

COMANDOS

en

conf t

hostname R0

enable secret contraseña

line console 0

password contraseña

login

exec-timeout 30

exit

line aux 0

password contraseña

login

exec-timeout 30

exit

line vty 0 4

login local

transport input ssh telnet

exit

Configurar una longitud mínima para las contraseñas

security passwords min-length 8

Crear un usuario con privilegio 15 (administrativo) y contraseña

username nombre_usuario privilege 15 secret contraseña

username nombre_usuario secret contraseña_usuario

do wr

Configurar SSH

ip domain-name **dominio_nombre.com**

crypto key generate rsa -> Generar claves RSA para SSH

How many bits in the modulus [512]: 1024

ip ssh version 2

ip ssh authentication-retries 3 -> Número de intentos permitidos

ip ssh time-out 30

do wr

DHCP

ip dhcp excluded-address **ip_del_router: 192.168.1.1**

ip dhcp pool **nombre**

network **ip_de_la_red: 192.168.1.0 255.255.255.0**

default-router **ip_del_router: 192.168.1.1**

dns-server **servidor: 8.8.4.4**

ex

do wr

VLANS

Switch, en, conf t

vlan 2

name **nombre**

vlan 3

name **nombre**

end

interface FastEthernet0/1

Switch(config-if)# switchport mode access #modo de acceso

Switch(config-if)# switchport access vlan 2 #Asignar la interfaz a la VLAN 2

switch# show vlan

```
int f0/1
switchport access vlan 2
ex
do wr
```

```
int s0/0/0 / int f0/0 / int g0/0
ip add 192.168.1.1 255.255.255.0
no shutdown
do wr
```

Ruteo Estático - seriales

```
clock rate 20000 - 12500
no shutdown
ip route 192.168.1.0 255.255.255.0 10.10.10.2
do wr
```

RIP

se utiliza en redes pequeñas y medianas

Versiones: Existen dos versiones de RIP:

- **RIPv1:** No admite subredes ni VLSM.
- **RIPv2:** Sí admite subredes y utiliza autenticación para mayor seguridad.

R1

```
router rip
version 2
network 192.168.2.0
network 192.168.3.0
ex
do wr
```

R2

```
router rip
version 2
network 192.168.2.0
```

network 192.168.3.0

ex

do wr

PRUEBAS

show ip route | begin Gateway

show ip protocols

BGP

se utiliza en redes grandes e internet

R1

router bgp 100

network 192.168.0.0 mask 255.255.255.0

neighbor 10.10.10.2 remote-as 200

R2

router bgp 200

network 192.168.1.0 mask 255.255.255.0

neighbor 10.10.10.1 remote-as 100

OSPF

compartir rutas dentro de una red

router ospf 9

network 192.168.0.0 0.0.0.0 area 1

network 10.10.10.0 0.0.0.3 area 1

network 10.10.10.16 0.0.0.3 area 1

ex

do wr

—

CR

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname CR

CR(config)#router os

CR(config)#router ospf 9

OSPF process 9 cannot start. There must be at least one "up" IP interface

CR(config-router)#network 192.168.1.0 0.0.0.255 area 1

CR(config-router)#network 10.10.10.0 0.0.0.3 area 1

CR(config-router)#network 10.10.10.8 0.0.0.3 area 1

CR(config-router)#exit

CR(config)#do wr

Building configuration...

[OK]

CR(config)#

COL

Router>conf t

^

% Invalid input detected at '^' marker.

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#router osp

Router(config)#router ospf 9

OSPF process 9 cannot start. There must be at least one "up" IP interface

Router(config-router)#network 192.168.2.0 0.0.0.255 area 1

Router(config-router)#network 10.10.10.8 0.0.0.3 area 1

Router(config-router)#network 10.10.10.16 0.0.0.3 area 1

Router(config-router)#exit

Router(config)#do wr

Building configuration...

[OK]

Router(config)#

Configuración ASA

Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, California 95134-1706

Reading from flash...

!

Type help or '?' for a list of available commands.

ciscoasa>en

Password:

ciscoasa#show ru

ciscoasa#show running-config

: Saved

:

ASA Version 8.4(2)

!

hostname ciscoasa

names

!

interface Ethernet0/0

switchport access vlan 2

!

interface Ethernet0/1

!

interface Ethernet0/2

!

interface Ethernet0/3

!

interface Ethernet0/4

```
!  
interface Ethernet0/5  
!  
interface Ethernet0/6  
!  
interface Ethernet0/7  
!  
interface Vlan1  
nameif inside  
security-level 100  
ip address 192.168.1.1 255.255.255.0  
!  
interface Vlan2  
nameif outside  
security-level 0  
ip address dhcp  
!  
!  
!  
!  
!  
!  
!  
!  
!  
telnet timeout 5  
ssh timeout 5  
!  
dhcpd auto_config outside  
!  
dhcpd address 192.168.1.5-192.168.1.36 inside  
dhcpd enable inside  
!  
!  
!  
!  
ciscoasa#  
ciscoasa#  
ciscoasa#conf t  
ciscoasa(config)#int vlan 1  
ciscoasa(config-if)#ip add 192.168.1.1 255.255.255.0  
ciscoasa(config-if)#exit  
ciscoasa(config)#int vlan 2  
ciscoasa(config-if)#ip add 192.168.3.1 255.255.255.0  
ciscoasa(config-if)#exit  
ciscoasa(config)#
```

```
ciscoasa(config)#int eth 0/0
ciscoasa(config-if)#swi
ciscoasa(config-if)#switchport acc
ciscoasa(config-if)#switchport access vlan 1
ciscoasa(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to down
ciscoasa(config-if)#no s
ciscoasa(config-if)#no sh
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#exit
ciscoasa(config)#int eth0/1
ciscoasa(config-if)#swi
ciscoasa(config-if)#switchport acc
ciscoasa(config-if)#switchport mode acc
ciscoasa(config-if)#switchport mode access vlan 2
```

^

% Invalid input detected at '^' marker.

```
ciscoasa(config-if)#switchport access vlan 2
ciscoasa(config-if)#no sh
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#
ciscoasa(config-if)#exit
ciscoasa(config)#cla
ciscoasa(config)#class-map seguridad1
ciscoasa(config-cmap)#match
ciscoasa(config-cmap)#match de
ciscoasa(config-cmap)#match default-inspection-traffic ?
<cr>
ciscoasa(config-cmap)#match default-inspection-traffic
ciscoasa(config-cmap)#match default-inspection-traffic icmp
```

^

% Invalid input detected at '^' marker.

```
ciscoasa(config-cmap)#match default-inspection-traffic icmp
```

^

% Invalid input detected at '^' marker.

```
ciscoasa(config-cmap)#cla
ciscoasa(config-cmap)#class-map ?
configure mode commands/options:
WORD class-map name
ciscoasa(config-cmap)#exit
ciscoasa(config)#pli
ciscoasa(config)#pol
ciscoasa(config)#policy-map glo
ciscoasa(config)#policy-map glob
ciscoasa(config)#policy-map glob?
```


WORD

ciscoasa(config)#policy-map ?

configure mode commands/options:

WORD policy-map name

type Specifies the type of policy-map

ciscoasa(config)#policy-map global ?

<cr>

ciscoasa(config)#policy-map seguridad

ciscoasa(config-pmap)#class seguridad1

ciscoasa(config-pmap-c)#ins

ciscoasa(config-pmap-c)#inspect ?

mode commands/options:

dns

ftp

h323

http

icmp

tftp

ciscoasa(config-pmap-c)#inspect icmp

ciscoasa(config-pmap-c)#ser

ciscoasa(config-pmap-c)#servi

ciscoasa(config-pmap-c)#exit

ciscoasa(config)#serv

ciscoasa(config)#service-policy glo

ciscoasa(config)#service-policy se

ciscoasa(config)#service-policy seguridad global

ciscoasa(config)#

DMZ

ciscoasa#

ciscoasa#conf t

ciscoasa(config)#int vlan 3

ciscoasa(config-if)#nam

ciscoasa(config-if)#nameif DMZ

ERROR: This license does not allow configuring more than 2 interfaces with nameif and without a "no forward" command on this interface or on 1 interface(s) with nameif already configured.

```
ciscoasa(config-if)#no fo
ciscoasa(config-if)#no forward in
ciscoasa(config-if)#no forward interface vlan 1
ciscoasa(config-if)#name
ciscoasa(config-if)#nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
ciscoasa(config-if)#se
ciscoasa(config-if)#security-level 50
ciscoasa(config-if)#ip add 192.168.4.1 255.255.255.0
ciscoasa(config-if)#no sh
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#exit
ciscoasa(config)#do wr
ciscoasa(config)#exit
ciscoasa#show run
ciscoasa#show running-config
```

```
ciscoasa#
ciscoasa#
ciscoasa#conf t
ciscoasa(config)#int eth0/2
ciscoasa(config-if)#swi
ciscoasa(config-if)#switchport acc
ciscoasa(config-if)#switchport access vlan 3
ciscoasa(config-if)#no sh
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#exit
ciscoasa(config)#
ciscoasa(config)#acc
ciscoasa(config)#int eth0/2
ciscoasa(config-if)#acc
ciscoasa(config-if)#access
ciscoasa(config-if)#access-list acl1 ex
ciscoasa(config-if)#exit
ciscoasa(config)#acc
ciscoasa(config)#access
ciscoasa(config)#access-list acl1 exten
ciscoasa(config)#access-list acl1 extended per
ciscoasa(config)#access-list acl1 extended permit icmp
% Incomplete command.
ciscoasa(config)#access-list acl1 extended permit ?
configure mode commands/options:
icmp
icmp6
ip
object-group Specify a service or protocol object-group after this keyword
```

```

tcp      Transmission Control Protocol
udp      User Datagram Protocol
ciscoasa(config)#access-list acl1 extended permit icmp any any
ciscoasa(config)#acce
ciscoasa(config)#access-group acl1 out int
ciscoasa(config)#access-group acl1 out interface ?
configure mode commands/options:
inside   Name of interface Vlan1
outside  Name of interface Vlan2
DMZ      Name of interface Vlan3
ciscoasa(config)#access-group acl1 out interface DMZ
ciscoasa(config)#

```

Ejercicio

