

CAPÍTULO 14

SEGURIDAD: ACL, FIREWALL y DMZ

Contenido

ACL. Listas de control de acceso

Firewall y DMZ

14.1. ACL. Listas de control de acceso

14.1.1. Definición y características

En el ámbito de los dispositivos enrutadores, las ACL son listas de condiciones que se aplican al tráfico que viaja a través de una interfaz del router.

Las ACL indican al router qué tipo de paquetes aceptar o rechazar en base a las condiciones establecidas en ellas. La aceptación y rechazo se pueden basar en la dirección origen, dirección destino, protocolo de capa superior (tcp, udp, icmp, ip, etc.) y números de puerto.

Para cada paquete se comprueba una secuencia de condiciones, donde el orden es esencial, ya que la primera condición que se cumpla determina la acción a realizar y se sale de la ACL, es decir, no se continúa comprobando el resto de las condiciones.

Por lo tanto, una ACL es un grupo de reglas configuradas en el router, que definen cómo se procesan los paquetes que:

- Entren por las interfaces de entrada del router
- Se reenvían a través del router
- Salen por las interfaces de salida del router

Cada interfaz del router puede configurarse como interfaz de entrada y como interfaz de salida, con una ACL distinta para cada caso.

Si no hemos configurado ninguna ACL, todos los paquetes que pasen a través del router tendrán acceso a cualquier parte de la red.

Para modificar una ACL, es conveniente borrarla y volverla a crear.

Finalmente, es importante tener en cuenta, que la última línea de una ACL no aparece de forma explícita y siempre es *denegar cualquiera*.

Tipo de ACL:

- **Estándar:** solamente comprueban la dirección de origen del paquete, pueden ser numeradas o nombradas, el rango válido de números en TCP/IP es 1-99 y 1300-1999
- **Extendidas:** comprueban dirección de origen, dirección de destino del paquete, protocolo y puertos, pueden ser numeradas o nombradas, el rango válido de números es 100-199 y 2000-2699
- **Dinámicas:** sirven para exigir la autenticación del usuario en el router vía Telnet
- **Reflexivas:** se utilizan para permitir el tráfico saliente y para limitar el tráfico de regreso como respuesta al tráfico iniciado en el router
- **Basadas en tiempo:** permiten definir un intervalo de tiempo real, válido para el tráfico de paquetes a través del router

En este capítulo trataremos las dos primeras, ACL estándar y extendidas, que son las más utilizadas.

14.1.2. Funcionamiento de las ACL

El orden en el que se escriben las sentencias de una ACL es fundamental.

Cuando el router recibe un paquete, verifica si cumple o no cada sentencia en el mismo orden en que fueron creadas.

Una vez que se cumple alguna sentencia, ya no se siguen verificando otras sentencias de condición.

Por ejemplo, si una ACL permite todo el tráfico y está ubicada en la parte superior de la lista, ya no se verifica ninguna sentencia que esté por debajo.

```
Router(config)# access-list 1 permit any
```

Al final de la lista se coloca por defecto una sentencia implícita *deny any* (denegar cualquiera). Esta regla no aparece explícitamente pero siempre está, de modo que si no se cumple ninguna regla anterior, denegará el paquete.

Para cada trama recibida, se realiza un procesamiento similar a lo siguiente:

1. Si la trama es aceptada, se desencapsula y se comprueba si hay una ACL asociada a la interfaz de entrada
2. Si existe la ACL y el paquete es denegado se descarta
3. Si no existe la ACL o el paquete es aceptado, se busca la interfaz de salida en la tabla de enrutamiento
4. Se comprueba si la interfaz de salida tiene una ACL asociada
5. Si existe la ACL y el paquete es denegado se descarta
6. Si no existe la ACL o el paquete es aceptado se envía por la interfaz de salida

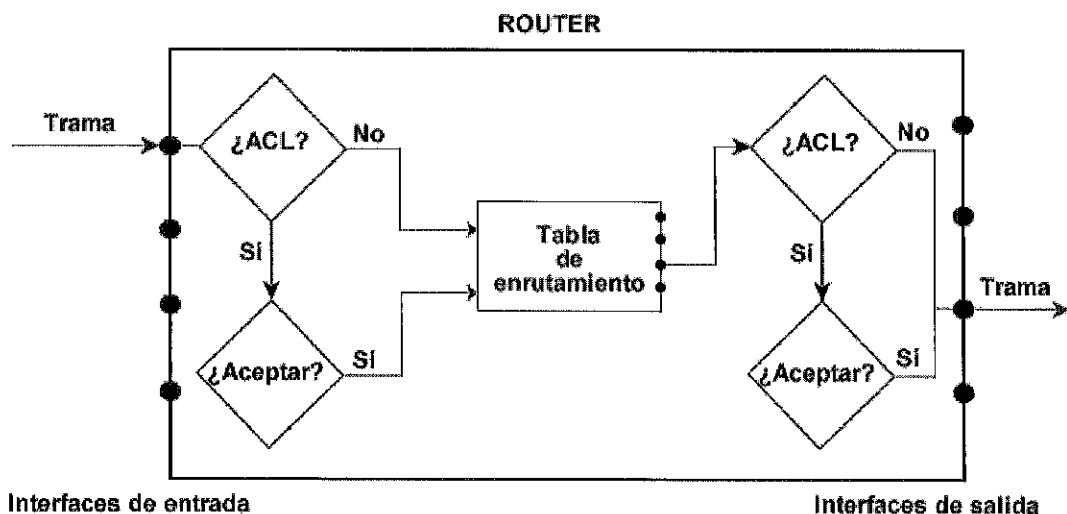


Figura 14.1: Procesamiento de tramas con ACL

14.1.3. ACL estándar

Numeración

Las ACL utilizan un número único no repetido para identificarse.

Dicho número determina el tipo:

- Estándar: se numeran del 1 al 99 y del 1300 al 1999
- Extendidas: se numeran del 100 al 199 y del 2000 al 2699

Máscara wildcard

Se trata de una máscara opuesta a la máscara tradicional, porque intercambia los unos por los ceros y viceversa. Por ejemplo, la dirección 192.168.1.1 cuya máscara normal sería 255.255.255.0 tiene como máscara wildcard 0.0.0.255

La máscara wildcard indica con 0 el bit se compara y con 1 indica que el bit correspondiente se ignora. Por ejemplo, si queremos especificar toda la red 192.168.1.0/24 se hace mediante la dirección 192.168.1.0 y máscara 0.0.0.255. Si queremos especificar solamente el host 192.168.1.1 se hace mediante la dirección 192.168.1.1 y la máscara 0.0.0.0. La máscara 255.255.255.255 indica que todas las direcciones son evaluadas y equivale a *any*.

Creación

En el modo de configuración global:

```
Router(config)# access-list <num_ACL>
                 {permit | deny}
                 <dirección_origen>
```

Este comando crea (si no existe) una ACL estándar, que define una regla de permiso/bloqueo de tráfico. De momento la ACL no está asignada a ninguna interfaz.

Hay 3 formatos posibles para indicar la dirección_origen a la que aplicar la regla:

- **host** <dir_IP>: representa un único host
- <dir_red> <máscara_wildcard>: estos dos valores representan una dirección de red y la máscara en formato *wildcard* (opuesta).
- **any**: representa cualquier equipo

Ejemplo 1: Crear una ACL estándar en el Router, que deniegue el tráfico procedente del host 192.168.1.4 y permita el resto de tráfico:

```
Router(config)# access-list 1 deny host 192.168.1.4
Router(config)# access-list 1 deny 192.168.1.4 0.0.0.0

(Ambas instrucciones son equivalentes)

Router(config)# access-list 1 permit any
```

Asignación de la ACL a una interfaz

Una vez creada la ACL se debe asignar a una interfaz, de lo contrario, la ACL no tendrá efecto. Para ello, hay que seleccionar primero la interfaz con el comando `interface`, y a continuación asociarle la ACL.

```
Router(config)# interface <interfaz>
Router(config-if)# ip access-group <número_ACL> {in | out}
```

El último parámetro indica el tráfico al que se aplica:

in = tráfico a filtrar que **entra** por la interfaz seleccionada

out = tráfico a filtrar que **sale** por la interfaz seleccionada

Ubicación de la ACL estándar

La regla es instalar la ACL estándar lo más cerca posible del destino.

La razón es que las ACL estándar solo especifican la dirección de origen del tráfico.

Ejemplo 2:

Dada la siguiente red, se quiere definir una ACL estándar que impida el tráfico procedente del equipo PC 1.2 y permita el resto de tráfico de salida desde la red 192.168.1.0/24.

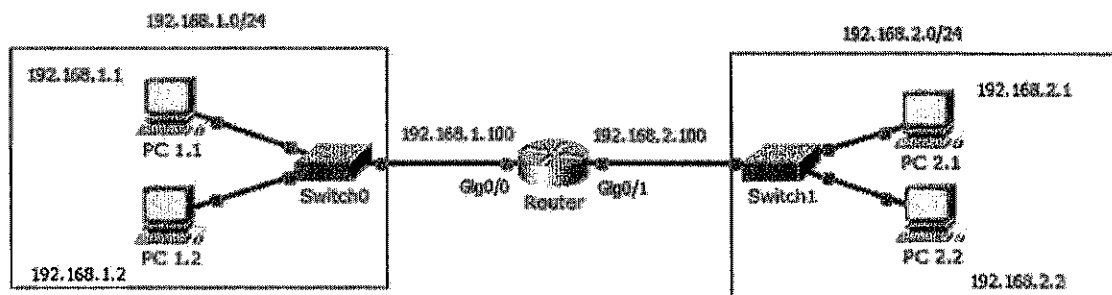


Figura 14.2: Ejemplo 2 de ACL estándar

Como la regla siempre es instalar la ACL lo más cerca posible del destino, la asignamos al interfaz Gig0/1 del Router. Vamos a crear y asignar la ACL:

```
Router(config)#access-list 1 deny 192.168.1.2 0.0.0.0
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)#interface Gig0/1
Router(config-if)#ip access-group 1 out
```

La siguiente figura muestra el proceso completo:

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 1 deny 192.168.1.2 0.0.0.0
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)#interface Gig0/1
Router(config-if)#ip access-group 1 out
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show access-list
Standard IP access list 1
    deny host 192.168.1.2
    permit 192.168.1.0 0.0.0.255
Router#
```

Figura 14.3: Creación, asignación y visualización de ACL estándar

Comprobación

Realizamos un ping desde PC 1.1 al PC 2.1 y comprobamos que funciona. Realizamos un ping desde PC 1.2 al PC 2.2 y vemos qué falla.





Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit	Delete
	Successful	PC 1.1	PC 2.1	ICMP		0.000	N	0	(edit)	(delete)
	Failed	PC 1.2	PC 2.2	ICMP		0.000	N	1	(edit)	(delete)

Figura 14.4: Comprobación de la ACL estándar

Con el comando show access-list podemos ver los paquetes aceptados y rechazados:

```
Router#show access-list
Standard IP access list 1
    deny host 192.168.1.2 (1 match(es))
    permit 192.168.1.0 0.0.0.255 (1 match(es))
Router#
```

Figura 14.5: Estadísticas de paquetes aceptados y rechazados

Eliminar una ACL

```
Router0(config)# no access-list <1-99>
```

Liberar a un interfaz de su ACL

```
Router(config)# interface <interfaz>
```

```
Router(config-if)# no ip access-group <número_ACL> {in | out}
```

14.1.4. ACL extendida

Creación

En el modo de configuración global:

```
Router(config)#
  access-list <num_ACL> [dynamic <nombre>]
  {deny | permit}
  <protocolo>
  <dirección_origen> [<operador> <puerto>]
  <dirección_destino> [<operador> <puerto>]
  [<tipo_icmp>]
  [established]
  [precedence <p>]
  [tos <t>]
  [time-range <tiempo>]
  [remark <comentario>]
```

Este comando crea (si no existe) una ACL extendida, que define una regla de permiso/bloqueo de tráfico. Sólo se puede especificar una ACL por protocolo y por interfaz. Nada más crear la ACL no está asignada a ninguna interfaz.

Parámetros

- num_ACL: número de ACL en el rango 100 al 199 o 2000 al 2699
- dynamic: permite asignar un nombre a la ACL
- protocolo: los más utilizados son eigrp, gre, icmp, ip, ospf, tcp, udp
- dirección_origen y dirección_destino: tiene el mismo formato que en las ACL estándar
- operador puerto: se usan solamente con algunos protocolos como tcp o udp

Operador	Se aplica a paquetes...
eq <puerto>	por un número de puerto igual que el indicado
gt <puerto>	por un número de puerto mayor que el indicado
lt <puerto>	por un número de puerto menor que el indicado
neq <puerto>	por un número de puerto distinto que el indicado
range <puerto1> <puerto2>	por un rango de puertos indicados

Tabla 14.1: Operadores aplicables al puerto en ACL extendida

- tipo_icmp: una vez seleccionado el protocolo ICMP se podrá indicar los tipos *echo*, *echo-reply*, *host-unreachable*, *net-unreachable*, etc.
- established: permite que pase el tráfico TCP si el paquete utiliza una conexión establecida
- precedence: permite filtrar tráfico en función de un nivel de precedencia
- tos: permite filtrar tráfico en función del tipo de servicio
- time_range: permite establecer el intervalo de tiempo en el que la ACL está activa
- remark: sirve para agregar comentarios a la ACL

Ubicación de la ACL extendida

La regla es colocar las ACL extendidas lo más cerca posible del origen del tráfico denegado. De este modo el tráfico no deseado se filtra lo antes posible, sin consumir recursos innecesariamente.

Ejemplo 1:

Dada la siguiente red, crear un ACL extendida que impida el tráfico HTTP desde la red 192.168.2.0/24 a la red 192.168.1.0 y que permita el resto de tráfico.

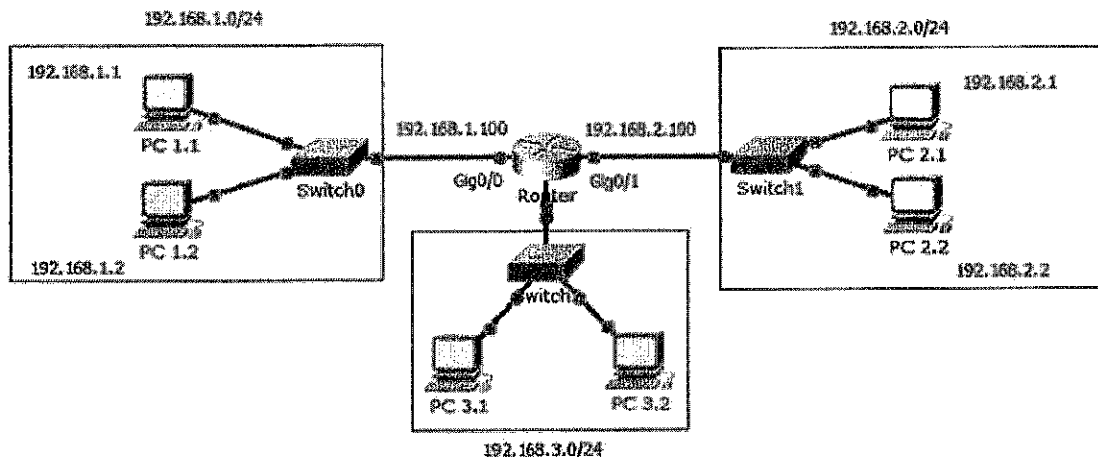


Figura 14.6: Red para ACL extendida

Como la regla siempre es colocar la ACL extendida, lo más cerca posible del origen del tráfico denegado, en este caso es de nuevo la interfaz Gig0/1.

```
Router(config)#access-list 101 deny tcp 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 eq 80
Router(config)#access-list 101 permit ip any any
Router(config)#interface Gig0/1
Router(config-if)#ip access-group 101 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show access-l
Extended IP access list 101
    deny tcp 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 eq www
    permit ip any any
Router#
```

Figura 14.7: Ejemplo 1 de ACL extendida

Ejemplo 2:

En la misma red anterior, crear una ACL que impida el tráfico de ping hacia la red 192.168.1.0

Se trata de impedir el tráfico icmp desde las redes 192.168.2.0 y 192.168.3.0 hacia la red 192.168.1.0. Por tanto, tenemos dos opciones:

- Crear una ACL extendida de entrada y asignarla a las interfaces Gig0/1 y Gig0/2
- Crear una ACL extendida de salida y asignarla a la interfaz Gig0/0

La siguiente figura muestra las dos soluciones:

```
Router(config)#access-list 102 deny icmp any 192.168.1.0 0.0.0.255
Router(config)#access-list 102 permit ip any any
Router(config)#interface Gig0/1
Router(config-if)#ip access-group 102 in
Router(config-if)#exit
Router(config)#interface Gig0/2
Router(config-if)#ip access-group 102 in

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 102 deny icmp any 192.168.1.0 0.0.0.255
Router(config)#access-list 102 permit ip any any
Router(config)#interface Gig0/0
Router(config-if)#ip access-group 102 out
Router(config-if)#exit
Router(config)#exit
```

Figura 14.8: Ejemplo 2 de ACL extendida

Comprobamos que impide el tráfico icmp cuando interviene la red 192.168.1.0:







Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit	Delete
	Failed	PC 1.1	PC 2.1	ICMP		0.000	N	0	(edit)	(delete)
	Failed	PC 1.1	PC 3.1	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC 2.1	PC 3.1	ICMP		0.000	N	2	(edit)	(delete)

Figura 14.9: Comprobación del Ejemplo 2

Las dos soluciones son equivalentes en cuanto al resultado, pero no son iguales. En el primer caso los paquetes son analizados por la ACL en la interfaz de entrada. Pero en el segundo caso los paquetes son enrutados hacia la interfaz de salida Gig0/0 y entonces se evalúa la ACL. En el segundo caso hay más procesamiento porque se consulta la tabla de enrutamiento. La regla de ubicación nos indica que la opción más correcta es la primera.

14.2. Firewall y DMZ

14.2.1. Definición

Un firewall o cortafuegos es un componente de red, hardware o software, cuya finalidad es filtrar tráfico por diferentes aspectos: direcciones de origen y/o destino, puertos de origen y/o destino, protocolos de origen y/o destino.

En general, firewall se define como un mecanismo de seguridad tanto en los accesos como en los envíos de datos, basado principalmente en el filtrado de paquetes.

Existen dispositivos físicos dedicados y programas informáticos que realizan una función semejante. Algunos routers, mediante las ACL recién vistas, pueden realizar también la misma función.

Además, hay cortafuegos que operan en muy distintos niveles del modelo OSI. Un cortafuegos que opere en los niveles más bajos será más fácilmente configurable pero menos flexible. Los que trabajan en los niveles superiores, pueden llegar a investigar el contenido de cada paquete, lo que los hace más lentos pero muy flexibles.

Los primeros elementos que aparecieron en el mercado de redes, con las funciones de cortafuegos fueron los “screening routers”, pues eran capaces de filtrar los paquetes según las características de la red y de la configuración propuesta por el administrador de red.

En la actualidad, como ya se ha comentado, se han ido ampliando sus funciones, que también han ido escalando por las sucesivas capas OSI.

Estos nuevos cortafuegos incluyen nuevos añadidos para la seguridad, como son:

- **Traducción de direcciones (NAT):** consiste en que las direcciones IP utilizadas por los equipos de la Intranet sólo tienen validez dentro de la propia LAN

El cortafuegos se encarga de sustituir cada dirección IP de la Intranet por otras direcciones IP virtuales, protegiendo de este modo contra accesos indeseados a través de direcciones Internet que realmente no existen en la Intranet.

- **Protección frente a virus:** al operar en las capas altas, estos cortafuegos son capaces de analizar la información que fluye hacia la Intranet, pudiendo detectar anomalías en los datos y programas.

- **Auditoría:** El cortafuegos puede auditar recursos concretos de la Intranet y avisar a través de un sistema de mensajería electrónica del intento de violación de algún recurso o de accesos indebidos.

- **Gestión de actividad:** A través de agentes SNMP o DMI, propios de gestión de red, se puede monitorizar el cortafuegos con el fin de realizar informes sobre la actividad de la red.

Los firewall tipo software.

- Firewall personal: para uso doméstico, se instala en cada equipo. Ej.: *Zone Alarm*.

- Firewall específico: para uso en empresa, se instala en el/los equipos que realizarán el filtrado para ofrecer seguridad a la red. Ejemplo: *iptables*, *wipfw*.

14.2.2. Arquitectura de firewalls

Existen diversas arquitecturas de firewalls

Host Dual-Homed

Una arquitectura *dual-homed host* está construida con un equipo con dos interfaces de red y software específico de filtrado. Este host suele denominarse **bastión** y actúa como router entre las dos redes que conoce.

Los paquetes IP de una red a la otra no son enrutados directamente. La red interna puede comunicarse con el dual-homed host, y la red externa también puede comunicarse con él, pero las redes no se comunican directamente.

Se trata de un primer nivel de seguridad en arquitectura de firewalls.

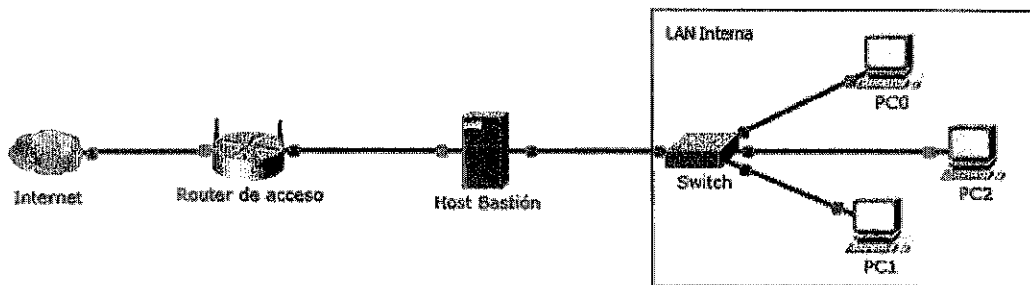


Figura 14.10: Firewall dual-homed

Arquitectura Screened Host (Firewall de 3 patas)

En esta arquitectura se combina un *screening router* con un *host bastión* y el principal nivel de seguridad proviene del filtrado de paquetes mediante listas de control de acceso (ACL).

Las reglas de acceso tienen que ser definidas por el administrador de la red, según las direcciones IP origen y destino y los servicios que van a ser utilizados.

El filtrado de paquetes en el *screening router* está configurado de modo que el *host bastión* es el único sistema de la red interna accesible desde la red externa.

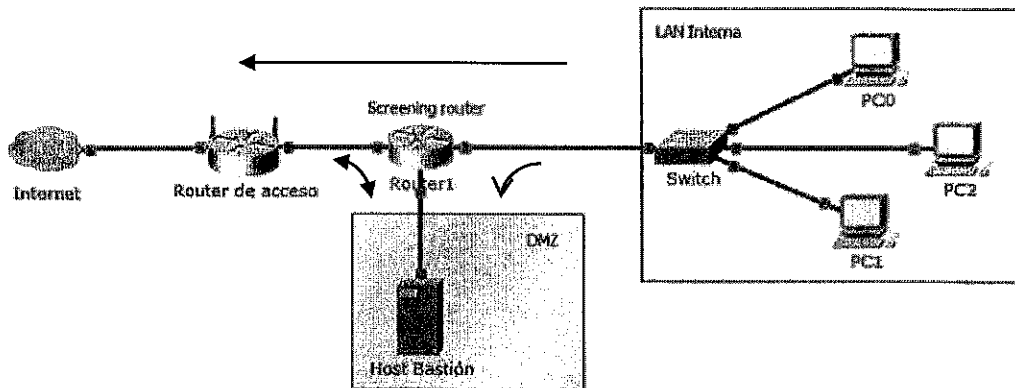


Figura 14.11: Firewall Screened Host (3 patas)

Una zona desmilitarizada (DMZ) o red perimetral, es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet.

El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ solo se permitan a la red externa, de modo que los equipos en la DMZ no pueden conectar con la red interna. Esto permite que los equipos de la DMZ puedan dar servicios a la red externa, a la vez que protegen la red interna, en el caso de que intrusos comprometan la seguridad de los equipos de la zona desmilitarizada.

Arquitectura Screened Subnet

Es la arquitectura más segura. Aumenta un nivel más de seguridad sobre la arquitectura "screened host", agregando un perímetro a la red, que aísla fuertemente la red interna de Internet. Los hosts Bastión son las máquinas más vulnerables en la red. A pesar de los esfuerzos por protegerlas, son las máquinas que pueden ser atacadas, porque son visibles desde la red externa.

Al aislar el host Bastión en un perímetro o red intermedia, se puede reducir el impacto del ataque. Esta arquitectura tiene dos "screening router", cada uno conectado al perímetro. Uno está situado entre el perímetro y la red interna y, otro entre el perímetro y la red externa. Para alcanzar la red interna con este tipo de arquitectura, el atacante debe pasar por ambos routers. Si un atacante logra acceder al host Bastión, deberá lograr pasar por el router interno. La idea es que un ataque a una máquina en el perímetro más no afecte a la red interna.

Perímetro: Es una red adicional entre la red externa y la LAN interna. Si un ataque logra romper el firewall más externo, el perímetro ofrecerá un nivel adicional de protección entre la red interna y el atacante.

Router exterior: Situado entre el mundo externo y el perímetro. Realiza un filtrado de paquetes. Las reglas de filtrado de paquetes son las que protegen las máquinas del perímetro (el host Bastión y el router interno).

Router Interior: Ubicado entre la red interna y el perímetro. Este router no realiza el filtrado principal de paquetes, sino que permite seleccionar servicios de la red interna. Los servicios que este router permite entre la DMZ y la LAN interna no son los mismos que permite el router externo. La razón para limitar estos servicios es que reduce el riesgo de ataque desde el host Bastión hacia la LAN interna.

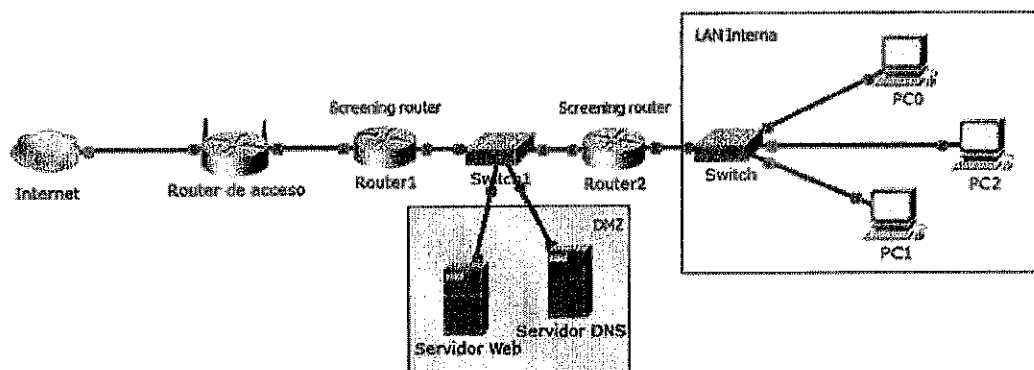


Figura 14.12: Firewall screened subnet