



**INFORME DE PRÁCTICAS**

Período académico: P37

|  |  |  |
| --- | --- | --- |
| **INFORME DE PRÁCTICAS DE LA ASIGNATURA** | | |
| **Carrera:**  Desarrollo de Software | **Fecha de ejecución práctica:**  15/10/2024 | **Código:**  Código de materia en el PEA  MAPLPROFE |
| **Asignatura:**  Redes y Diseño de Interfaces | **Nivel:**  Cuarto | **Sede:**  La Magdalena |

|  |
| --- |
| **RESPONSABLE DE LA ASIGNATURA** |
| **Profesor:** Christian Moscoso |
| **Correo:** chdavidm@gmail.com |
| **Teléfono:** 0991831019 |

**1.-TEMA DE LA PRÁCTICA**

Instalación y Configuración de Servidores Proxy

**2.- OBJETIVO GENERAL: 1**

Implementar un servidor proxy para los routers adquiridos en el Instituto Superior Tecnológico “Tecnoecuatoriano”, con el propósito de gestionar eficientemente el tráfico de red, reforzar la seguridad, regular el acceso a internet y supervisar el uso de recursos, asegurando así un entorno digital más controlado y seguro para estudiantes, docentes y personal administrativo.

**3.- OBJETIVOS ESPECÍFICOS: 3**

1. **Implementación del entorno virtual:** Realizar la instalación de VMware Workstation para crear una máquina virtual con Ubuntu Server, asegurando un entorno aislado y controlado para el funcionamiento del servidor proxy.
2. **Instalación y configuración de Squid:** Implementar Squid en Ubuntu, configurando parámetros esenciales como puertos, caché, y reglas de acceso para asegurar un rendimiento óptimo del servidor y una administración eficiente del tráfico de red.
3. **Gestión y monitoreo del acceso a internet:** Establecer reglas de filtrado mediante Squid para regular el acceso a sitios web, alineando su uso con las necesidades académicas y administrativas, mientras se implementan herramientas de registro que permitan supervisar el tráfico y detectar posibles problemas o usos indebidos.

**4.- HERRAMIENTAS, EQUIPOS Y MATERIALES UTIIZADAS**

|  |  |  |
| --- | --- | --- |
| **Herramientas** | **Equipos** | **Materiales** |
| -VMware Workstation  -Ubuntu Server  -Proxy Squid | - Router rompemuros TPLINK  -Computador Para Alojar La Máquina Virtual de Ubuntu Server. | -Cable Ethernet  -Monitor  -Teclado  -Ratón |
|  |  |  |

**5.- MARCO TEÓRICO:**

**¿Qué es un Servidor Proxy?**

Un servidor proxy proporciona una puerta de enlace entre los usuarios e Internet. Es un servidor denominado “intermediario”, porque está entre los usuarios finales y las páginas web que visitan en línea.

Cuando una computadora se conecta a Internet, utiliza una dirección IP. Esto es similar a la dirección de su casa: le indica a los datos entrantes adónde ir y marca los datos salientes con una dirección de devolución para que otros dispositivos se autentiquen. Un servidor proxy es esencialmente una computadora en Internet que tiene una dirección IP propia.

**Servidores Proxy y Seguridad de Red**

Los servidores proxy añaden una capa extra de seguridad para las computadoras al funcionar como filtros web o firewalls, protegiéndolas contra amenazas en línea como el malware. Además, al combinarse con herramientas de seguridad adicionales, como pasarelas web seguras o soluciones para correos electrónicos, permiten un filtrado del tráfico según los niveles de seguridad establecidos o la capacidad de la red y los dispositivos.

Aunque algunos los utilizan para ocultar su ubicación al ver contenido en línea, en entornos empresariales los proxys cumplen funciones clave como:

* Reforzar la seguridad de la red.
* Proteger la actividad en línea de los empleados frente a posibles espías.
* Distribuir de forma equilibrada el tráfico para evitar sobrecargas.
* Controlar el acceso de los empleados a ciertos sitios web.
* Optimizar el ancho de banda mediante el almacenamiento en caché y la compresión del tráfico.

**Cómo Funciona un Servidor Proxy**

El servidor proxy actúa como intermediario entre el dispositivo del usuario e internet al contar con su propia dirección IP. Cuando se realiza una solicitud en línea, esta pasa primero por el proxy, que se encarga de contactar con el servidor web correspondiente. Una vez obtenida la respuesta, el proxy reenvía los datos al navegador del usuario (como Chrome, Safari, Firefox o Edge).

**Tipos de Servidores Proxy**

Existen varios tipos de servidores proxy, cada uno con características diferentes según el nivel de privacidad que ofrecen. A continuación, se presentan los tipos más comunes:

**Proxys Transparentes**

Los proxies transparentes no brindan ningún tipo de privacidad ni seguridad adicional. Al usarlos, los servidores web pueden acceder a su dirección IP real y saber que está utilizando un proxy. Estos proxies se emplean comúnmente para el filtrado de contenido y el almacenamiento en caché, pero no se utilizan para mejorar la seguridad. Es común que se utilicen proxies transparentes en entornos empresariales o educativos.

**Proxys Anónimos**

Los proxies anónimos aseguran que su dirección IP no sea revelada a los sitios web y servicios que visita. En lugar de mostrar su IP real, presentan una dirección IP falsa, lo que lleva a que a veces se les denomine proxies de distorsión. Aunque ocultan su dirección IP, no ocultan el hecho de que se está utilizando un proxy. Si un sitio decide restringir el acceso a usuarios que utilizan proxies, no podrá accederse mientras se utilice un proxy anónimo. Aunque estos proxies ofrecen un control básico sobre la privacidad en línea, no alcanzan el mismo nivel de protección que una VPN, que cifra el tráfico y oculta la dirección IP.

**Proxys de Gran Anonimato**

Los proxies de gran anonimato, también conocidos como proxies de élite, representan una mejora sobre los proxies anónimos. Además de ocultar su dirección IP, estos proxies también disimulan el uso de un proxy ante los sitios web. Esto significa que los sitios no podrán detectar que se está utilizando un proxy. Logran esta protección adicional al cambiar periódicamente su dirección IP y eliminar cualquier rastro de que están actuando como proxies. Son considerados el tipo de proxy más seguro.

**Proceso de Configuración**

La configuración de un proxy puede hacerse a través de la configuración del sistema operativo o directamente en el navegador. Sin embargo, iniciar el proceso en el navegador puede requerir completar la configuración en el sistema operativo. Para configurar un proxy, es necesario ingresar la dirección del proxy y otros datos relevantes en la configuración de proxies del equipo o del navegador. Para obtener más detalles, se puede consultar una guía paso a paso que explique cómo establecer la configuración de proxies en sistemas Windows, macOS y en los principales navegadores.

**6.- PROCEDIMIENTO:**

**1. Instalación de VMware Workstation**

* Descargar VMware Workstation desde el sitio oficial.
* Ejecutar el archivo de instalación y seguir las instrucciones.
* Reiniciar el equipo si es necesario.

**2. Creación de la Máquina Virtual con Ubuntu Server**

* Descargar la imagen ISO de Ubuntu Server desde la página oficial.
* Abrir VMware Workstation y seleccionar "Crear nueva máquina virtual".
* Elegir "Instalación típica" y cargar la imagen ISO de Ubuntu Server.
* Asignar un nombre y ubicación a la máquina virtual.
* Configurar la memoria RAM y núcleos de CPU asignados (recomendado: 2 GB de RAM y 2 núcleos).
* Configurar el disco duro virtual (recomendado: 20-30 GB).
* Se Selecciona la red como "Bridged" para acceso a la red local.
* Encender la máquina virtual y seguir los pasos del instalador de Ubuntu para completar la instalación.

**3. Actualizar el Sistema Operativo**

* Se Accede a la terminal o vía SSH.
* Se Ejecuta: *sudo apt update && sudo apt upgrade -y*

**4. Instalar herramientas esenciales**

* Se Ejecuta: *sudo apt install net-tools curl openssh-server -y*

**5. Instalar el Servidor Proxy Squid**

* Se Ejecuta: *sudo apt install squid -y*

**6. Verificar el estado del servicio Squid**

* Se Ejecuta: *sudo systemctl status squid*

**7. Iniciar y habilitar Squid**

* Se Ejecuta: *sudo systemctl start squid, sudo systemctl enable squid*

**8. Editar el archivo de configuración de Squid**

* Se Ejecuta: *sudo nano /etc/squid/squid.conf*

**9. Modificar la configuración**

* Asegúrarse de que el puerto de escucha sea el proporcionado por squid y añade las reglas de acceso necesarias.
* Guardar y salir
* Presiona Ctrl + O para guardar y Ctrl + X para salir.

**10. Verificar la configuración**

* Se Ejecuta: *sudo squid -k parse*

**11. Reiniciar Squid**

* Se Ejecuta: *sudo systemctl restart squid*

**12. Configurar Proxy en el Navegador**

* En el navegador web, acceder a las opciones de red.
* Configurar el proxy manualmente con la IP del servidor y el puerto asignado.

**13. Verificar la conexión**

* Se Abre el navegador y accede a un sitio web para confirmar que el tráfico se enruta a través del servidor proxy.

**14. Revisar los registros de Squid**

* Ejecuta: *cat /var/log/squid/access.log*

**15. Monitorear el rendimiento de Squid**

* Ajustar la configuración según sea necesario.
* Revisar periódicamente los registros para detectar problemas o patrones inusuales.

**7.-TABULACIÓN Y DATOS: (sacar información de las medidas mínimas de cada elemento expuesto a trabajo)**

|  |  |
| --- | --- |
| Elemento | Medidas Mínimas |
| VMware Workstation | 4 GB de RAM (mínimo), 1 CPU (mínimo), 30 GB de espacio en disco (mínimo). |
| Ubuntu Server | 1 GB de RAM (mínimo), 2.5 GB de espacio en disco (mínimo). |
| Proxy Squid | 512 MB de RAM (mínimo), CPU de 1 GHz (mínimo), 100 MB de espacio en disco. |
| Router rompemuros TP-LINK | Soportar al menos 10 dispositivos simultáneamente, velocidad de 300 Mbps (mínimo). |
| Computador para Alojar la Máquina Virtual | 8 GB de RAM (recomendado), procesador de 2 núcleos (mínimo), 500 GB de espacio en disco. |
| Cable Ethernet | Al menos Cat5e para soportar velocidades de hasta 1 Gbps. |
| Monitor | 1024x768 píxeles. |

**8.- ANÁLISIS DE RESULTADOS:**

La actividad de instalación y configuración del servidor proxy en los routers adquiridos en el Instituto ha logrado cumplir con los objetivos establecidos, implementando de manera efectiva una capa de seguridad que resguarda la red interna del instituto de amenazas externas, como malware y accesos no autorizados. Asi mismo, se han creado políticas de filtrado que regulan el acceso de empleados y estudiantes a determinados sitios web, fomentando un uso responsable de los recursos de Internet. La configuración de Squid para almacenar en caché las solicitudes más frecuentes ha permitido optimizar el ancho de banda, disminuyendo su uso y mejorando los tiempos de carga de los sitios más visitados.

El uso de herramientas de monitoreo, como el análisis de registros, ha ofrecido información valiosa sobre los patrones de tráfico, evidenciando un aumento en la eficiencia de la navegación y tiempos de respuesta más ágiles para los usuarios que acceden a recursos ya almacenados en caché. Además, el examen de los logs de Squid ha facilitado la identificación de picos de tráfico y el uso de aplicaciones o sitios específicos, lo que contribuye a una gestión más eficaz de los recursos.

No obstante, se han detectado algunas áreas que pueden mejorarse. A pesar de que se han establecido políticas de filtrado básicas, la creación de listas de control de acceso más detalladas podría perfeccionar aún más el control sobre los sitios permitidos y restringidos. También es fundamental llevar a cabo sesiones de capacitación para que empleados y estudiantes comprendan el propósito del proxy y aprendan a utilizarlo de manera efectiva, además de conocer las políticas de uso. Mantener actualizados Squid y Ubuntu es esencial para protegerse contra vulnerabilidades y aprovechar nuevas funcionalidades que puedan mejorar la seguridad y el rendimiento.

En resumen, la actividad de instalación y configuración de un servidor proxy con Squid ha sido exitosa y ha proporcionado múltiples beneficios al instituto, mejorando tanto la seguridad como el control del acceso a Internet, además de optimizar el uso del ancho de banda. Es importante continuar monitoreando el rendimiento y la actividad de la red, así como realizar ajustes y capacitaciones adicionales para maximizar el valor del servidor proxy en el entorno educativo.

**9.- CUESTIONARIO:**

**¿Cuál es la función principal de un servidor proxy como Squid en una red educativa?**

La función principal de un servidor proxy como Squid es actuar como un intermediario entre los usuarios de la red interna y los servidores de Internet. Al recibir las solicitudes de los usuarios, Squid las procesa y las reenvía a los servidores de destino, filtrando el contenido según las políticas establecidas. Esto permite no solo mejorar la seguridad al bloquear accesos no autorizados y proteger contra malware, sino también controlar y monitorear el acceso a Internet, asegurando que los empleados y estudiantes utilicen los recursos de manera responsable.

**¿Qué puerto utiliza por defecto Squid para escuchar las solicitudes de proxy?**

Squid utiliza por defecto el puerto 3128 para escuchar las solicitudes de proxy. Este puerto es el estándar, pero se puede modificar en la configuración si se desea utilizar un puerto diferente. Es importante asegurarse de que este puerto esté permitido en el firewall de la máquina donde está instalado Squid, para que las solicitudes de los clientes puedan llegar al servidor proxy sin problemas.

**10.- APORTES TÉCNICOS – CIENTÍFICOS:**

* **Efectividad en Ambientes Educativos**

Estudios han mostrado que el uso de proxys como Squid mejora el acceso a recursos digitales y crea un entorno de aprendizaje más seguro y eficiente.

* **Optimización de Recursos de Red**

Investigaciones indican que el almacenamiento en caché puede disminuir el uso de ancho de banda en hasta un 40%, permitiendo una mejor distribución de recursos.

* **Impacto en el Comportamiento de Usuarios**

La regulación del acceso a sitios web mediante proxies puede aumentar la productividad de los estudiantes y reducir distracciones, mejorando el aprendizaje.

**11.- CONCLUSIONES:**

La implementación de un servidor proxy con Squid en un entorno educativo ha resultado ser una medida eficaz para fortalecer la seguridad de la red, optimizar el uso del ancho de banda y regular el acceso a Internet. La funcionalidad de almacenamiento en caché de Squid no solo mejora la velocidad de navegación, sino que también permite a las instituciones gestionar de manera más eficiente los recursos digitales. Además, las políticas de filtrado implementadas ayudan a crear un entorno más seguro y adecuado para el aprendizaje, limitando el acceso a contenido inapropiado y reduciendo el riesgo de amenazas cibernéticas.

Los beneficios observados, como la disminución en el tiempo de carga de recursos y la reducción de distracciones, enfatizan la importancia de utilizar herramientas como Squid en el contexto educativo. La integración de un servidor proxy puede ser un elemento clave para promover una cultura de uso responsable de Internet entre estudiantes y personal.

**12.- RECOMENDACIONES:**

* **Capacitación Continua:** Es esencial proporcionar formación regular a empleados y estudiantes sobre el funcionamiento del servidor proxy y las políticas de acceso. Esto garantizará que todos comprendan su propósito y la importancia de navegar de manera segura.
* **Mantenimiento y Actualización:** Se aconseja mantener actualizados tanto el servidor Squid como el sistema operativo Ubuntu para protegerse contra vulnerabilidades de seguridad y aprovechar nuevas funcionalidades que mejoren el rendimiento.
* **Revisión de Políticas de Filtrado:** Realizar revisiones periódicas de las políticas de filtrado y acceso ayudará a adaptarse a las necesidades cambiantes de la comunidad educativa, asegurando la eficacia del sistema.
* **Monitoreo del Rendimiento:** Implementar herramientas de monitoreo para evaluar el rendimiento del servidor proxy permitirá identificar áreas de mejora y ajustar la configuración según sea necesario.
* **Evaluación de Recursos Digitales:** Considerar la inclusión de más recursos digitales y la utilización de contenido educativo en línea que pueda beneficiarse del almacenamiento en caché optimizará el acceso a información relevante para los estudiantes.

**13.- BIBLIOGRAFÍA:**

*¿Qué es un servidor proxy? Cómo funciona & Cómo usarlo. (s/f). Fortinet. Recuperado el 16 de octubre de 2024, de* [*https://www.fortinet.com/lat/resources/cyberglossary/proxy-server*](https://www.fortinet.com/lat/resources/cyberglossary/proxy-server)

*Belcic, I. (2020, March 11). ¿Qué es un servidor proxy y cómo funciona? ¿Qué es un servidor proxy y cómo funciona?; Avast.* [*https://www.avast.com/es-es/c-what-is-a-proxy-server*](https://www.avast.com/es-es/c-what-is-a-proxy-server)

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | N° de resolución CAS: | | | | Elaborado por: | **Revisado por:** | **Aprobado por:** | | Firma | **Firma** | **Firma** | | Nombre: Christian Moscoso  Cargo: Docente | **Nombre:** Christian Echeverría  **Cargo:** Coordinador | **Nombre:** Elsa Pezo  **Cargo:** Directora Académica | |

**TÍTULO: Myriad Pro**