|  | | |
| --- | --- | --- |
| Jefe de laboratorio | Ing. Raúl Ortiz Gaona, PhD | |
| Técnico de laboratorio | Ing. Andrea Mory | |
| Curso / Ciclo | Séptimo Nivel | |
| Práctica # 13 | Listas de Control de Acceso | |
| Integrantes | John Vacacela, Marisol Peñafiel, Emily Romero, Santiago Armijos | |
|  |  |  |
| 1. ANTECEDENTES | | |
| Muchas veces se necesita negar a permitir el acceso a ciertos recursos que existen en una red. Una forma de hacerlo es utilizando listas de control de acceso ACL (Access Control List).  Un Access Control List (ACL), o Lista de Control de Acceso, es una herramienta fundamental en el ámbito de las redes informáticas para gestionar y controlar el flujo de tráfico de datos. Se trata de una lista de reglas o directrices que se aplican a un conjunto específico de datos, con el propósito de determinar si se permite o se deniega su paso a través de una red. Estas reglas pueden basarse en diversos criterios, como direcciones IP de origen o destino, números de puerto, protocolos de comunicación, entre otros.    Figura 1. Uso de ACL  Las ACL se configuran y aplican en dispositivos de red, como routers, switches y firewalls, y desempeñan un papel crucial en la seguridad y gestión de la red. Al establecer criterios específicos, las ACL permiten a los administradores de red definir políticas de acceso, dictando qué dispositivos o usuarios tienen autorización para acceder a determinados recursos o servicios y cuáles están restringidos.  Además, las ACL se utilizan para prevenir tráfico no deseado o no autorizado, lo que contribuye a fortalecer la seguridad de la red. Pueden ser implementadas tanto en entornos empresariales como en redes domésticas, proporcionando un mecanismo flexible y adaptable para personalizar la conectividad de acuerdo con los requisitos específicos de cada red.  **Tipos de Access Control List**  Las Listas de Control de Acceso (ACL) se clasifican en dos categorías principales: ACL estándar y ACL extendida. Estas categorías se diferencian en la amplitud de los criterios que pueden utilizarse para filtrar el tráfico en una red. Aquí se presenta una descripción de ambas:  ACL Estándar   * Las ACL estándar se centran principalmente en la dirección IP de origen del tráfico. Se utilizan para permitir o denegar el tráfico en función de las direcciones IP de origen. Por lo general, se implementan en routers para controlar el acceso de ciertos hosts o redes.   ACL Extendida   * Las ACL extendidas ofrecen una mayor flexibilidad al permitir la especificación de criterios más detallados, como direcciones IP de origen y destino, protocolos, puertos, e incluso tipos de aplicaciones.Se emplean para un filtrado más preciso y específico, permitiendo una gestión más granular del tráfico. Se utilizan comúnmente en routers y firewalls, y son ideales para implementaciones donde se requiere un control detallado sobre los servicios y aplicaciones permitidas.   **Funcionamiento de ACL**  Las Listas de Control de Acceso (ACL) operan mediante declaraciones condicionales que determinan el tratamiento del tráfico de red en un router. Estas declaraciones, similares a las condicionales en programación, desencadenan acciones específicas cuando se cumple una condición determinada. En un router, se toman decisiones de filtrado en dos puntos clave: en la entrada y en la salida del dispositivo.  Cuando un paquete ingresa a la interfaz del enrutador (entrada), las ACL entrantes aplican condiciones antes de que el enrutador tome decisiones sobre el tráfico. Por otro lado, en el punto de salida, las ACL salientes intervienen después de que el enrutador ha tomado decisiones. Las condiciones de filtrado pueden permitir o denegar ciertos tipos de tráfico, y se aplican secuencialmente a cada paquete que pasa por la interfaz. | | |
|  |  |  |
| 1. OBJETIVO | | |
| El objetivo de la práctica es el siguiente:   1. Impedir que una red tenga acceso a otra red. | | |
|  |  |  |
| 1. EQUIPO Y MATERIALES | | |
| 2 ruteadores  2 switches  4 PCs  9 cables directos  1 cable cruzado  1 cable de consola | | |
|  |  |  |
| 1. DISEÑO DE LA RED CON MÁSCARA DE SUBRED DE LONGITUD FIJA | | |
| **Datos:**  Se desea que la red con dirección 192.168.0.0 no pueda acceder a la red con dirección 172.16.0.0, y que la red con dirección 192.168.1.0 sí pueda acceder a la red 172.16.0.0 | | |
|  |  |  |
| 1. INSTALACIÓN Y CONFIGURACIÓN DE LOS EQUIPOS | | |
| 1. Conectar los equipos como se indica en la Figura 1. 2. Configurar las PCs. 3. Configurar las interfaces de red de los enrutadores. 4. Configurar enrutamiento dinámico RIP en los enrutadores 5. Impedir que la red 192.168.0.0 no pued acceder a la red 172.16.0.0   Router(config)# access-list 101 deny ip 192.168.0.0 0.0.0.255 172.16.0.0 0.0.0.0 Router(config)# interface gigabitEthernet 0/0  Router(config-if)# ip access-group 101 out   1. Comprobar conectividad 2. Permitir que la red 192.168.1.0 sí pueda acceder a la red 172.16.0.0   Router(config)# access-list 101 permit ip 192.168.1.0 0.0.0.255 172.16.0.0 0.0.255.255   1. Volver a probar la conectividad Luego, los estudiantes configurarán NAT con dos redes LAN conectadas al enrutador R1, con direcciones de red privadas clase A y B respectivamente.     *Figura 1. Topología de la red* | | |
|  |  |  |
| 1. RESULTADOS OBTENIDOS | | |
| 1. **Diseño de Topología**   En el transcurso de la ejecución de esta práctica, llevamos a cabo la creación de una estructura de red que involucra la interconexión de dos redes distintas. Este entorno se caracteriza por la presencia de dos routers que facilitan la comunicación, estableciendo así una conexión fluida entre los sistemas y servicios esenciales, como el servidor FTP y el servidor web. La confección de esta estructura se materializa a través de la configuración de dos redes independientes, las cuales se interconectan a través de un cable serial que conecta los routers. Este enlace entre los routers se convierte en el medio clave para facilitar el flujo de datos entre las redes y posibilitar la interacción efectiva con los servidores FTP y web. Este diseño de red, implementa las bases para la posterior implementación y configuración de las Listas de Control de Acceso (ACL), lo cual será crucial para controlar y gestionar el acceso a los servicios específicos, como el servidor FTP y el servidor web. La interconexión de las redes mediante routers y la preparación de esta infraestructura sirven como cimientos sólidos para la comprensión y aplicación práctica de los conceptos asociados a las ACL en el contexto de la gestión del tráfico en redes informáticas simuladas.    *Figura 2. Diseño de Topología*   1. **Configuración del router Router (R0)**   La configuración del router R0 se inicia con la asignación de direcciones IP a interfaces específicas, estableciendo así la base para una conectividad efectiva. En este proceso, la interfaz Ethernet1/0 es configurada con la dirección IP 10.0.0.1 y una máscara de subred de 255.0.0.0. Adicionalmente, para facilitar la conectividad entre routers, implementamos el protocolo de enrutamiento RIP (Routing Information Protocol).. La implementación del protocolo RIP agrega una capa de flexibilidad y eficiencia al sistema, promoviendo una gestión dinámica y adaptativa de la conectividad en el entorno de la red.    *Figura 3. Direccionamiento del Ethernet*    *Figura 4: Direccionamiento de fastEthernet*    *Figura 5: Asignación RIP*   1. **Configuración del router Router (R1)**   Para la configuración del R1 se optó por mantener las mismas configuraciones que se han realizado previamente en el paso 2 para R0.    *Figura 6: Direccionamiento del Ethernet*    *Figura 7: Direccionamiento del fastEthernet*    *Figura 8: Asignación RIP*   1. **Primera comprobación de conexión**   En este paso se comprueba que los host de ambas redes tengan conexión con los servidores FTP y Web.    *Figura 9. Comprobación conectividad host-servidores*  Como se observa en la Figura 9, los hosts de las redes 192.168.10.0 y 192.168.20.0 tienen conexión con ambos servidores FTP y Web.   1. **Configuración Router (R1)**   El objetivo de nuestra configuración es establecer restricciones de acceso específicas para los hosts ubicados en las redes 192.168.0.0 y 192.168.1.0. En este caso, se pretende limitar el acceso de los hosts de la red 192.168.0.0 exclusivamente al servidor FTP, mientras que los hosts de la red 192.168.0.0 deben tener acceso tanto al servidor FTP como al servidor web.  Los comandos presentados en la Figura 10 reflejan la implementación de restricciones de tráfico TCP procedente de la red 192.168.0.0. Estos comandos configuran reglas específicas en la Listas de Control de Acceso (ACL), las cuales actúan como filtros para determinar qué tipo de tráfico se permite o se deniega. Dichas reglas están diseñadas para restringir selectivamente el acceso desde la red 192.168.1.0 al servidor FTP, proporcionando así un nivel adicional de control sobre la conectividad en la red.    *Figura 10. Configuración access-list para denegar y permitir el acceso*  Esta configuración permite una administración personalizada del tráfico, asegurando que los hosts en la red 192.168.0.0 se limiten al acceso al servidor FTP, al tiempo que los hosts de la red 192.168.20.0 conservan la capacidad de acceder tanto al servidor FTP como al servidor web. Este enfoque estratégico en la gestión de ACL demuestra cómo la implementación cuidadosa de reglas específicas puede adaptarse a los requisitos de seguridad y acceso en una red, proporcionando así un mayor control sobre el flujo de datos. Se procede a permitir el acceso para ambas redes al servidor FTP y solo a la red 192.168.1.0 le damos acceso al servidor Web, esto se muestra en la figura 11.    Figura 11. Configuración access-list para permitir el acceso   1. **Comprobación de conexión host con servidores**   Finalmente para comprobar las configuraciones se procedió a verificar el acceso de los host de las dos redes a ambos servidores:    *Fig 12. Comprobación de la conectividad desde la red 192.168.0.0 con el server 172.1.0.2*    *Fig 13. Comprobación de la conectividad desde la red 192.168.0.0 con el server 172.1.0.3*    *Fig 14. Conexión ftp de la red 192.168.1.0 con el server 172.168.0.2*  Como se observa en la Figura 12, 13 y 14 , la red 192.168.1.0 tiene acceso al servidor Ftp, pero no tiene acceso al servidor Web. | | |
|  |  |  |
| 7. CONCLUSIONES | | |
| En resumen, la práctica centrada en la implementación de Listas de Control de Acceso (ACL) ha proporcionado una comprensión integral de su utilidad para gestionar la conectividad en redes. La configuración precisa de dispositivos mediante reglas ACL ha demostrado ser una herramienta efectiva para filtrar el tráfico, aportando niveles mejorados de seguridad y control.  La capacidad de permitir o denegar el acceso a servicios específicos según las necesidades de la red se evidenció claramente, al conceder permisos selectivos a los hosts de una red mientras se restringía el acceso a otros. Este enfoque estratégico no solo optimiza la seguridad sino también la eficiencia en la conectividad.  La práctica subraya la importancia crucial de una planificación meticulosa al definir reglas, asegurando la alineación de la configuración de las ACL con los requisitos específicos de la red y los servicios deseados. En última instancia, la aplicación hábil de las ACL se presenta como un componente esencial para una conectividad segura y eficiente en entornos de redes informáticas, brindando un control refinado sobre el tráfico y la salvaguarda de la integridad de la red. o. | | |
|  |  |  |
| 8. RECOMENDACIONES | | |
| En esta práctica no se presentaron inconvenientes con la parte de la configuración de los dispositivos. Sin embargo, es importante conocer sobre el funcionamiento del hardware de los equipos para poder resolver los problemas. | | |
|  |  |  |
| 9. FUENTES DE INFORMACIÓN | | |
| [1] Walton, A. (2017, diciembre 27). Listas de Control de Acceso (ACL): Funcionamiento y Creación. CCNA desde Cero. https://ccnadesdecero.es/listas-control-acceso-acl-router-cisco/  [2] Welekwe, A. (2021, abril 8). How to create & configure an access control list. Comparitech. https://www.comparitech.com/net-admin/create-configure-acl/  [3] Configurar ACL de IP de uso general. (2023, noviembre 27). Cisco. https://www.cisco.com/c/es\_mx/support/docs/ip/access-lists/26448-ACLsamples.html | | |