APACHE SERVER

CONTROL DE ACCESO POR IP O DOMINIO

Salvador Mira

IES Pere Maria Orts

CONTROL DE ACCESO POR IP

En las redes se suele permitir o denegar el acceso a los servicios haciendo uso de firewalls

Algunos servicios implementan o pueden hacer uso de motores propios de control de acceso más allá de los firewalls

Apache incorpora el módulo **mod_authz_host** que permite denegar o permitir el acceso a los recursos basándose en la **IP** de la petición o el **dominio** de petición (en este último caso, es necesaria la resolución inversa)

CONTROL DE ACCESO POR IP

Los recursos compartidos y sus atributos se definen con las directivas **<Directory>**, **<Files>** y **<Location>**

Podemos indicar directivas internas del tipo **Allow** y **Deny** para especificar que se permite o deniega el acceso a cierto recurso

Es importante especificar el orden de precedencia entre **Allow** y **Deny** a través de la directiva **Order**

- Ejemplo: **Order Deny, Allow** evalúa en primer lugar las directivas **Deny** y a continuación las **Allow**

CONTROL DE ACCESO POR IP

Order Allow, Deny:

- En primer lugar evalúa todas las directivas **Allow**, y al menos una de ellas debe encajar o la petición será rechazada.
- A continuación se evalúan las directivas **Deny**, y si alguna encaja, la petición se rechaza.
- Finalmente, si la petición no encaja ni con ninguna directiva **Allow** ni con ninguna **Deny**, la petición se rechaza

MÓDULOS DE APACHE

EJEMPLO: MOD_USERDIR

Order Deny, Allow:

- En primer lugar se evalúan las directivas **Deny**, y si alguna encaja, la petición se rechaza a menos que también encaje con alguna directiva **Allow**
- Las peticiones que no encajan ni con **Allow** ni con **Deny** se permitirán

Match	Allow,Deny result	Deny,Allow result
Match Allow only	Request allowed	Request allowed
Match Deny only	Request denied	Request denied
No match	Default to second directive: Denied	Default to second directive: Allowed
Match both Allow & Deny	Final match controls: Denied	Final match controls: Allowed

CONTROL DE ACCESO POR IP

Ejemplo:

```
<Directory /var/www/html/>
        Order Deny,Allow
        Deny from all
        Allow from 192.168.1.0/25
</Directory>
```

En el ejemplo, estas directivas han sido establecidas en el **VirtualHost** por defecto

CONTROL DE ACCESO POR IP

Directivas **Allow** y **Deny**, ejemplos:

- Limitar o permitir peticiones de un nombre de dominio completo o parcial
  Allow from apache.org
  Allow from .net example.edu

- Limitar o permitir peticiones de ciertas direcciones IP
  Allow from 10.1.2.3
  Allow from 192.168.1.104 192.168.1.205

CONTROL DE ACCESO POR IP

Directivas **Allow** y **Deny**, ejemplos (2):

- Limitar o permitir peticiones de IPs expresadas parcialmente
  Allow from 10.1
  Allow from 10 172.20 192.168.2

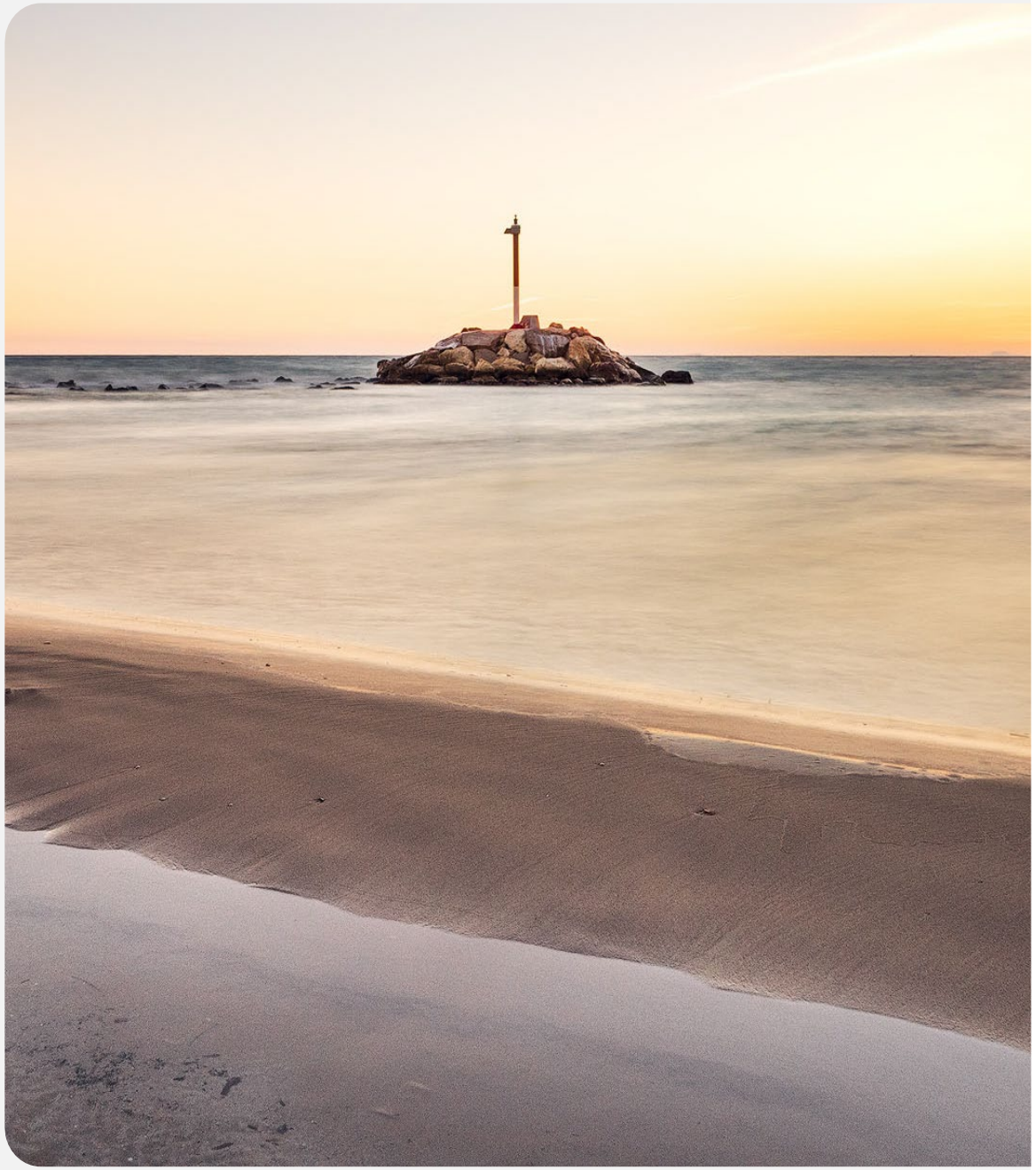
- Limitar o permitir peticiones de redes expresadas con su máscara
  Allow from 10.1.0.0/255.255.0.0

CONTROL DE ACCESO POR IP

Directivas **Allow** y **Deny**, ejemplos (3)

- Limitar o permitir peticiones de redes expresadas con su máscara CIDR
  Allow from 10.1.0.0/16

- Limitar o permitir peticiones IPv6
  Allow from 2001:db8::a00:20ff:fea7:ccea
  Allow from 2001:db8::a00:20ff:fea7:ccea/10



CONTROL DE ACCESO POR IP

Página limitada por reglas de control de acceso