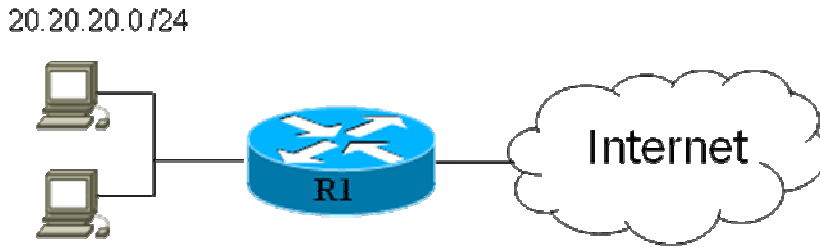


## TIME-BASED ACCESS LISTS

**Introducción.** Esta funcionalidad nos permite implementar reglas en listas de acceso que estarían habilitadas dependiendo de la hora y día de la semana en que sean requeridas. Cabe resaltar que esta opción sólo está permitida para IP (IPv4, IPv6) e IPX y el horario de funcionamiento depende de la hora de sistema del equipo.

### Topología.



### Objetivo.

En la topología mostrada, se requieren dos filtros basados en tiempo. El primer requisito es permitir acceso a un servidor externo (1.1.1.1) durante un periodo estricto del año 2013 que va del 29 de enero a las 9 A.M. al 6 julio a las 6 P.M.. Asimismo, se permite acceso remoto a R1 vía telnet o SSH únicamente en horario de ventanas de mantenimiento que son los martes, jueves y sábados de 1 A.M. a 3 A.M.

### Modo de Operación.

Este tipo de lista de acceso debe ser siempre una lista extendida y los requisitos para la configuración son los siguientes:

1. Crear un periodo de operación (**time range**).
2. Crear las entradas en la línea de acceso que estarán ligadas a los horarios de operación y hacer referencia al periodo configurado.
3. Aplicar la lista de acceso donde sea requerida (PBR, access-group, crypto map, QoS, SLA, etc.)

### Configuración.

Para las time-based access-lists podemos definir dos tipos de rangos de tiempo: absoluto y periódico.

Para el primer requisito necesitamos establecer un periodo absoluto que abarca desde las 9 A.M. del 29 de enero al 6 de julio a las 6 P.M. Esto se realiza de la siguiente manera:

```
R1(config)#time-range SERVER
R1(config-time-range)#absolute start 09:00 29 jan 2013 end 17:59 6 jul 2013
```

Finalmente, configuramos la lista de acceso que hace referencia al periodo configurado anteriormente y la aplicamos como filtro a la entrada de R1.

```
R1(config)#ip access-list extended INSIDE
R1(config-ext-nacl)#permit ip 20.20.20.0 0.0.0.255 host 1.1.1.1 time-range SERVER
R1(config-ext-nacl)#deny ip 20.20.20.0 0.0.0.255 host 1.1.1.1
R1(config-ext-nacl)#permit ip any any
R1(config-ext-nacl)#
R1(config-ext-nacl)#int e0/0
R1(config-if)#ip access-group INSIDE in
```

Como se observa en la configuración, primero establecimos una línea que permite el tráfico hacia el servidor 1.1.1.1 durante el tiempo definido en el periodo que llamamos SERVER. Después de esta línea, agregamos una instrucción que niega este tráfico y finalmente permitimos el resto del tráfico. De esta manera, cuando haya tráfico hacia el equipo 1.1.1.1 fuera del rango de tiempo establecido el tráfico será bloqueado por el filtro INSIDE.

Para el segundo requisito necesitamos establecer un rango de tiempo periódico para las ventanas de mantenimiento:

```
R1(config-if)#time-range MWINDOWS
R1(config-time-range)#periodic Tuesday 01:00 to 03:00
R1(config-time-range)#periodic Thursday 01:00 to 03:00
R1(config-time-range)#periodic Saturday 01:00 to 03:00
```

Para rangos de tiempo periódicos se pueden configurar varias instancias, en rangos absolutos solo se puede configurar uno. Otras opciones para el rango periódico son diario (daily), días laborales (weekdays) y fines de semana (weekend).

Para finalizar, creamos la lista de acceso que permita acceso desde cualquier IP externa o interna al equipo y lo aplicamos dentro de una access-class ya que este tipo de filtro sólo afecta al acceso remoto a R1:

```
R1(config)#ip access-list extended ACCESS
R1(config-ext-nacl)#permit ip any any time-range MWINDOWS
R1(config-ext-nacl)#exit
R1(config)#line vty 0 4
R1(config-line)#access-class ACCESS in
R1(config-line)#transport input telnet ssh
```

El comando “transport input telnet ssh” es el que restringe el acceso al equipo sólo a través de estos dos protocolos. También se podría haber configurado un filtro con access-group haciendo referencia a los protocolos específicamente.

Para comprobar el estado de las entradas en la lista de acceso, se puede utilizar el comando “show access-list” como en los ejemplos:

```
R1#show clock
```

```
*18:18:22.867 PST Sat Apr 28 2012
```

```
R1#sh access-list INSIDE
```

```
Extended IP access list INSIDE
```

```
10 permit ip 20.20.20.0 0.0.0.255 host 1.1.1.1 time-range SERVER (inactive)
```

```
20 deny ip 20.20.20.0 0.0.0.255 host 1.1.1.1
```

```
30 permit ip any any
```

```
R1#show access-list ACCESS
```

```
Extended IP access list ACCESS
```

```
10 permit ip any any time-range MWINDOWS (inactive)
```

Como se puede observar, el acceso remoto al equipo está prohibido por el momento, ya que la línea que permite el acceso está inactiva y por default las listas de acceso niegan todo lo que no está permitido, como se observa a continuación:

```
HOST#telnet 20.20.20.1
```

```
Trying 20.20.20.1 ...
```

```
% Connection refused by remote host
```

```
HOST#
```

```
HOST#ping 1.1.1.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
```

```
U.U.U
```

```
Success rate is 0 percent (0/5)
```

Si cambiamos el reloj de R1 a uno que permita los dos tipos de tráfico veríamos lo siguiente:

```
R1#clock set 1:30:00 13 april 2013
```

```
Apr 13 01:30:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 18:22:40 PST Sat Apr 28 2012 to 01:30:00 PST Sat Apr 13 2013, configured from console by console.
```

```
R1#sh access-list ACCESS
Extended IP access list ACCESS
 10 permit ip any any time-range MWINDOWS (active)
R1#sh access-list INSIDE
Extended IP access list INSIDE
 10 permit ip 20.20.20.0 0.0.0.255 host 1.1.1.1 time-range SERVER (active)
 20 deny ip 20.20.20.0 0.0.0.255 host 1.1.1.1 (8 matches)
 30 permit ip any any (2 matches)
```

Las líneas de las listas de acceso están activas ahora y el tráfico ya está permitido:

```
HOST#ping 1.1.1.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/52/56 ms
HOST#
HOST#
HOST#telnet 20.20.20.1
Trying 20.20.20.1 ... Open
```

User Access Verification

```
Password:
R1>
```

Para más información sobre esta funcionalidad pueden consultar la siguiente página:

[http://www.cisco.com/en/US/docs/ios/12\\_0t/12\\_0t1/feature/guide/timerang.html](http://www.cisco.com/en/US/docs/ios/12_0t/12_0t1/feature/guide/timerang.html)