DATOS DE LA ACTIVIDAD							
No. de Actividad:	**2.4**	**Actividad**	Actividad Tipos de Listas de Control de Acceso ACLs				
Unidad:	2: Configuración de seguridad en firewall, Switches, Routers y Access point						
Carrera:	Tgo. en Desarrollo de Software						
Materia	**SEGURIDAD EN ITI**					Clave	MPF3608DSO
Profesor:	Andrés Figueroa Flores						
Alumno:	David Alejandro López Torres					Registro:	17300155
Institución:	**Centro de Enseñanza Técnica Industrial plantel Colomos**						
Semestre:	8	Grupo:	D1	Período:	Feb-Jun 2021	Fecha:	23/04/2021
Compet. Genéricas		4.1, 4.5, 5.2,		Compet. Profesional		CP1-1	

1. Objetivo(s) de la actividad

- Conocer los tipos de listas de control de acceso.

2. Introducción

Los controles de acceso son soluciones de hardware y software que se utilizan para administrar el acceso a recursos y a los sistemas, las listas de control de acceso (ACL) definen el tipo de tráfico permitido en una red informática.

3. Instrucciones (Descripción) de la actividad

1. Para esta actividad puedes trabajar en equipo en parejas, leer la presentación de Power point de ""Listas de Acceso"".

2. Elaborar una tabla con 5 columnas en WORD.

3. Describir (lo más completo posible) las ACLs estándar, y ACLs extendidas, (numeradas y nombradas), ACLs reflexivas, ACLs dinámicas y ACLs basadas en tiempo. Incluir los comandos para configuración básica de cada tipo. (Nota: Considerar para ACLs estándar, extendidas, la presentación, para los demás tipos pueden basarse en Internet o en el PDF Cisco Security)

4. Entrar a https://www.netacad.com/ en el curso de Cybersecurity Essentials y realizar la actividad 7.4.2.4 Packet Tracer: Firewalls del servidor y ACL del router. (agregar en el documento de WORD sólo la impresión de pantalla completa del Packet Tracer al 100%) y subir el archivo PKT junto con la actividad.

5. Usar el archivo de ejemplo de actividades Word, completar todos los datos del encabezado identificando si es Actividad, Investigación o Practica, así como las competencias a desarrollar para esta actividad.

6. Subir el archivo terminado, no se te olvide, la reflexión, agregar la bibliografía en formato APA y dar clic para marcar como entregada la actividad.

4. Resumen

Listas de Acceso Estándar

Las listas de acceso IP estándar comprueban las direcciones de origen de los paquetes que solicitan enrutamiento. El resultado es el permiso o la denegación de la salida del paquete por parte del protocolo, basándose en la dirección IP de la red-subred-host de origen.

```
Router(config)# access-list access-list-number
{permit|deny} {host|source source-wildcard|any}
Router(config)# access-list nº permit|deny origen
[wild-mask]
Router (config-if)# ip access-group nº in|out
```

Listas de Acceso Extendidas

Las listas de acceso IP estándar comprueban las direcciones de origen de los paquetes que solicitan enrutamiento. El resultado es el permiso o la denegación de la salida del paquete por parte del protocolo, basándose en la dirección IP de la red-subred-host de origen.

Numeradas

Las listas de acceso IP estándar comprueban las direcciones de origen de los paquetes que solicitan enrutamiento. El resultado es el permiso o la denegación de la salida del paquete por parte del protocolo, basándose en la dirección IP de la red-subred-host de origen.

IP estándar.....1–99 y 1300–1999
IP extendida.....100–199 y 2000–2699
DECnet.....300–399
XNS estándar....400–499
XNS extendida...500–599
Apple Talk.....600–699
IPX estándar.....800–899
IPX extendida...900–999
Filtros Sap.....1000–1099

```
Router (config)# access-list nº permit|deny
protocolo origen [wild-mask][operación] [puerto
origen] destino [wild-mask][operación] [puerto
destino][established]
```

```
Router (config-if)# ip access-group nº in|out
```

Nombradas

Permite que se les pueda dar a las ACL estándar y extendidas nombres, en lugar de números.

```
Router(config)#ip accesslist[standard|extended][nombre]
Router(config[std|ext]nac1)#[permit|deny][condicio
nes de prueba]
Router(config[std|ext]nac1)#no[permit|deny][condi
ciones de prueba]
Router(config)#Interfaz asociación de la ACL
Router(config-if)#ip access-group[nombre][in|out]
```

Lista de Acceso Reflexivas

Permiten que se filtren los paquetes IP según la información de sesión de capa superior. Generalmente, se utilizan para permitir el tráfico saliente y para limitar el tráfico entrante en respuesta a las sesiones que se originan dentro del router. Solo se pueden definir con ACL con nombre IP extendidas.

```
ip access-group {number|name} {in|out} ip accesslist extended name permit
protocol any any reflect
name [timeoutseconds] ip access-list extended
name evaluate name
```

Lista de Acceso Dinámicas

La configuración de cerradura y llave comienza con la aplicación de una ACL extendida para bloquear el tráfico a través del router. Los usuarios que desean atravesar el router son bloqueados por la ACL extendida hasta que realicen una conexión Telnet al router y sean autenticados. Luego, la conexión Telnet se pierde y se agrega una ACL dinámica de una única entrada a la ACL extendida existente. Esto permite el tráfico por un período de tiempo determinado; son posibles los tiempos de espera inactivo y absoluto

```
username user-name password password interface
<interface> ip access-group {number|name}{in|out}
access-list access-list-number dynamic name
{permit|deny}   [protocol]   {source   sourcewildcard|any}   {destination
destinationwildcard|any} [precedence
precedence][tostos][established] [log|log-input]
[operator destination-port|destination port]
```

Lista de Acceso Basadas en el Tiempo

Se crea un intervalo de tiempo que define las horas específicas del día y de la semana para implementar las ACL basadas en El intervalo de tiempo se identifica con un nombre y luego se remite a él a través de una función. Por lo tanto, las restricciones de tiempo se imponen en la misma función. El intervalo de tiempo depende del reloj del sistema del router.

Se puede utilizar el reloj del router, pero la función funciona mejor con la sincronización de Network TimeProtocol (NTP).

```
“Rango de tiempo”: time-range time-range-name
“Tiempo periódico”: periodic days-of-the-week
hh:mm to [days-of-the-week] hh:mm
“Tiempo absoluto”: absolute [start time date] [end
time date]
“Usado en la ACL”: ip access-list name|number
<extended_definition>time-rangename_of_timerange
```

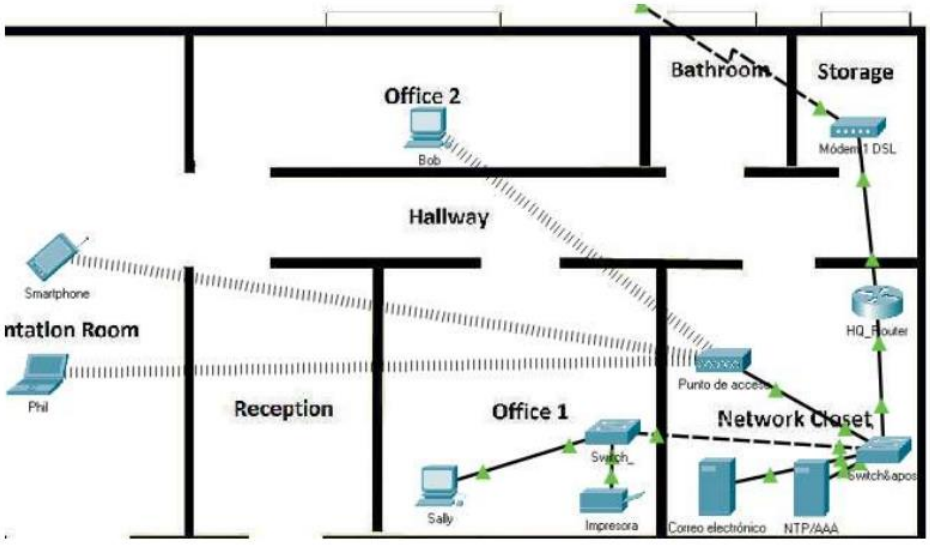
Configuración de Listas de Acceso IP. Recuperado el 22/04/2021 de: https://www.cisco.com/c/es_mx/support/docs/security/ios-firewall/23602-confaccesslists.pdf

5. Material y Equipo

• Computadora
• Acceso a Packet Tracer

6. Desarrollo

• Topología

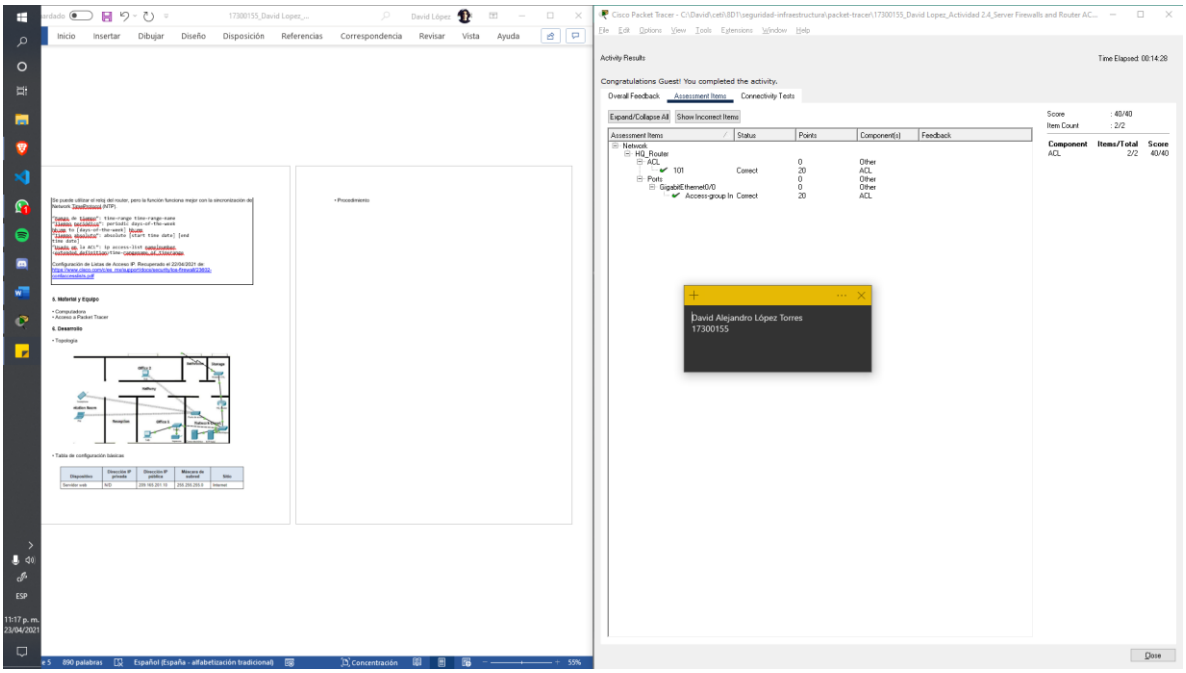


• Tabla de configuración básicas

Dispositivo	Dirección IP privada	Dirección IP pública	Máscara de subred	Sitio
Servidor web	N/D	209.165.201.10	255.255.255.0	Internet

• Procedimiento

Actividad Completa



7. Observaciones

Es recomendable contar con un directorio de puertos conectados y su relación con los dispositivos finales, de maneta que la administración por listas de control sea más intuitiva, dinámica y más eficiente; en particular, cuando se tiene una gran cantidad de dispositivos involucrados en la lista de acceso.

8. Conclusiones

La implementación de listas de accesos requiere de una particular atención en los pequeños detalles, pues un pequeño error de gestión puede representar un gran obstáculo para el desarrollo de las actividades propias de la empresa donde se implementa. Además, tener un orden estricto en la designación de permisos facilita la gestión y mantenimiento de la red y en particular del apartado correspondiente a las listas de acceso. A pesar de estar consideraciones, las ACLs constituyen en gran medida una herramienta base para garantizar la eficiencia de la red y el control del tráfico de la red.

9. Referencias

Configuración de Listas de Acceso IP. Recuperado el 22/04/2021 de: https://www.cisco.com/c/es_mx/support/docs/security/ios-firewall/23602-confaccesslists.pdf