire(CRAH *Computer room air handler*).

La metodología en el manejo de los datacenter está relacionado al objetivo de construir un procedimiento de eficiencia energético de un datacenter mediante una serie de conceptos, parámetros y métodos matemáticos. Por otro lado, se profundizará en los conceptos de DCIM dando a conocer su estructura, características principales y aspectos de implementación, que también se expondrán en un listado de procesos con el fin de facilitar su entendimiento.

1.1. Gestión de la Eficiencia Eléctrica

El estudio de la eficiencia eléctrica permite conocer el estado real del entorno en el datacenter al relacionar la demanda y el consumo energético de los equipos. Esto facilita la evaluación y modelación de la energía eléctrica para determinar su rendimiento. De esta manera, se busca diferentes alternativas que ayuden a reducir el consumo energético si afectar su normal funcionamiento

Las grandes empresas tienden a un elevado costo de consumo de energía eléctrica debido a las enormes de cantidades de información de los datacenter. Por lo tanto, se ven en la necesidad de generar controles de consumo eléctrico y la generación de parámetros de gestión de eficiencia de éstas, para reducir los costos económicos que conlleva.

1.2. Parámetros de eficiencia energética en un Centro de Datos

Generalmente los operadores no tienen toda la información posible en el manejo de eficiencia energética del datacenter. Además, el poco análisis que

se realiza a la hora de determinar el funcionamiento de los equipos. Para ello el operador debe tener en cuenta en la realización de sus tareas lo siguiente:

- Definición de la eficiencia del centro de datos.
- Medición de la eficiencia del centro de datos.
- Análisis de la eficiencia del centro de datos.
- Modelos de eficiencia para evaluar alternativas.

1.3. Preparación de un plan de medición de Eficiencia

Las mediciones se deben realizar con un lapso periódico de tiempo y son parte importante de la gestión y están diferenciadas por dos tipos que describimos a continuación:

1.3.1. Mediciones Iniciales

Se usa para el equilibrio del modelo de eficiencia del centro de datos, establecer el rendimiento real e identificar oportunidades de mejoramiento en la eficacia en la gestión. Estas mediciones se hacen en el sistema de alimentación y de enfriamiento por separado. Adicionalmente se hacen menciones generales en todo el sistema energético.

1.3.2. Mediciones Continuas

Una vez medida la eficiencia energética del datacenter y calibrado el modelo, deben tomarse mediciones continuas para cuantificar todas las

posibles mejoras de eficiencia y ofrecer advertencias sobre perdidas en la eficacia del sistema.

Estas mediciones permiten identificar cambios en los valores de la eficiencia y por ende encontrar cambios en la carga informática o en las condiciones climáticas permitiendo modificar el modelo para corregirse. Esto ayuda a determinar si las variaciones de la eficacia son los efectos de la carga de TI en las condiciones ambientales.

1.4. Puntos de registro en el centro de información

Los puntos de registro deben agrupar los siguientes sistemas:

1. **Registro en la Entrada:** Siempre y cuando se puede acceder a este lugar para adquirir datos, el registro en este punto permite:
    - Gestionar las condiciones de compra de energía.
    - Determinará el estado de la carga de la instalación, permitiendo evaluar posibles ampliaciones o para identificar perdidas energéticas.
    - El numerador del PUE en kWh.
2. **Registro del Clima:** Registrar el clima es importante ya que contribuye negativamente a la eficiencia del PC, este registro dará información sobre el sistema de enfriamientos.
3. **Registro a la entrada de los sistemas de UPS:** El registro de entrada y salida (cargas TI) de los sistemas UPS mostrará las pérdidas reales y la dependencia de éstas con las cargas de TI. En este registro se pueden ensayar diferentes situaciones como por ejemplo la desconexión de algunos módulos.

4. **Registro de la carga de TI:** Es la carga útil y el denominador del PUE, permite analizar el perfil de carga diaria y puede ayudar a cuantificar posibles ahorros energéticos. Este registro permitiría a los operadores programar ciertas tareas informáticas.

5. **Registro del alumbrado y otros:** Permite brindar mejoras del PC, este puede indicar el gasto innecesario de iluminación durante la noche y el día.

1.5. Modelos de eficiencia del Centro de Datos

Las mediciones del efecto de actividades que se realizan en un centro de datos no se realizan con una sola medición de PUE (*Power Usage Effectiveness*). Este método no es eficiente a la hora de brindar la información sobre oportunidades de mejora de eficiencia, para ello se sostendrá en otros modelos. Un modelo puede brindar datos sobre las condiciones de entrada, permitiendo a los operadores actuar sobre los trabajos en el datacenter, para ello es necesario conocer en el sistema de la siguiente manera:

- Valorar la eficiencia con carga completa cuando la carga de TI real es una pequeña fracción de la carga nominal.

- Realizar comparaciones entre los centros de datos al ingresar las condiciones de entrada sobre los modelos de éstos.

- Predecir el comportamiento de un centro de datos con la ayuda de un modelo anterior a la construcción del datacenter.

Esa serie de tareas otorga a los operadores beneficios que no podrían obtener midiendo y registrando la eficiencia del datacenter. Las ventajas de ellos son las siguientes:

- Predecir el rendimiento de la eficiencia de diseño propuesto un centro de información.
- Calcula con precisión el rendimiento de la eficiencia de un datacenter en funcionamiento y con cargas TI diferentes.
- Calcula el rendimiento de la eficiencia en situaciones donde solo se cuenta con la información parcial.
- Identificar cuanto contribuyen los sistemas de alimentación enfriamiento e iluminación en la eficiencia del datacenter.
- Analizar mediciones bajo diferentes condiciones climáticas para establecer el rendimiento operativo del centro de datos.

1.6. Importancia de la DCIM

El Data Center *Infraestructure Management* (DCIM) es una herramienta que colecta y maneja información sobre los bienes del datacenter, el uso de recursos y el restador de operación. Esta información es distribuida, integrada, analizada y utilizada de formas que ayuden a operar el datacenter de manera eficiente. Las principales características y funciones de DCIM incluyen:

- Alertas, advertencias y notificaciones de eventos.
- Funciones de control de automatización.
- Herramientas de gestión de activos, flujos de operación, y asignación de recursos.
- Capacidad de elaboración de informes y modelos de datos.

Composición del Datacenter: Un datacenter puede consistir en cientos de software administrativo. Entonces, el primer paso cuando se clasifican estos subsistemas es agruparlos dentro de un subconjunto general que también puede ser usado para clasificar el software administrativo para TI.

Estos subconjuntos están asociados por una interfaz gráfica de usuarios (GUI) o por una interfaz humana maquina (HMI). Por otro lado, el subconjunto de tablero de instrumentos es el área principal dentro del mapa conceptual que permite la visualización.

1.7. Pasos para integración DCIM

La implementación y el uso de software se hacen sobre el personal y sobre los procesos en la capacidad técnica. El proveedor de servicio debe estar capacitado de los procesos y personal para implantar DCIM, los siguientes pasos describen como es una integración en la solución DCIM en los datacenter:

1. **Evaluación de las capacidades:** Cuando se establece un DCIM deben indicarse las funciones que debe soportar la solución esto significa que la solución debe evaluarse según las herramientas de gestión que otorgue el datacenter.

2. **Objetivos a largo plazo:** Evalúa futuros planteamientos en la dirección de los requisitos de TI y del datacenter. Así se visualiza las capacidades tecnológicas de la solución DCIM para saber si será es capaz de adaptarse a los planes de crecimiento a largo plazo y los requerimientos cambiantes.

3. **Evaluación de Informes:** La solución que plantea DCIM debe establecer la información que realmente es necesaria y útil para dar soporte a los requerimientos específicos dentro del informe deben indicarse lo siguiente:

    - Personas y grupos tienen acceso a la información de los informes específicos.
    - El nivel descriptivo del informe.
    - La frecuencia con la que se elaboran.
    - El aspecto que se tenga en el panel de control.

4. **Evolución en la industria:** Los cambios y retos en el sector del datacenter traerán nuevas tecnologías como virtualización aumentos de capacidad. Colocación o nube, etc. al prepararse para estos cambios se deben evaluar si la evaluación DCIM ayudara al datacenter a proveer y estar listo para afrontar los cambios a futuro.

1.8. Control de Acceso

Estar protegidos frente a la intrusión de personas extrañas del datacenter es una preocupación siempre es evidente que la primera prevención debe estar en el acceso a las instalaciones. En este sentido es fundamental que un datacenter tenga los controles de acceso eficiente, ya sea por medios físicos o con soporte digital tales como tarjetas, uso de biometría de reconocimiento esto permite que el acceso sea restringido a todas las personas y sea imposible saltar este hito.

Por supuesto que exista la posibilidad de establecer controles cuando los accesos son autorizados por personal de la dirección, para ello

estableceremos medidas con el fin de proteger la mayor fuente de ingresos que tiene la empresa en este caso los Datos.

Para evitar esto el datacenter debe contar con un sistema de vigilancia que nos permita controlar cualquier tipo de riesgo y estar preparados ante posibles intrusos. Para establecer un mayor análisis se deberá establecer un sistema de videovigilancia con reconocimiento facial y análisis inteligente de imagen.

1.9. Sistema de Alarmas

Con las restricciones establecidas para el control de acceso de las personas se considera el gasto en la protección del datacenter. La destrucción de accesos viene del exterior al interior, por lo tanto, un sistema de alarmas establecerá otro de alertas en el momento que se detecten movimientos sospechosos e intrusos. Proteger la periferia de nuestro datacenter es tan importante como mantener a salvo el interior.

1.10. Monitorización

A estos requisitos se siguen sumando nuevos accesorios y dispositivos hay que añadirle la posibilidad de tener forma periódica controlada al estado de temperatura, generadores, suministros comunicaciones y seguridad. El monitoreo constante de los distintos mecanismos de control de temperatura, de acceso y seguridad del datacenter se debe realizar minuciosamente para una mejor gestión de datos.

1.11. Sistema de Climatización

Además de controlar los accesos y vigilar que personas ingresan a un datacenter es evidente que los servidores físicos deben contar con una

temperatura y condiciones climáticas. En parte necesitan un propio ecosistema que los proteja ante cualquier incidencia.

2. Seguridad del lado del Cliente

La información que se desea proteger en un datacenter reconoce diversos niveles de sensibilidad, es decir, el grado de importancia que tienen los datos en las empresas. A ello se le llama criticidad de la información, así como los niveles variados de severidad y probabilidad de compromiso, a menos que los niveles de seguridad para ciertos datos estén prescritos por ley (por ejemplo, seguridad nacional o privacidad) y/o requieren alineación con compromisos regionales o internacionales. La definición de los niveles de seguridad queda a discreción de la organización particular. Esto no significa necesariamente que el cumplimiento de los requisitos legales requiera categorías de clasificación independiente.

2.1. Por el lado del cliente

Es muy claro el escenario en cuanto al uso de un datacenter, sin embargo, se deben establecer ciertos parámetros a la hora de elegir uno que sostenga un modelo de negocio si es que la empresa desea contratar un proveedor en esta área.

Desde las certificaciones que estandarizan la infraestructura pasando por ubicación, clima, fuente de energía /métodos de enfriamiento, son algunos de los aspectos para tener en cuenta.

Para que la empresa o cliente tome una decisión deben fijarse en algunos detalles que exponemos a continuación:

La tendencia actual en la construcción de inmobiliarias está centrada en la ubicación como mejor opción para explotar el rendimiento de un negocio.

En la actualidad, los altos precios de las áreas céntricas de las ciudades cosmopolitas incrementan los costos operativos y, por lo tanto, el servicio prestado aumenta en valor. También, debe considerarse la afectación del cambio climático que tienden a crear un gasto adicional que debe ser incorporado a dichos servicios. El exceso de humedad, lluvias calor, o terrenos con posibilidad de expandir la infraestructura local son parte del inconveniente a tratar.

Según Ultime institute, sobre el estudio del cambio climático, el 70% de los datacenter indican que planean tomar medidas para mejorar la resiliencia de su infraestructura critica. El tema de la distancia también influenciará en la calidad de la velocidad de transmisión de datos o los tiempos de respuesta ante emergencias queda en un segundo plano cuando se hablan de las instalaciones en fibra óptica de alta velocidad como la Optical Network ofrece.

2.2. Resiliencia y Tiempo de actividad

Es importante destacar que esta última década ha sido marcada por múltiples fallos de continuidad del servicio de internet y disponibilidad de datos de grandes empresa y proveedoras de data center algunos casos conocidos pueden ser:

- CDN Fasty. Fallo en 2021.
- Facebook: Fallo en tiempo de inactividad en octubre del 2021.
- Amazon Web Services. Interrupción prolongada del servicio en diciembre de 2021.

De allí la importancia de establecer mejoras en la adopción de infraestructuras hibridas para que el tiempo de actividad no se vea interrumpida por fallas en las copias de seguridad, la conmutación hacia la nube o la infraestructura perimetral.

2.3. Abastecimiento de los suministros tecnológicos del datacenter

Es una de las grandes preocupaciones que tienen muchos proveedores alrededor del mundo por el creciente aumento de la construcción de nuevos datacenter y las restricciones de acceso a partes y piezas. Por eso sabe si el proveedor tecnológico tenga planes de expansión y crecimiento es buena noticia, pero se debe estar seguro de contratar servicios. No habrá inconvenientes en la escalabilidad del datacenter si así lo requiriese.

2.4. Incremento de Inversión en regiones y en Innovación tecnológica

El crecimiento también trae consigo una transformación digital tanto a pequeñas empresas como a grandes corporaciones en procesos estratégicos de fusión para la integración de soluciones y unión de esfuerzos. Pero, más allá de eso, ha ido desconcentrando esa inversión de países desarrollados a regiones como Latinoamérica y sur de Asia.

2.5. Sistemas de Refrigeración Líquida

Siguiendo con los lineamientos de innovación y energías limpias y en este aspecto las nuevas tendencias en requisitos para estas instalaciones están centradas en el control de temperatura en los equipos. Evitar que los datacenter colapsen por deterioro de los equipos o degradación del rendimiento por caudas térmicas es vital para el negocio.

Por ello ante los sistemas tradicionales de enfriamiento por aire acondicionado se están adoptando de forma más segura y rápida sistemas de enfriamiento por agua y alternativas de refrigeración líquida (*immersión cooling* o refrigeración por inmersión) en sustitución agua y otros medios.

Este tipo de técnicas consiste en el enfriamiento de los servidores al sumergirlos en un líquido dieléctrico; el líquido en contacto directo con componentes calientes adsorbe el calor que a continuación a través de intercambiadores de calor se disipa en el exterior.

2.6. Garantías de seguridad

Es un estándar que los proveedores del servicio ofrezcan servicios 24/7 con protocolos de ciberseguridad DRP actualizados pero gran parte de esta seguridad está en la validación de sus procesos y/o infraestructuras son pocos los que han podido certificarse en ese ámbito.

Tanto la seguridad física de la infraestructura como la ciberseguridad son esenciales para el datacenter. Tener instalados sistema de gestión eficaces ante incidente y la puesta en marcha de la continuidad del negocio, así como las múltiples barreras de accesos a salas privadas y demás son esenciales en el sitio.

Cumplir con los estándares de certificación internacional como ANSI/TIA y TIER con en nuestro caso en Optical Network fortalece nuestro vínculo con los actuales clientes y los futuros usuarios.

3. Seguridad a nivel de Red Interna

La seguridad en la red no es más que la implementación de los mecanismos ya sea hardware o software que se encargar de procesar y filtrar a los usuarios o programas que quieran interferir o infiltrarse ya sea con la integridad de la red o con la información que se encuentra en esta.

¿Para qué sirven?

Los sistemas informáticos incluyendo los datacenter necesitan algún sistema de seguridad para proteger a los computadores conectadas en una red. De tal forma que solo se puedan usar de una forma segura en la cual los usuarios puedan comunicarse de manera que nos salgan datos a lugares o a personas no deseadas y se puedan procesar solo en un orden deseado bajo los parámetros de restricción que se establece. Para ello, ya sea por una orden escrita establecida por el administrador de dicha cuenta para lograr ese estatus se requieren de varios pasos a seguir y distintos niveles de seguridad. De los cuales se hablará a continuación:

¿Como se inicia la Seguridad en la Red?

Para establecer una seguridad en la red se tiene que empezar por lo más básico que en el caso de los computadores actuales sería activar el Firewall. En este programa se filtran los accesos a la red y bloquea la accesibilidad a personas no autorizadas a redes privadas. No obstante, el Firewall tiene algunas desventajas de las cuales se pueden mencionar las siguientes.

Sin embargo, el cortafuegos no puede proteger de las amenazas a las que está sometido por ataques internos o usuarios negligentes. El cortafuegos no

puede prohibir a espías corporativos copiar datos sensibles en medios físicos de almacenamiento (discos, memorias etc.) y sustraer del edificio.

Además, el cortafuegos no protege contra aquellos ataques cuyo tráfico no pase a través del cortafuegos no puede proteger contra los ataques de la ingeniería social. Tampoco protege contra los ataques a la red interna por virus informático a través de archivos y software. La sesión parte cuando la organización establece un cortafuego para cada uno de los ordenadores que componen a la organización para protegerse de los virus que llegan desde cualquier lugar medio de almacenamiento u otra fuente.

El cortafuegos no protege de los fallos de seguridad de los servicios y protocolos cuyo tráfico está permitido hay que configurar correctamente y cuidar la seguridad de los servicios que se publiquen en internet.

¿Y si no se activan los controles del Firewall?

En caso de que la primera opción falle se pueden adquirir otras metodologías de control tal es el caso de los antivirus. Por consiguiente, el software establecido para ello detectará fácilmente y eliminará, o en el peor de los casos, controlar que el virus no se expanda. Para ello, hará la contención respectiva no dando las autorizaciones respectivas si en el permiso de un usuario o administrador para que no se puedan desactivar otros dispositivos de seguridad o se puedan recolectar datos o contraseñas necesarias para poder controlar la red o la infraestructura de esta o dañarla. Para aclarar, el antivirus y el firewall no protegen de todos los riesgos en una red abierta, ya que en una red cerrada no se entrometen los usuarios de otros lados siempre cuando sea una red privada. Existen otras opciones a la hora de implementar con el hecho de encriptar los archivos, claves comando, pero sobre esto no me internare porque es un tema demasiado avanzado.

3.1. Los Firewall

Desde la creación de las redes los cortafuegos o(firewall) se implementa en el perímetro de la red y filtran el tráfico según las direcciones IP, los números de puerto y los protocolos. Estos firewalls de red generalmente se crearon con el objetivo de que en forma independiente podían identificar y bloquear ataques dirigidos a cualquier cosa dentro del perímetro de la red. Dado que las organizaciones operaban su centro de datos locales y podían tener independencia de su infraestructura de red, este enfoque se torna viable para la seguridad de la red.

Actualmente, los Firewall incorporan características adicionales, más allá de un firewall tradicional, donde incluyen la inspección de aplicaciones, la implementación de prevención de amenazas y la inteligencia de las amenazas integrada. Un firewall en la nube está diseñado para proteger la red moderna que contiene entornos en las nubes y protege las aplicaciones en la nube de una organización contra los taques donde sea que se encuentre.

3.2. Funciones Esenciales para el Firewall Moderno

La principal diferencia radica que entre los firewalls tradicionales y una actual nos ofrece una infinidad de funciones más allá de la simple inspección, de tal manera, protege eficazmente de las ciberamenazas.

Gestión de la Seguridad Unificada: Actualmente las organizaciones se enfrentan a un enemigo que cada día crece en las posibilidades de ataque se extiende en un panorama de ciberamenazas sofisticado y en constante evolución. Por lo tanto, deben proteger entornos de red diversos y escalables. Un firewall de nueva generación permite a los equipos de seguridad

monitorear y administrar la seguridad en toda la red desde la comodidad de una consola.

3.3. Prevención integrada de Amenazas

Como su principio de operación lo establece un firewall debe estar diseñado contra las amenazas cibernéticas tanto de la forma más sencilla hasta la solución más compleja. Esto requiere tecnología de prevención central como protección antivirus, antimalware y Anti-Phishing, así como tener la capacidad de recibir fuentes de inteligencia de amenazas y usarlas para identificar ataques más sofisticados.

3.4. Inspección Basada en Aplicaciones e Identidad

Cuando se usan diferentes sistemas y usuario en la red de una empresa u organización se deben establecer los permisos necesarios en niveles de acceso y políticas de seguridad que difieren. Un firewall moderno debe poder identificar la aplicación, el sistema o el usuario asociado con un flujo de red y aplicar políticas de seguridad específicas basadas en los parámetros establecidos previamente.

3.5. Soporte de Nube Hibrida

Casi todas las organizaciones utilizan la nube como soporte de una red o como almacenamiento y alguno que otro tipo de procedimiento la mayoría tiene una infraestructura de red de la organización lo que permite que el equipo de seguridad administre esas políticas desde una única consola.

3.6. Rendimiento Ecuable

Los firewalls de hardware tradicionales no escalan bien, lo que dificulta y encarece la adaptación de una empresa a las condiciones cambiantes durante su ejecución. Los firewalls modernos aprovechan la nube para escalar rápidamente y satisfacer las necesidades cambiantes de la empresa que protegen.

3.7. Firewall de aplicaciones Web

El firewall aplicado en las aplicaciones web permite inspeccionar las peticiones que pueden realizar sobre una web o aplicación web logrando interceptar el tráfico malicioso. Esto alcanza a la aplicación origen y, por lo tanto, salvaguardando la información más sensible complementa los sistemas tradicionales de seguridad perimetral (firewall a nivel de red) ofreciendo protección a nivel de aplicación (nivel 7) donde un firewall tradicional no podrá proteger.

¿Cómo funciona?

Se une al en línea entre el cliente que realiza la conexión y la plataforma de servidores y aplicaciones web de esta forma identifica, a su vez, clasifica cualquier transacción comparándola con patrones conocidos de tráfico malicioso. Así como detecta vulnerabilidades específicas de aplicación mientras registras las conexiones realizadas para posteriores ejercicios de auditoría.

Las conexiones que se identifican potencialmente fraudulentas son interceptadas por el firewall impidiendo así que alcancen el origen de la data y aplicaciones vulnerables.

3.8. Beneficios

Mediante la inspección del tráfico origen/destino de las aplicaciones web protegiendo a esta de potenciales ataques y trafico malicioso los principales beneficios son:

Reducción de costos operativos: Menor consumo de ancho de banda, menores requerimientos de hardware, software y personal autorizado en seguridad y un mejor dimensionamiento de las plataformas:

- Reducción del "Down time" de la plataforma protegida y, en consecuencia, incremento de la capacidad de generación de negocio.
- Colabora en el cumplimiento de la normativa PCI-DSS.
- Evita ataques sobre aplicación no detectados a nivel de red.
- Mayor seguridad en el acceso de los datos.
- Pago por uso.
- Auditoria de seguridad (extracción de accesos y análisis post-mortem de las conexiones recibidas).
- Transparente para la aplicación, fácil implantación e integración.

El firewall de aplicaciones web es una solución de seguridad preventiva de nueva generación especialmente indicado para organizaciones grandes o administraciones públicas que tengan fuertes requerimientos de disponibilidad y confidencialidad de datos:

- Aplicaciones y páginas web con elevados requerimientos de seguridad (fidelización de clientes, suplantación de identidad, reputación de marca).
- Tiendas online y e-commerce.
- Plataformas con BD de alto contenido LOPD (posible inyección de SQL.).
- Protección de las aplicaciones de webmail (especialmente Outlook web Access).
- Empresas con filtración especifica de plataformas.

3.9. Firewall en General

Dentro de las funcionalidades de un Firewall está el de cortar y bloquear, aplicar restricciones, colocar un muro o colocar restricciones de uso a cualquier intento de acceso no autorizado a dispositivos internos privados de nuestra red de datos (LAN) desde las conexiones externas de internet comúnmente llamada WAN.

Establece un filtro a la información que se transporta a través de la comunicación de la red cuando hablamos de un equipo individual se denomina un firewall personal. Pero, cuando se trata de un firewall en una red empresarial para la protección de múltiples equipos se denomina Firewall de red. De tal manera que establece un bloqueo a la comunicación entre equipos basados en reglas, cada regla tiene un determinado patrón de trafico de red y la acción a realizar cuando se detecta. Estas reglas son personalizables y proporcionan control y dan fluidez a la comunicación sobre el uso de la red.

Un firewall puede ser un programa o un dispositivo Hardware o algún tipo de restricción física por ejemplo el sistema operativo Windows o Linux Firewall son ejemplos de firewall de software ZyXELZyWALL USG o SonicWall TZ firewall son ejemplos de firewall de hardware.

3.10. Funcionalidad de un Firewall

Como ya lo indicamos líneas arriba actúa bloqueando el tráfico no autorizado bajo una política este tipo de política lo establecerá el usuario es decir existen dos políticas: la política permisiva y la política prohibitiva en cada configuración del firewall se enfocará a cada característica que la organización así lo establezca.

3.11. Políticas de Firewall

En este caso solo lo permite las comunicaciones a la red protegida sobre las bases de las peticiones que provienen de los equipos dentro de esa red. Nadie va a poder escanear la red. Desde el exterior solo se ve la dirección IP del cortafuegos, no se verán los recursos dentro de la red, a además de los enlaces entrantes están cerrados y todos los puertos salientes están abiertos.

3.12. Filtrado de Contenido

Esta función permite el filtrado de paquetes, examina los paquetes de comunicación que intentan pasar a través del firewall, comprándolos con las reglas esto determinara como se maneja la comunicación y en todo caso la fluides como se establece las comunicaciones entre equipos y estas reglas están basadas en la dirección IP de origen de los datos.

El filtrado de contenidos permite a los encargados del sistema a bloquear fácilmente algunos tipos de contenidos web sin tener que hacerlo manualmente con cada URL individual.

Se podrán bloquear de sitios web inapropiados y sitios web inapropiados y sitios web de redes sociales de forma rápida y sencilla.

3.13. Servicios Antivirus de red (AV)

En el caso de los firewalls ZyWALL USG se implementa con algún tipo de firewall de software es la primera línea de defensa para proteger la red interna contra ataques que provengan de internet o enlace WAN.

Las empresas deberían considerar activar el servicio de AV en el firewall, ya que en los ordenadores y servidores los AV pueden ser fácilmente desactivados o manipulados por los usuarios creando potenciales riesgos al propio ordenador o incluso a la red.

(AS) Anti-Spam del Firewall: Este servicio contar alas intrusiones de software es decir contra el ataque de phishing y correos electrónicos argados de virus malicioso. La tecnología proviene de la detección de patrón recurrente (RPD) de tal manera que analiza la capacidad a través de millones de nuevos patrones a diario (24x7x365). Para bloquear todos los mensajes enviados se menciona como bloqueo porque existe la posibilidad que el usuario acepte el mensaje bloqueado y libere el spam infectando a todo el sistema, ese es otro capítulo aparte. El antispam se aplica a la IP remitente basado en reputación para eliminar más del 80% del corre4o electrónico no deseado.

3.14. Servicios de IDP

IDP, Intrusion Detección y Prevención, permite al administrador controlar aplicaciones específicas conocidos como troyanos y aplicaciones de puerta trasera que pueden infectar a todo el sistema IDP usa tecnología de inspección profunda de paquetes DPI (*Deep Packet Inspeccion*) y puede llegar a soportar 8000 firma. A esto se añade otra capa critica de seguridad informática y suministra al administrador del sistema la flexibilidad necesaria para bloquear programas específicos que no están permitidos en la red como el intercambio de archivos P2P o la mensajería instantánea. También permite al encargado de sistemas identificar, caracterizar, categorizar, y controlar más de 3000 aplicaciones sociales, juegos, aplicaciones productivas. Los administradores pueden priorizar las aplicaciones productivas y bloquear las no productivas evitando el abuso del ancho de banda, estas solicitudes son muy usuales en los casos que las organizaciones.

Con esta función se logra crear un túnel de comunicación de datos encriptado entre el firewall y el usuario en forma veloz y segura sin necesidad que implementar software adicional en el equipo de usuario.

3.15. VPN Software Cliente

Esta función se realiza a través del software instalado para ello en el ordenador del cliente, con autenticación fuerte, soporta SHA-2 512 bits y tiene conexión rápida al ejecutar.

3.16. FirewallD CentOS 7

Una de las disposiciones incluidas en los sistemas operativos Linux para el aumento de la seguridad y así establecer un control sobre las conexiones entrantes y salientes del sistema. El FirewallD es una parte fundamental en la seguridad de nuestros equipos independientemente del sistema ya que es el guardián que impide que contenido indebido pueda dañar nuestros equipos. Por suerte en sistemas como Linux, el FirewallD ya viene integrado por defecto y nos ofrece multitud de opciones para enfrentarnos a este tipo de situaciones concretamente en CentOS el FirewallD integrado se llama firewall y realiza diferentes tareas de seguridad en nuestro distro de Linux.

Es importante saber dentro del entorno que ya viene establecido este tipo de Firewall nos ofrece a nivel de protección y es importante saber que en CentOS 7 la solución incida a nivel de Firewall se llamada Firewall las cuales nos ofrece las siguientes ventajas:

- Es un cortafuego Dinámico.
- Estable.
- Múltiples opciones de configuración.
- Soporta configuraciones Ipv4, Ipv6 y puentes de Ethernet.
- Podemos definir diversas formas de configuración de firewall (continua y ejecución).

Analizaremos en detalle cómo funciona FirewallD en CentOS 7 y de esta manera comprenderemos su alcance.

3.17. Glosario a la Hora de Usa FirewallD CentOS 7

Antes de ver como se usa firewallD en CentOS 7 existen diversa términos los cuales debemos prestarles total interés ya que estarán en forma continua en CentOS 7.

¿Qué es una Zona?

Es aquella cuya función es definir el nivel de confianza que tendrá la conexión de red. Estas Zonas son administradas por FirewallD en diversos grupos de reglas y una zona puede sr usada por muchas conexiones de red. Existen diversas zonas de FirewallD las cuales son:

- ***Drop:*** Es el nivel de confianza más bajo, ya que todos los paquetes de entradas son rechazados de forma automática y solo se habilita los paquetes salientes.

- ***Block:*** Este nivel de confianza es similar al *Drop*, pero difieren en que los paquetes entrantes son rechazados con mensajes *icmp-host-prohibited* para IPv4 y icmp6-adm-prohibited para IPv6.

- ***Public:*** Este nivel de confianza hace referencia a las redes públicas no confiables, solo se acepta conexiones confiables.

- ***External:*** Es tipo de nivel se utiliza cuando usamos el FirewallD como puerta de enlace y su enmascarado este habilitado para otros routers.

- **DMZ:** Este nivel es usado en equipos situados en una zona DMZ (desmilitarizada) es decir tiene acceso público con restricciones a la red interna solo conexiones aceptadas.

- ***Work:*** Es usado en áreas de trabajo por lo cual la mayor parte de los equipos de la red tendrán acceso a ella.
- **Home:** Nivel usado en un entorno de hogar y son aceptadas a la mayoría de los equipos.
- ***Internal:*** Este tipo de nivel es usado en redes internas por lo que todos los equipos de la red serán aceptados.
- ***Trusted:*** Este es el nivel más alto y confía en todas las conexiones entrantes.

3.18. FirewallD en CentOS

FirewallD es un controlador fron-tend para la tabla iptables que se usa para implementar reglas de trafico de red persistente. Provee una línea de comando e interfaces gráficas y está disponible en los repositorios de la mayoría de las distribuciones Linux. Trabajar con FirewallD tiene dos diferencias principales cuando se compara a trabajar directamente con iptables:

1. Firewalld usa zonas y servicios en lugar de cadenas y reglas.
2. Firewalld administra los grupos de reglas dinámicamente, permitiendo actualizaciones sin tener que romper las sesiones y conexiones.

3.19. Instalar y Gestionar FirewallD

FirewallD está incluido por defecto ene CentOS 7 y en fedora20+ pero viene desactivado controlarlo es igual con otras unidades de systemd.

1. Para iniciar el servicio y habilitar la ejecución de firewallD al inicio del servidor:

Sudo systemctl start firewalld

Sudo systemctl enable firewalld

Para detenerlo y deshabilitarlo:

Sudo systemctl stop firewalld

Sudo systemctl disable firewalld

2. Verifique el estatus del firewallD, la salida debe decirle si se está ejecutando o no running o notó running:

Sudo firewall-cmd –state

3. Para ver el estatus del demonio FirewallD:

Sudo systemctl status firewalld

Salida de ejemplo:

firewalld.service - firewalld - dynamic firewall daemon

Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled)

Active: active (running) since Wed 2015-09-02 18:03:22 UTC; 1min 12s ago

Main PID: 11954 (firewalld)

CGroup: /system.slice/firewalld.service

└─11954 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid

1. Para volver a cargar una configuración de FirewallD:

Sudo firewall-cmd –reload

3.20. Configurar FirewallD

FirewallD está configurado a través de archivos XML. Con la excepción de configuraciones muy particulares, no tendrá que lidiar con los archivos XML ya que podrá usar en cambio firewall-cmd. Los archivos de configuración están ubicados en dos directorios:

/usr/lib/FirewallD tiene las configuraciones predeterminadas como las zonas por defecto y los servicios comunes. Evite actualizarlos porque estos archivos serán sobrescritos cada vez que instala paquetes de actualización de firewallD.

/etc/firewalld tiene los archivos de configuración del sistema. Estos archivos sobrescribirán una configuración predeterminada.

3.21. Conjuntos de configuración

FirewallD usa dos conjuntos de configuración: en ejecución y permanente. Los cambios en la configuración en ejecución no son retenidos tras un reinicio del servidor o después de reiniciar FirewallD, mientras que los cambios permanentes no son aplicados a un sistema en ejecución.

Por defecto los comando Firewall-cmd aplicados sal a configuración en ejecución pero que usan la bandera –permanent establecerán una configuración persistente. Para agregar y activar una regla permanente puede usar uno de estos dos métodos:

1. Agregar la regla tanto al conjunto de configuración permanente como a la configuración en ejecución. Por ejemplo:

   Sudo firewall-cmd --zone=public --add-service=http --permanent

   Sudo firewall-cmd --zone=public --add-service=http

2. Añadir la regla al conjunto permanente y volver a cargar FirewallD. Por ejemplo:

   Sudo firewall-cmd --zone=public --add-service=http --permanent

   Sudo firewall-cmd –reload.-

Nota: El comando de recarga elimina cualquier configuración en ejecución y aplica la configuración permanente almacenada. Debido a que FirewallD administra el conjunto de reglas de forma dinámica, no se interrumpirán las conexiones y sesiones existentes.

3.22. Zonas de Firewall

Las zonas son conjuntos de reglas predefinidas para varios niveles de confianza que probablemente utilizaría en ubicaciones o escenarios comunes (ejemplos: en el hogar, en una red pública, en una red de confianza, etc.). Las distintas zonas admiten distintos servicios de red y tipos de tráfico entrante mientras que niegan todo lo demás. Después de activar FirewallD por primera vez, *public* o "pública" será su zona predeterminada.

Las zonas también pueden ser aplicadas a diferentes interfaces de red. Por ejemplo, con interfaces separadas tanto para una red interna como para el Internet, puede permitir DHCP en una zona interna pero solo HTTP y SSH en una zona externa. Cualquier interfaz que no esté establecida explícitamente en una zona especificada será añadida a la zona predeterminada. Para ver la zona predeterminada ejecute:

Sudo firewall-cmd --get-default-zone

Para cambiar la zona predeterminada puede utilizar:

Sudo firewall-cmd --set-default-zone=internal

Para ver las zonas utilizadas por su(s) interfaz o interfaces de red:

Sudo firewall-cmd --get-active-zones

Ejemplo de una salida:

Public interfaces: eth0

Para obtener todas las configuraciones para una zona específica:

Sudo firewall-cmd --zone=public --list-all

Ejemplo de salida:

public (default, active)
interfaces: ens160
sources:
services: dhcpv6-client http ssh
ports: 12345/tcp
masquerade: no

forward-ports:

icmp-blocks:

rich rules:

Para obtener todas las configuraciones para todas las zonas:

Sudo firewall-cmd --list-all-zones

Salida de ejemplo:

block

interfaces:

sources:

services:

ports:

masquerade: no

forward-ports:

icmp-blocks:

rich rules:

...

work

interfaces:

sources:

services: dhcpv6-client ipp-client ssh

ports:

masquerade: no

forward-ports:

icmp-blocks:

rich rules:

3.23. Trabajar con servicios:

FirewallD puede admitir tráfico con base en reglas predefinidas según servicios de red específicos. Puede crear sus propias reglas personalizadas para un servicio y agregarlas a cualquier zona. Los archivos de configuración para los servicios soportados por defecto están ubicados en /usr/lib/firewalld/services y los archivos para los servicios creados por el usuario estarían en /etc/firewalld/services.

Para ver los servicios disponibles de forma predeterminada:

Sudo firewall-cmd --get-services

Por ejemplo, para habilitar o deshabilitar el servicio HTTP:

Sudo firewall-cmd --zone=public --add-service=http --permanent

Sudo firewall-cmd --zone=public --remove-service=http --permanent

3.24. Permitir o denegar un puerto/protocolo arbitrario

Digamos que queremos permitir o denegar el tráfico TCP en el puerto 12345. Podríamos usar el siguiente comando:

Sudo firewall-cmd --zone=public --add-port=12345/tcp --permanent

Sudo firewall-cmd --zone=public --remove-port=12345/tcp --permanent

3.25. Redirección de puertos

La siguiente regla de ejemplo redirige el tráfico del puerto 80 al puerto 12345 del mismo servidor:

Sudo firewall-cmd --zone="public" --add-forward-port=port=80:proto=tcp:toport=12345

Para redirigir el tráfico en un puerto a otro servidor:

1. Active el enmascarado en la zona deseada:

Sudo firewall-cmd --zone=public --add-masquerade

2. Añada la regla de redirección. En este ejemplo redirigimos el tráfico local en el puerto 80 al puerto 8080 de un servidor remoto ubicada en la dirección IP: 123.45.67.8

Sudo firewall-cmd --zone="public" --add-forward port=port=80:proto=tcp:toport=8080:toaddr=123.45.67.8

Para remover las reglas, sustituya --add con --remove.

Por ejemplo:

Sudo firewall-cmd --zone=public --remove-masquerade

3.26. Construir un conjunto de reglas con FirewallD

A continuación, se provee un ejemplo en el cual se utiliza FirewallD para asignar reglas básicas a su servidor blueHosting suponiendo que lo está utilizando como servidor web.

1. Asigne la zona DMZ como la zona predeterminada a la interfaz eth0. De las zonas ofrecidas, DMZ (zona desmilitarizada) es una de las más apropiadas para comenzar con esta aplicación porque solo admite SSH e ICMP.

Sudo firewall-cmd --set-default-zone=dmz

Sudo firewall-cmd --zone=dmz --add-interface=eth0

2. Agregue las reglas permanentes para el servicio de HTTP y HTTPS a la zona DMZ:

Sudo firewall-cmd --zone=dmz --add-service=http --permanent

Sudo firewall-cmd --zone=dmz --add-service=https --permanent

3. Vuelva a cargar FirewallD para que las reglas surtan efecto inmediatamente:

Sudo firewall-cmd --reload

4. Si ahora ejecuta el comando firewall-cmd --zone=dmz --list-all, la salida debería ser como sigue:

dmz (default)
interfaces: eth0
sources:
services: http https ssh
ports:
masquerade: no
forward-ports:
icmp-blocks:
rich rules:

Esto nos dice que la zona DMZ es la zona predeterminada que aplica en la interfaz eth0, a todos los puertos y fuentes de la red. Se admite el tráfico entrante HTTP (puerto 80), HTTPS (puerto 443) y SSH (puerto 22) y debido a que no hay restricciones en la versión del protocolo IP, esta regla aplicará tanto a IPv4 como a IPv6. No se permite el enmascaramiento y redirección de puertos. No tenemos bloques ICMP, así que el tráfico ICMP es totalmente admitido. Tampoco se emplean reglas en lenguaje rich. Todo el tráfico saliente es permitido.

3.27. Configuración avanzada

Los servicios y puertos están bien para una configuración básica, pero pueden ser limitantes en escenarios más avanzados. Las reglas Rich y las interfaces directas le permiten agregan reglas de firewall completamente personalizadas a cualquier zona para cualquier puerto, protocolo, dirección o acción.

3.28. Reglas Rich

La sintaxis de las reglas en el lenguaje rico (o rich) están documentadas en el manual FirewallD Rich Language. También puede ejecutar man.firewalld.richlanguage desde su terminal para ver la información de ayuda del propio FirewallD. Use --add-rich-rule, --list-rich-rules y --remove-rich-rule con el comando firewall-cmd para administrar estas reglas.

Se presentan algunos ejemplos comunes:

Permitir todo el tráfico IPv4 del host 192.168.0.14:

Sudo firewall-cmd --zone=public --add-rich-rule 'rule family="ipv4"
Source address=192.168.0.14 accept'

Denegar el tráfico IPv4 sobre TCP del host 192.168.1.10 al puerto 22:

Sudo firewall-cmd --zone=public --add-rich-rule 'rule family="ipv4" Source address="192.168.1.10" port port=22 protocol=tcp reject'

Permitir el tráfico IPv4 sobre TCP del host 10.1.0.3 al puerto 80 y redirigirlo localmente al puerto 6532:

Sudo firewall-cmd --zone=public --add-rich-rule 'rule family=ipv4 source address=10.1.0.3 forward-port port=80 protocol=tcp to-port=6532'

Redirigir todo el tráfico IPv4 en los puertos 80 al puerto 8080 en el host 172.31.4.2 (el enmascaramiento debe estar activo en esta zona):

Sudo firewall-cmd --zone=public --add-rich-rule 'rule family=ipv4 forward-port port=80 protocol=tcp to-port=8080 to-addr=172.31.4.2'

Para ver una lista de sus reglas rich actuales ejecute:

Sudo firewall-cmd --list-rich-rules

3.29. Interfaz directa a iptables

Para un uso aún más avanzado, o para expertos en iptables, FirewallD proporciona una interfaz directa que permite pasarle comandos de iptables directamente. Las reglas de Interfaz Directa no son persistentes a menos que utilice el parámetro --permanent.

Para ver todas las cadenas o reglas personalizadas añadidas a Firewall use:

firewall-cmd --direct --get-all-chains

firewall-cmd --direct --get-all-rules “

Bluehosting doccs. (2016). *Introduccion a FrewallD en CentOS*. Consultado en septiembre 2022. Disponible en: https://bit.ly/3KMFZJo

3.30. Niveles de Seguridad en redes

Para poder determinar el grado de seguridad de una red, se impuso la clasificación propuesta por el departamento de defensa de los Estados Unidos de América. Acorde a las especificaciones que hace referencia en su "Libro Naranja" estos niveles imponen los límites y condiciones que deben reunir un sistema completo para alcanzar un esquema determinado de seguridad tanto en Hardware, software de datos los niveles son D, C, B, y A de menor a mayor.

Existen varios métodos para asegurar tus datos como encriptar, preguntas de seguridad, huellas digitales, etc. Pero dependiendo de que tanto se haga para poder Accesar a los datos se clasifica en los siguientes niveles:

Nivel D1:

Este constituye la seguridad más básica, sus características esenciales son:

- No existe protección del Hardware.
- El sistema operativo es fácilmente vulnerable.
- Los usuarios no poseen autenticación de red, ni derechos.
- Ejemplo: MS-DOS, Windows (95-98) Apple, etc.

Nivel C1:

Este subnivel es llamado nivel de seguridad discrecional, es característico de un sistema operativo tipo UNIX en su implementación básica:

- Existe algún nivel de protección para el hardware.
- Los usuarios deberán registrarse en el sistema por medio de nombre y contraseña y por medio de estos tendrá lo derechos de acceso.
- La cuenta de administrador del sistema no posee ninguna restricción.

Nivel C2:

Incluye algunas características adicionales de seguridad, como son:

- Refuerza las restricciones de los usuarios en n la ejecución de algunos comandos de acceso.
- Permite especificar niveles de acceso a los archivos y/o recursos.
- Requiere de auditorías del sistema con la creación de sus registros correspondientes.
- Windows NT fue reconoció para alcanzar este nivel.

Nivel B1:

Es el primero de esta clase, también llamado Protección de Seguridad Etiquetada sus características son:

- Reconoce seguridad multinivel: confidencial, secreta, ultrasecreta, etc.

- Trabaja bajo el mismo control de acceso a "Objetos" cuyos cambios se desea solo pueden ser realizados por su dueño

Este nivel es conocido como Protección estructurada, sus características son:

- Cada Objeto debe encontrarse etiquetado, acorde a la protección necesaria.
- Cada dispositivo podrá tener un nivel de seguridad sencilla o múltiple.
- Establece las pautas de comunicación de un objeto de nivel más elevado de seguridad con otro nivel inferior.

Nivel B3:

También llamado de dominios de Seguridad sus características son:

- Impone Hardware de seguridad.
- Establecimiento de rutas seguras en toda comunicación de usuario.

Nivel A:

También llamado Nivel de Diseño Verificado es el más alto de seguridad, sus características son:

- Niveles de diseño, control y verificación de Hardware y software.
- Existe distribución confiable de Hardware y software es decir desde el fabricante hasta el destino final deberá contar con la seguridad exigida.
- Los diseños deberían verificarse en forma matemática.

4. Seguridad de acceso por redes externas

Desde el inicio de implementación de redes se ha producido una necesidad de acceso a las redes usando diferentes medios de accesibilidad. Esto se debe a que las empresas tienen cada vez redes más distribuidas con oficinas y centros de negocios repartidos en diferentes locaciones geográficas e incluso dentro de un espacio se desarrollan diferentes tipos de comunicación dependiendo la segregación que se haga en cuanto a su política interna.

Se ha intensificado el uso de aplicaciones multimedia que requieren que la red le garantice condiciones de seguridad y confidencialidad para el tráfico de datos que intercambian. Hoy más que nunca la seguridad de los sistemas informáticos se encuentra amenazada sea por:

- Rápido desarrollo de las tecnologías de Red.
- Cambios en los servicios de red y aumento en el uso de estas.
- Crecimiento en la tipología y la infinidad de ataques.

Las redes de computadores son cada vez más importantes para el éxito de los negocios y como soporte en la vida diaria de las personas. Los ataques e intrusiones a través de las redes públicas y privadas son cada vez más frecuentes y pueden causar interrupciones costosas de servicios críticos para la continuidad del negocio, así como perdida de información y perdidas considerables de dinero.

Este tipo de ataques se clasifican en 4 grades grupos:

1. **Interrupción:** Un servicio de comunicación o deterioro del software o secuestro de un pc vía remota por lo que la comunicación se pierde, queda inutilizable o no está disponible.

2. **Interceptación:** Un elemento no autorizado consigue un acceso a un determinado modelo de negocio obtienen el control del computador personal mientras está siendo utilizado.

3. **Modificación:** Además de la perdida de privacidad y del acceso, el atacante consigue modificar los datos sin que el usuario incluso se dé cuenta arrojando con ello la pérdida económica además ya obtenido el control es posible que el siguiente paso sería la destrucción de los datos.

4. **Fabricación:** Es posible que se realice la modificación de los datos o el reemplazo de los mismo y entonces es difícil distinguir entre el original y el "falso".

Los ejemplos más conocidos para este tipo de amenazas por medio de las redes externas son:

- Ataque de Denegación de Servicio.
- *Sniffing.*
- *Man in the Middle*.
- *Spoofing.*
- *Pharming.*

Ataque de Denegación de Servicio (DoS) ***Deny of service***: Es un método de ataque en el cual el atacante toma posesión del equipo o del servicio que se presta ya sea en un ordenador vía remota o dentro del datacenter. Esto causa que un recurso o servicio sea de algún amanera inaccesible, provocando perdida de la conectividad de la red por el consumo del ancho de banda o por medio de sobrecargas de los recursos.

Existe una ampliación a este tipo de ataques, bien llamado ataque distribuido por denegación de servicios (DDoS), a través de una botnet.

- ***Sniffing:*** En este tipo de intrusiones del atacante realiza una tarea más elaborada usa la técnica de la interceptación y consiste en rastrear e interceptar, y luego de tomado el control monitoriza el tráfico de red para luego ir tomando la información más conveniente y confidencial de tal manera que el atacante puede vender esta información para obtener un beneficio económico.

Man in the Middle (mitM): Es el mismo modelo del *snifing* con ciertas variantes el proceso por el cual atacante se hace del servicio y utiliza la interceptación y la modificación de la identidad de los extremos y por tanto recibiendo en los dos sentidos.

Spoofing: Este modelo de taque desarrollado por los atacantes suplantando la identidad o realizando una copia o falsificación de IP, MAC, web o mail.

Pharming: Realizado por el atacante aplicando la técnica de modificación aplican la explotación de una vulnerabilidad en el SW de los servidores DNS o en el de los equipos de los propios usuarios, permite modificar las tablas DNS redirigiendo un nombre de dominio (*domain name*) conocido, a otra maquina (IP) distinta, falsificada y probadamente fraudulenta.

4.1. Tipos de Amenazas

Las amenazas de seguridad causadas por intrusos en redes corporativas pueden ser:

- **Amenaza externa (o de acceso remoto):** Es este tipo de ataques los atacantes externos a la red privada y logran introducirse desde redes públicas el objetivo de ataque son los servidores y routers accesibles desde el exterior y que sirven de pasarela de acceso a la red corporativa

- **Amenaza Interna (o corporativa):** Es realizada por atacantes que acceden son los permisos necesarios y pertenecen a la organización privada de tal manera que comprometen a la seguridad y sobre todo la información sensible en la organización sin embargo también cabe la posibilidad mediante la ingeniería social suplantas dichas identidades y hacen uso de forma externa este ataque.

Propuestas para la Protección ante posibles amenazas Internas:

- Realizar una auditoria detectando las fallas de las redes para realizar un buen diseño de subredes dentro de la red corporativa para se instalarán.

- Subneting, Redes locales virtuales o VLAN, Creación de zonas desmilitarizadas o DMZ.

- Aplicación de políticas administrativas de direccionamiento estático para servidores y routers.

- Monitoreo del tráfico de red y de asignación de direccionamiento dinámico y de las tablas ARP.

- Modificación de acuerdo con una política de seguridad en especial, uso adecuado y manejo de contraseñas por defecto de la administración de servicios.

- Máximo nivel de seguridad en redes Inalámbricas.

4.2. Sistema de Detección de intrusos (IDS)

Es una herramienta de seguridad de software usad para detectar accesos no autorizados a un computador o a una red establece algunas observaciones con realizar algunos métodos:

- Suele disponer de una base de datos de firmas de ataques conocidos.

- Analizan el tráfico de red, comparando firmas de ataques conocidos o comportamientos sospechosos (escaneo de puertos, paquetes mal formados).

- No están diseñados para detener un ataque normalmente se integran con un firewall (encargado de bloquear los paquetes si se detecta si son peligrosos).

- Aportan capacidad de prevención y de alerta anticipada.

Tipos de IDS:

- **HIDS (Host IDS):** protegen un único servidor, PC o Host.

- **NISS (Net IDS):** protegen un sistema basado en red, capturan uy analizan paquetes de red, es decir, son *sniffers* del tráfico de red.

Se arquitectura está formada por:

- La fuente de recolección de datos (un log, dispositivo de red, o el propio sistema el caso de HIDS).
- Reglas y filtros sobre los datos y patrones para la detección de anomalías.
- Dispositivos generadores de informes y alarmas (algunos pueden enviar alertas vía mail o SMS).

4.3. Entendiendo el escenario, amenazas dentro y fuera de la red

Lo más importante en el control de acceso de forma externa o interna a las redes es poder encontrarse, porque las empresas tienen redes distribución en diferente ubicación ya sea como centros de negocios oficinas o el más simple de los almacenes todos con la necesidad de acceso a la red y sistema de la compañía para ello se soportarán mediante varios métodos.

Este entorno de interconexión tan complejo subido a la mayor criticidad de los datos que poseen las empresa y organizaciones. Además, la necesidad de acceso a los datos desde cualquier dispositivo y ubicación, todo ello sin comprometer la integridad y confidencialidad de los datos, ante ello la aparición de innumerables y nuevos puntos débiles de acceso.

En concordancia surgen iniciativas y tecnologías para resolverlas que se engloban dentro de lo que se conoce como Control de Acceso a la Red.

4.4. NAC (Network Access Control)

Las soluciones NAC son diferentes, pero pueden ser clasificadas en dos grupos:

- ***Clieness*:** No necesita ningún software instalado en los dispositivos.
- ***Client-based*:** Un componente de software es preinstalado en los dispositivos para poder asistir al proceso NAC.

Pre-Admisión NAC:

Determina que un dispositivo cumpla con ciertos criterios predeterminados antes de permitir o autorizar al acceso a la red. Si esos criterios no se cumplen, no permite que el dispositivo se conecte a la red, o le asigna un acceso restringido.

La pre-Admisión NAC se encuentra en las diferentes soluciones:

Microsoft NAP, cisco nac, mobiles NAC, IPsec VPN, SSL VPN.

4.5. Estrategia de desarrollo

Existen tres metodologías de implementación de las NMAC basado en donde se inserta del control de la red, así que uno debe decidir cuál de los tres se ajusta más a las características y particularidades de la organización estas estrategias son:

1. **Control en el Perímetro (*Edge Control*):** establece el control de acceso a la red desde el exterior, es decir en el punto donde se conectan los sistemas a esta, por ejemplo, en el switch de una LAN, o en concentrador VPN.

2. **Control Central (*Core control*):** El control de acceso se puede implementar en cualquier punto de acceso a la red, por ejem. Través de un dispositivo que se coloca en medio de la red por el que pasa el tráfico de los equipos cuyo acceso se quiere analizar.

3. **Control en el Clientes (*Client control*):** La implementación de las políticas de seguridad y control de acceso se realiza fundamentalmente en el usuario final, instalando en cada uno de los equipos y sistemas que se dese gestionar de tal manera que controla todas las aplicaciones necesarias para realizar el control como firewalls personales, aplicaciones de control de acceso inalámbrico, control de dispositivos USB.

4.6. NAC Network Admisión Control

Es una solución de control de acceso a redes de cisco, es una arquitectura propietaria que en el lado del cliente se compone de un agente denominado Cisco Trust Agent, software gratuito sus funciones la de recibir la información del estrado de la seguridad el equipo a conectar a la red proporcionando la información recogida para recopilar esta información puede usarse otro tipo de aplicaciones de diferentes fabricantes.

Cisco Lo define como el control de la admisión de la red de cisco (NAC) solución que usa infraestructura en red para hacer cumplir con las políticas de seguridad establecidas por las empresas hacia todos los dispositivos que intentan tener acceso a recurso de computación de la red. Ayuda a la seguridad de los Host cumplan con las políticas corporativas tales como antivirus, software de la seguridad y *patch* (remiendo) de sistema operativo antes de obtener el acceso de red normal.

4.7. Riesgos Potenciales en los Servicios de Red

TCP/IP: es una arquitectura de protocolos que usan los computadores para comunicarse en la red emplean puertos de comunicación o numeración lógica que se asigna para la identificación de cada una de las conexiones de red tanto en el origen como en el destino. Los servicios de red más usuales:

Protocolo de aplicación	Números de puertos	Protocolo de transporte
FTP	20,21	TCP
Telnet	23	TCP
SMTP	25	TCP
DNS	53	UDP (TCP(*))
TFTP	69	UDP
HTTP	80	TCP
POP3	110	TCP
RIP	520	UDP

Figura 1: Servicio por el número de puerto

Fuente: https://www.monografias.com/docs115/introduccion-arquitectura-redes/img13.png

Controles: Análisis y control de puertos: Los sistemas y sus aplicaciones de red ofrecen y reciben servicios a través de dichos puertos de comunicación mediante un análisis exhaustivo a nivel de puertos para proteger nuestras conexiones.

El análisis y control de los puertos se pueden realizar en una maquina local, observando las conexiones y puertos que se encuentren abiertos y que aplicaciones controlan:

- Comando netstat; permite ver el estado de las conexiones en tiempo real.
- Cortafuegos(firewall) personales, como medida de protección frente ataques externos.

En la administración de la red, para ver que puertos y en qué estado se encuentran lo de un grupo de puertos y de equipos:

- Aplicación nmap, permite el escaneo de puertos, aplicaciones y SSOO en un rango de direcciones.
- Cortafuegos y proxys perimetrales, ofrecen protección mediante filtrado de puertos y conexiones hacia y desde el exterior de una red privada.

4.8. Comunicaciones Seguras

Referidos a los protocolos más conocidos sin cifrados protocolos como HTTP, FTP o SMTP/POP.

4.9. Comunicaciones Cifradas

- **SSH (Secure Shell, interprete de ordenes seguras):** permite acceder a maquinas remotas y ejecutar comandos a través de una red Puerto 22.
- **SSL (Segure Sockets Layer, protocolo de capa de Conexión segura) y TLS (Transport layer Security, seguridad de la Capa de Transporte)**, su

sucesor, entre otros, se emplea a través de puertos específicos son: HTTPS, FTPS, SMTP, POP3, etc.

- **IPSEC (*Internet Protocol Security*):** Grupo de protocolos cuya función es asegurar las comunicaciones sobre los Protocolos de Internet (IP9 autenticando y/o cifrando cada paquete IP en un flujo de datos. Se usa para crear VPNs.

4.10. Redes Privadas Virtuales

VPN (Virtual Private Network)

Es una tecnología de red que permite una extensión de una red local de forma segura sobre una red pública, como internet.

Características:

- Conectar dos o más sucursales de una empresa a través de Internet.
- Conexión desde casa al centro de trabajo (teletrabajo).
- Acceso desde un sitio remoto (hotel, biblioteca…9 de un usuario al PC de casa.

Para hacerlo posible de manera segura, las VPN garantizan:

- **Autenticación y autorización:** Mediante la gestión de usuarios y permisos.
- **Integridad:** Los datos enunciados no han sido alterados, con el uso de funciones hash (MD5 o SHA).

- **Confidencialidad:** La información que viaja a través de la red pública es cifrada con DES, 3DES, AES… y solo puede ser interpretada por los destinatarios de esta.
- **No repudio:** Los datos se transmiten firmados.

5. Protocolos de Conmutación y Enrutamiento

Los protocolos de enrutamiento son un grupo de normas que son usadas por los routers cuando se comunica con otro router con el fin de encaminar los datos dicha información se usa para construir y mantener tablas de enrutamiento existen dos formas como se visualizan el enrutamiento:

Enrutamiento estático: La dificultad para mantener tablas estáticas, además que introducir en forma manual en los router la información que se desea enviar, es el router que no puede adaptarse por sí solo a los cambios que puedan producirse sin embargo reúne ciertas características que resulta ventajosos

- Existe una conexión con un solo ISP. En lugar de conocer todas las rutas globales, usa una sola ruta estática.
- Un cliente no desea cambiar la información de enrutamiento dinámico.

Enrutamiento Predeterminado: Es una ruta estática que se refiere a una conexión de salida o Gateway de "Último recurso" el tráfico hacia destinos desconocidos por el router se envía a dicha conexión de salida. Es la forma más fácil de enrutamiento para un dominio conectado a un único punto de salida esta ruta se indica como la red de destino 0.0.0.0/0.0.0.0.

Enrutamiento Dinámico: Las disposiciones protocolares mantienen tablas de enrutamiento dinámicas por medio de mensajes de actualización del enrutamiento, que contienen información acerca de los cambios sufridos en la red, y que indican al software del router que actualice la tabla de

enrutamiento en consecuencia, Intentar usar el enrutamiento dinámico sobre situaciones que no lo solicitan es una pérdida de ancho de banda, esfuerzo, y costos.

5.1. Los algoritmos de enrutamiento

Los algoritmos se dividen en:

1. Vector Distancia

Establece la dirección y la distancia hacia cualquier enlace de red. El establecimiento de su métrica está basado en los que se llama en redes "numero de saltos" toma en cuenta la cantidad de routers. Por lo que tiene que pasar el paquete de datos para llegar a la red destino, la ruta que tenga el menor número de saltos es la que se publicara para ello establecerá lo siguiente:

- Visualiza la red desde la perspectiva de los vecinos.
- Actualizaciones periódicas.
- Emite copias completas o parciales de las tablas de enrutamiento.
- Convergencia lenta.
- Incrementa las métricas a través de actualizaciones.

2. Estado de Enlace

También llamado "primero la ruta libre más corta" (OSP-*Open Shortest Path First),* recrea la topología exacta de toda la red. Su métrica se basa en el retardo, ancho de banda, carga y confiabilidad, de los distintos enlaces posibles para llegar a un destino en base a esos conceptos el protocolo opta por una ruta sobre otra, usan un tipo de publicación llamadas publicaciones de estado de enlace (LSA). El cual intercambian entre routers, mediante estas publicaciones cada router crea una base de datos de la topología de la red completa tratan de ubicar una unión común de la topología de red:

- Cada dispositivo calcula la ruta más corta a los otros routers.
- Las actualizaciones se activan por los eventos (cambios en la topología) de la red.

3. Métrica

Es el análisis en lo que se basa el algoritmo del protocolo de enrutamiento dinámico para elegir y preferir una ruta sobre otra, basándose en eso el protocolo creara la tabla de enrutamiento en el routers, publicando solo las mejores rutas para ello se soportara sobre la creación de métricas para determinar que vía va a utilizar para transmitir un paquete a través de un intercambio

La métrica usada por protocolos de enrutamiento incluye algunos conceptos que detallamos a continuación:

- **Numero de saltos:** Numero de router por los que pasar a un paquete.
- **Pulso:** Retraso en un enlace de datos usando pulso de reloj de PC.

- **Coste:** Valor arbitrario basado en el ancho de banda.
- **Ancho de banda:** Capacidad del traslado de datos de un enlace.
- **Retraso:** Cantidad e actividad existente en un recurso de red, como un router o un enlace.
- **Fiabilidad:** Se refiere al valor de errores de bits de cada enlace de red.
- **MTU (Unidad máxima de transmisión):** Longitud máxima de trama en octetos que puede ser aceptad por todos los enlaces de ruta.

4. Convergencia

Es el objetivo de todos los protocolos de enrutamiento cuando un grupo de enrutadores converge significa que todos sus elementos se han puesto de acuerdo y reflejan la situación real del entorno de red donde se encuentran, la velocidad con la que los protocolos convergen determina la eficacia del protocolo de enrutamiento.

5. Distancia Administrativa y métrica

Es una medida de confianza que se le da cada fuente de información de enrutamiento cada protocolo de enrutamiento lleva asociado una distancia administrativa. Los valores más bajos significan una mayor fiabilidad. Un enrutador puede ejecutar varios protocolos de enrutamiento a la vez, obteniendo información de una red por varias fuentes. En estos casos usara la ruta que provenga de la fuente con menor distancia administrativa de los protocolos de enrutamiento.

Cada protocolo de enrutamiento da prioridad a dos caminos de mayor a menor fiabilidad usando un valor de distancia administrativa. Es preferible un valor bajo por ejemplo una ruta OSPF con una distancia administrativa de 110 prevalecerá sobre una ruta RIP con una distancia administrativa de 120.

Mecanismo como se aprendió la ruta	Distancia administrativa
Red directamente conectada (C)	0
Ruta estática (S)	1
Sumarizada de EIGRP	5
BGP externa	20
EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
Routing bajo demanda	160
EIGRP externo	170
BGP interno	200
Desconocido	255

Este valor no es configurable

Las rutas con distancia 255 no se utilizan

Figura 2: Tabla de distancias administrativas usada por CISCO

Fuente: https://www.aulaclic.es/redes/secuencias/diapo/nueve/Diapositiva80.PNG

Algunos protocolos de enrutamiento dinámico son:

- **RIP:** Protocolos de enrutamiento de Gateway interior por vector distancia.
- **IGRP:** Protocolo de enrutamiento de Gateway interior por vector distancia del cual es propietario CISCO.

- **EIGP:** Protocolo de enrutamiento de Gateway interior por vector distancia, es una versión mejorad de IGRP.
- **OSPF:** Protocolo de enrutamiento de Gateway Interior por estado de enlace.
- **BGP:** Protocolo de enrutamiento de Gateway exterior por vector distancia.

RIP:

Es un protocolo de enrutamiento dinámico de vector de distancia esto quiere decir que su métrica para llegar a una red destino se basa en el número de saltos. Es un protocolo abierto a diferencia de por ejemplo IGRP y EIGRP que son propietario de CISCO, es ideal para redes pequeñas, el número de datos máximo hacia un destino es 15 (Cuando hable de número de saltos, me refiero a la cantidad de routers, por los que tiene que pasar el paquete para llegar a su destino) ya con 15 la red se declara inalcanzable.

Existen dos versiones: Es que RIPv1 es lo que se llama protocolo con clase que significa que cuando publica las tablas de enrutamiento este no adjunta las máscaras de subred.

En cambio, RIP v2 es un protocolo sin clase, que, si adjunta la máscara de subred por lo que permite el uso de VLSM, CDIR, sumarización.

RIP Versión 1:

- Protocolo abierto.
- Distancia administrativa: 120.

- Protocolo con clase.
- Métrica número de saltos.
- Actualizaciones cada 30 segundos.
- Envía las actualizaciones en forma de Broadcast.
- Número máximo de saltos 15.
- Red destino Inalcanzable, se declara como 16 saltos.
- No permite VLSM, CIDR.

RIP Versión 2:

En lo que difiere es lo siguiente, por aquellos demás es lo mismo que la versión 1:

- Protocolo sin clase.
- Envía las actualizaciones en forma de Multicast (224.0.09).
- Permite VLSM, CIDR.

6. Diseño de red basada en simulador

La simulación es la imitación de la funcionalidad de un sistema real durante un intervalo de tiempo, está basado en un modelo de la realidad; después de que el modelo es desarrollado y validado puede ser usado para investigar una gran variedad de cuestionamientos del tipo "¿Qué pasa si...?" acerca del sistema real.

6.1. Cambios en un sistema real simulados con el fin de predecir el impacto en el mismo

La simulación también puede ser usada como una estrategia en la etapa de diseño, antes de que el sistema sea construido, o puede ser usado en ambos casos a la vez, predecir el efecto de un cambio y diseñar variantes de un sistema actual.

Ventajas y desventajas de la Simulación:

Ventajas:

- Nuevas políticas, procedimientos, reglas, flujos de información entre otros pueden ser probados sin interrumpir las operaciones del sistema real.
- Nuevos diseños de hardware, emplazamientos físicos, sistema de transporte, entre otros, pueden ser testados sin comprometer los recursos para su adquisición.
- Probar hipótesis acerca del "¿Qué?" y el "¿Cómo?" De algún fenómeno.

- El tiempo poder comprimido o expandido permitiendo un aumento y disminución de la velocidad de los fenómenos de investigación.
- La comprensión del problema puede ser obtenida a través de la interacción de las variables.
- La comprensión del problema puede ser obtenida a través de la importancia de las variables para el desempeño del sistema.
- Análisis de los cuellos de botella, indicando donde los proceso, materiales, etc. están siendo retrasados en exceso.
- Un estudio de simulación ayuda a entender cómo opera el sistema, no como se cree que opera.
- El poder responder preguntas del tipo ¿Qué pasaría si...? es muy útil para el diseño de nuevos sistemas.

Desventajas:

- La construcción de un modelo no es fácil ni cualquiera puede llegar y hacerlo, requiere una preparación especial.
- Los resultados de la simulación pueden ser difíciles de interpretar.
- Hacer el modelo de simulación y de análisis pueden ser muy caro tanto en tiempo como en dinero.
- Usos de la Simulación.
- Predicción, entrenamiento, Entretenimiento, Mejor comprensión de la situación estudiada; apoyo en la toma de decisiones.

Metodología para Realizar un estudio de Simulación:

- Formulación del problema.
- Planteamiento de objetivos y plan de proyectos.
- Conceptualización del modelo.
- Conjunto de Datos.
- Traducción del modelo.
- Verificación.
- Validación.
- Ejecuciones de producción y análisis.
- ¿más ejecuciones?
- Documentación y reportes.
- Implementación.

6.2. Simulación en el diseño de Redes

Durante el diseño de redes el uso de la simulación permite establecer el comportamiento del sistema de los dispositivos de networking antes de establecimiento físico en la infraestructura, de tal forma tendremos un alto porcentaje de seguridad, de cómo el diseño de los equipos que vamos a utilizar cumple de manera más que satisfactoria sobre las funciones y los objetivos en los cuales fueron concebidos en la etapa del diseño. Además del aprendizaje que se obtiene al tener un continuo entrenamiento y

refrescamiento de los conocimientos al planear situaciones extremas o en todo caso habituales. De tal forma que podamos forzar al sistema para que sucedan situaciones muy parecidas a casos reales a través de los cuales los encargados del sistema podrán a poner a prueba el conocimiento y experimentar nuevas alternativas en la solución de problemas de red y su posible impacto en el mundo real, impacto relativo a costos de implementación, mantenimiento, escalabilidad y satisfacción del usuario final.

6.3. Herramientas más usuales en el caso de simulaciones

En el mercado actual existen simuladores de los cuales se mencionan a continuación sin embargo tomaremos los más importantes:

- Network Simulator Tesbed (NEST).
- Maryland Routing Simulator (MaRS).
- Realistic And Large Network Simulator (Real).
- Network Simulator 2 (ns-2).
- S3 Project / Scalable Simulation Framework.
- Java Simulator (J-Sim).
- Wireless IP Simulator (WIPSIM).
- NCTUns 2.0 Network Simulator / Emulator.
- Packet Tracer.

- SWANS.
- Qual-Net.
- CNET.
- GNS3.
- Kiva.
- FLAN (F-Links And Notes.

FLAN (F-Links And Notes): Es una aplicación desarrollada con JAVA y de licenciamiento publico GNU es de propósito general ya que por medio de java se pueden crear y configurar nuevos dispositivos, aplicaciones o protocolos de red aun así no estén incluidos dentro d ellas librerías del programa, inclusive se pueden realizar modificaciones al código fuente de FLAN.

Funcionalidades: Ventanas de consola en este caso muestra al usuario la información de la red y proporciona información de las acciones que se establecen durante la simulación, mediante un módulo el usuario tiene la posibilidad de ver los acontecimientos de eventos ocurridos en la hoja de diseño permite analizar y seguir las acciones que esos eventos produce.

Packet Tracer ™: Un simulador grafico de redes desarrollado por CISCO como herramienta de entrenamiento para la certificación CCNA14. Packet Tracer que es un simulador de redes de comunicaciones de fidelidad media, que permite crear topologías de red mediante la selección de dispositivos y su respectiva comunicación de fidelidad media que permite crear topologías de red mediante la selección de dispositivos y su respectiva ubicación en un área de trabajo 15, usando una interfaz gráfica.

Funcionalidades: Función de degradación del laboratorio y dispositivos modulares; CLI fácil de usar para el usuario y ayuda integrada de diferentes modelos de dispositivos para la creación de redes personalizadas y manuales de apoyo a un lenguaje internacional en modo simple.

KIVA: Es un simulador de redes basado en JAVA que especifica diferentes esquemas de datos y simular el encaminamiento de paquetes a través de dichas redes.

Funcionalidades: El objetivo del entorno es ayudar en el diseño y la comprensión del funcionamiento de redes de datos y en especial al encaminamiento de paquetes de arquitectura TCP/IP sin necesidad de una infraestructura real de herramientas de análisis de tráfico. KIVANS también cuenta con la capacidad de simulación distintos errores de funcionamiento de las redes como la perdida de paquetes o fallos en las tablas de encaminamiento.

6.4. Modelización de Procesos

Como cavamos de mencionar las empresas usan cada vez más los procesadores de simulación o bien llamados simuladores como parte de un proceso de innovación del negocio o mejora del servicio en actividad, se emplea para la comprensión de situación que se dan en la vida real y permite comprender y analizar el balance de una empresa, así como permite tener una visualización del futuro estado del sistema la pregunta mayor en una simulación debería ser: ¿Qué pasa sí? De tal manera que tendremos la posibilidad de plantear soluciones y proponer sugerencias con el fin a de mejorar los procesos de innovación.

En cada situación la simulación facilita los medios para analizar el sistema y permite un enfoque innovador para lograr mejorar soluciones, por otro lado, permite la representación de los procesos y recursos de productos y servicios en un modelo generalmente dinámico. Es decir, cambian en todo momento desde el establecimiento de nuevas aplicaciones so de un hardware que mejora en el mercado.

Pero para entender el proceso de simulación deberíamos definir que es un proceso el cual se podría definir como una serie de actividades lógicas relacionadas secuencialmente que toma un *INPUT* de un administrador, Le añade valor y produce un *OUTPUT* para el cliente. Un proceso generalmente integra más de una función dentro de la estructura organizativa y ello produce un impacto significativo en las funciones de la organización, Cuando un proceso es demasiado complejo para ser un diagrama a nivel de actividad, se divide, frecuentemente en subprocesos y en las cuales se aplican actividades definidas para lograr un objetivo específico en apoyo al proceso principal.

Por último, un sistema será el conjunto de componentes (hardware, procedimientos, funciones humanas y otros recursos) unidos por una especie de interacción regulada para formar un todo organizado.

En la simulación es muy importante establecer unos pasos en el análisis del proceso y estos serían los siguientes:

Representación del proceso: Es uno de los instrumentos más importantes contra la pérdida de tiempo y recursos económicos, para ello se establecerán diagrama de bloque, facilitando una visión rápida y nada complicada del proceso de tal manera que se presenta como un flujo de actividades a través de un proceso en modo de representación gráfica se tratade unir mediante

simbología las actividades paso a paso a todo ello se llama flujograma que básicamente es una ayuda visual del proceso su analogía es el uso de mapas para llegar un destino establecido en el diseño.

Análisis del proceso de Actuación: El objetivo es obtener la actuación referente a cada actividad en el proceso y para el uso de los datos para calcular la actuación del proceso total. La información que podría obtenerse en relación con cada actividad es el tiempo del ciclo total, el tiempo de proceso, el tiempo de espera, el coste y finalmente el rendimiento.

Diccionario del proceso de Conocimiento: Consiste en una forma de almacenar, en tiempo real, la información relativa a un proceso que se organiza de acuerdo a la actividad en el proceso este método es una extensión del análisis del proceso de actuación añadido a los datos de actuación se suelen recopilar los datos de la información relacionada con la actividad los típicos datos son: procedimientos, operativos, instrucciones de trabajo y documentos de formación, ello se guardara en tiempo real y será accesible para futuros proyectos.

Análisis de la variación en el proceso: Indicadores que podrían provocar una variación en el proceso:

- Un lujo de trabajo irregular.
- Diferencias en la complejidad del trabajo individual.
- Cambios en los conductores input.
- Equipos lentos u obsoletos.
- Variación estacional.

Animación del Flujo del Proceso: Con la animación del proceso de flujo a través de la pantalla se convierte en una realidad virtual del proceso así de tal manera pues se visualiza al detalle el flujo de transacción a través del proceso y determina los cuellos de botella que afecta el proceso de actuación por ejemplo a nivel de una empresa puede mostrar a los clientes que están esperando mientras las personas que le dan el servicio estén ocupadas.

Control de Flujo de Trabajo: Se usa para visualizar las transacciones en tiempo real o a lo largo del proceso cada vez que una transacción entra a la actividad esta es registrada en el mismo. Cuando abandona la actividad es desalojada, la información es analizada y computarizada de manera que la situación exacta de cada transacción es conocida en todo momento, generalmente el tiempo máximo de una transacción en cada actividad especifica está previsto en el programa de ordenador de manera que las excepciones son puestas de manifiesto y las prioridades restablecidas.

6.5. Elaboración e implantación de un modelo de simulación

La ejecución de un proyecto de simulación requiere el seguimiento de un proceso secuencial en tres fases:

1. **Evaluación y diseño:** Supone actividades tales como Responsabilidad del promotor del proceso de simulación para así obtener el compromiso de la gerencia:

Determinar las necesidades del proyecto de simulación: Determinara las características del proceso a modelizar (los procesos con altas tasas de

transacciones, pero de flujo directo tiene necesidades distintas que los procesos de baja tasa).

Estimación de recursos necesarios: mediante la elaboración y presentación de un plan financiero y el alcance del presupuesto en el que se estimen costos de tiempo y dinero.

Evaluación y selección de las tecnologías de simulación: Evalúa el coste y el tiempo necesarios en el desarrollo del proyecto.

Dentro de la selección y evaluación de la tecnología de simulación se deben establecer 4 métodos de simulación más comunes:

- Métodos analíticos.
- Métodos continuos.
- Métodos discretos.
- Todos orientados a objetos.

Análisis de las herramientas y las relaciones con los métodos de simulación: Con el fin de obtener sinergias, relacionado con ciertas herramientas y métodos con los flujogramas.

Evaluación y selección del software de simulación: Es de vital importancia.

Recaba la información más pertinente y gestión del proyecto piloto: Supone actividades como análisis y captura de datos de entrada, construcción del modelo piloto y diseño y realización de pruebas.

2. **Ejecución:** Una vez que el proyecto tiene éxito en los programas simuladores la fase de ejecución puede dar comienzo y consiste en las siguientes etapas:

Diseño del proyecto de simulación: Para la complementación de esta etapa es preciso realizar tres tareas:

- **Definir los objetivos:** Que se desean alcanzar con el modelo de simulación. Los más comunes suelen ser análisis del funcionamiento del proceso (si actúa de forma correcta bajo un determinado conjunto de circunstancias en medidas significativas.

- **Definir las restricciones:** Identificar las restricciones que afectan a la simulación la restricción as importantes es el tiempo; equipara la importancia entre proyectar una simulación para la solución de un problema si el tiempo de ejecución se extiende más allá del plazo posible.

- **Definir el campo de actuación del modelo:** Ello incluye aspectos tales como la extensión del modelo, nivel de detalle, grado de precisión, tipos de prueba a realizar y contenido.

Captura y análisis de Datos: Establecer una clasificación distinguiendo entre variables que dependen del tiempo las que dependen de los recursos y las que dependen de determinadas condiciones.

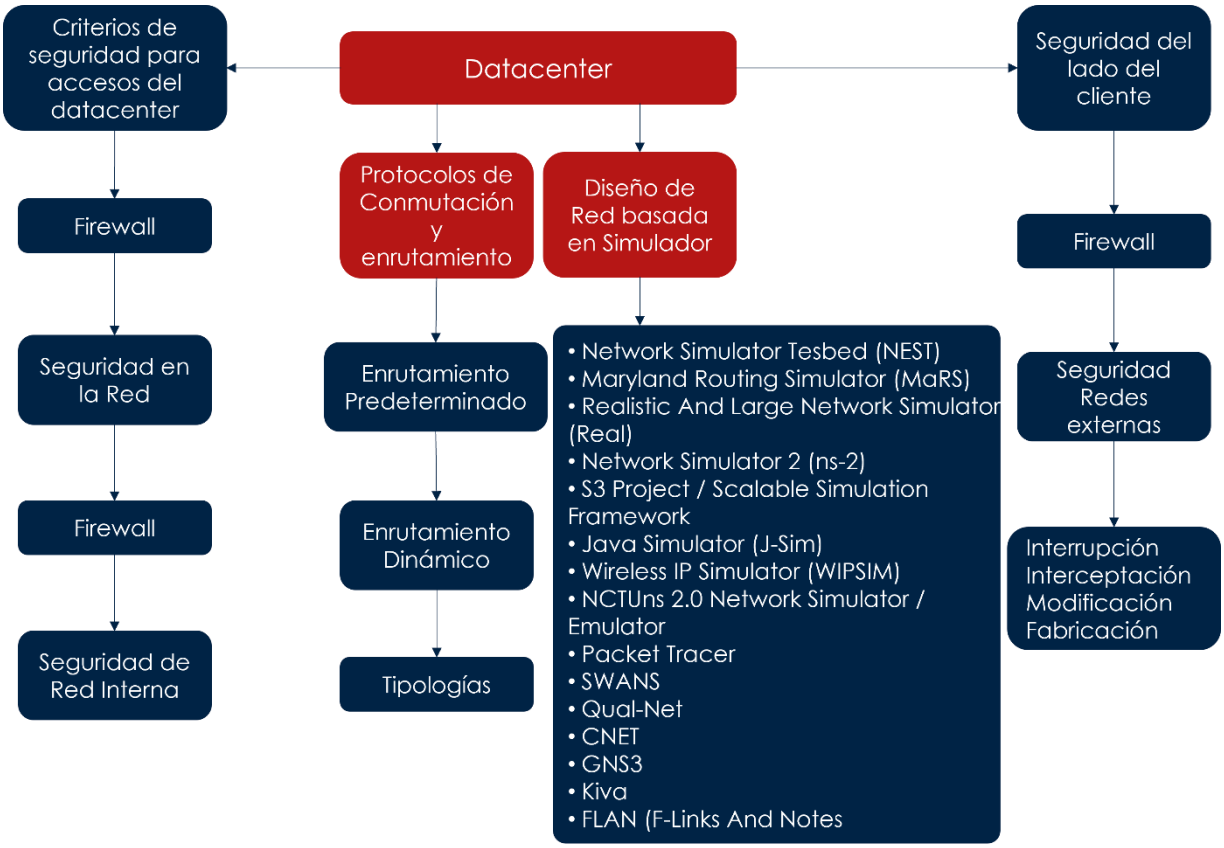
Construcción del Modelo: Las ventajas de simulación no incluye a lo detalles para ponerlos en funcionamiento. Ello permite que en su construcción se vayan realizando refinamientos progresivos hasta conseguir el formato definitivo para ello se plantear ir de menos a más.

Verificación del modelo: Realización de análisis pruebas y presentación de resultados.

3. **Medida de Logros y mejora continua:** Comprende acciones como revisión de metas y principios, debates, establecimiento de informes y procedimientos de retroalimentación y ejecución de procesos de mejora continua.

Cierre

Por medio del siguiente organizador gráfico, se destacan las ideas clave de esta semana:



¿Cómo se establece dentro de la seguridad física el control de acceso en un datacenter?

La seguridad física se establece aplicando las políticas de seguridad previamente determinada como un alcance de una política general de una empresa sin embargo dad las normas internacionales podemos establecer la aplicación de normas como la ISO27001 como lineamiento en el establecimientos de las seguridades en cualquier dimensión del datacenter las

seguridades más conocidas son sensores de movimiento, control de puertas de accesos , usos de CCTVs restricción perimetral , uso de tarjetas y control de accesos soportado documentalmente (firma al ingreso y salida), control biométrico etc.

Referencias bibliográficas

- U.S.A.: TIA. (2005). *Telecommunications Infrastructure Standard for Data Centers.* Consultado en septiembre 2022. Disponible en: https://bit.ly/3bxb9XX

- Abts, Dennis. High performance datacenter networks: architectures, algorithms, and opportunities ISBN: 9781608454020. Disponible en: https://bit.ly/3oqlVSL

- Mark A. Sportack. (2003). *Fundamentos de enrutamiento IP*. Pearson Educación - 354 páginas