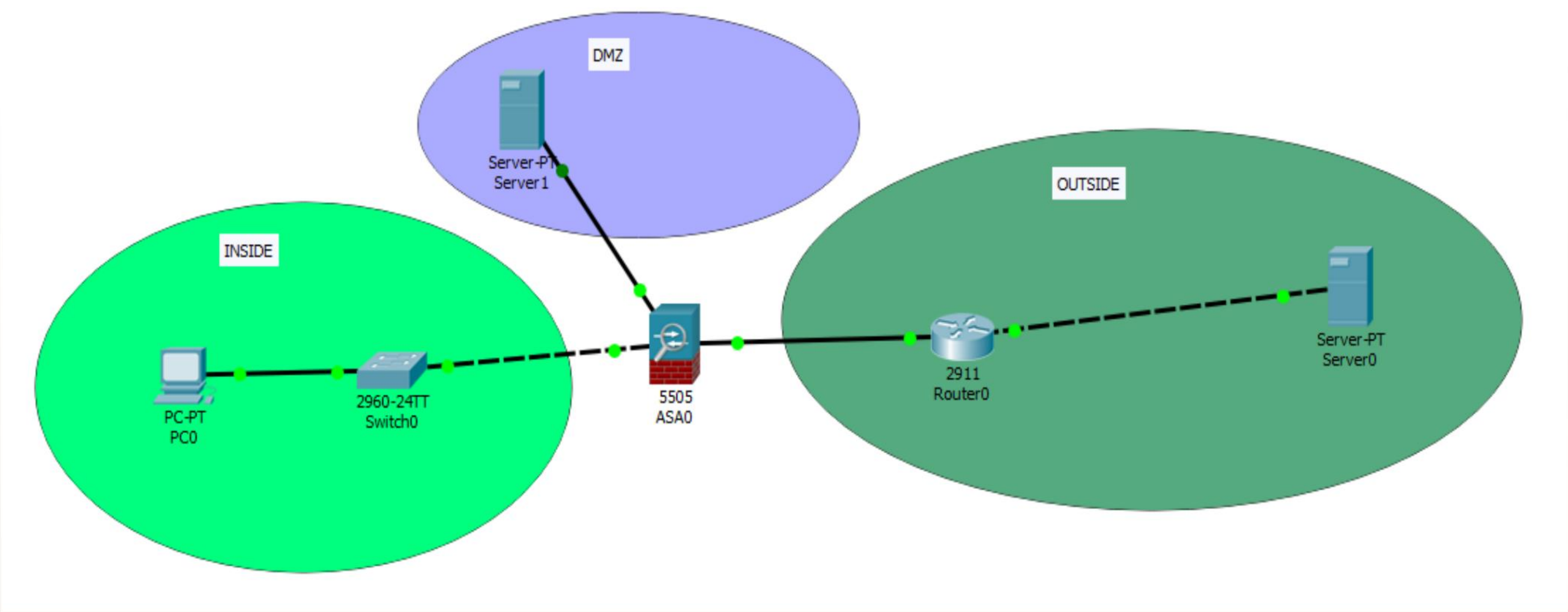
Cisco ASA5505 firewall configuration

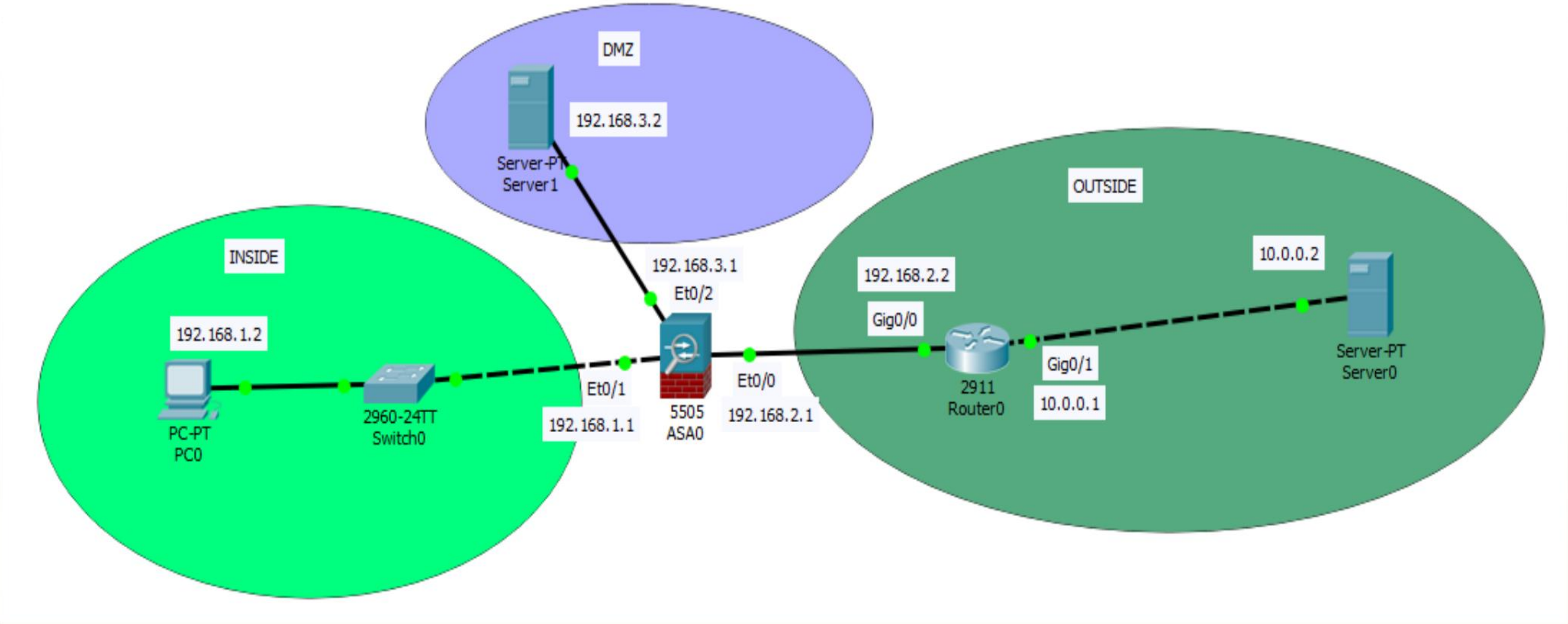
Topics to be covered:

- Creation of the network
- Address assignment
- Changing the default settings of existing vlan
- Assigning the vlan to an ethernet interface
- Set the dhcp and dns of a vlan
- Configure the route
- Creation of the network object and setting of the NAT
- Create and set access rules (ACCESS LIST)
- DMZ configuration

Network diagram:



We enter the network addresses:



Changing the vlan settings:

These steps must be done if you want to change the default settings of the vlan already existing in the asa5505 firewall configuration:

First let's see the existing configuration.

Select the terminal of the asa5505.

Let's run the **show running-config** command

Changing the vlan settings:

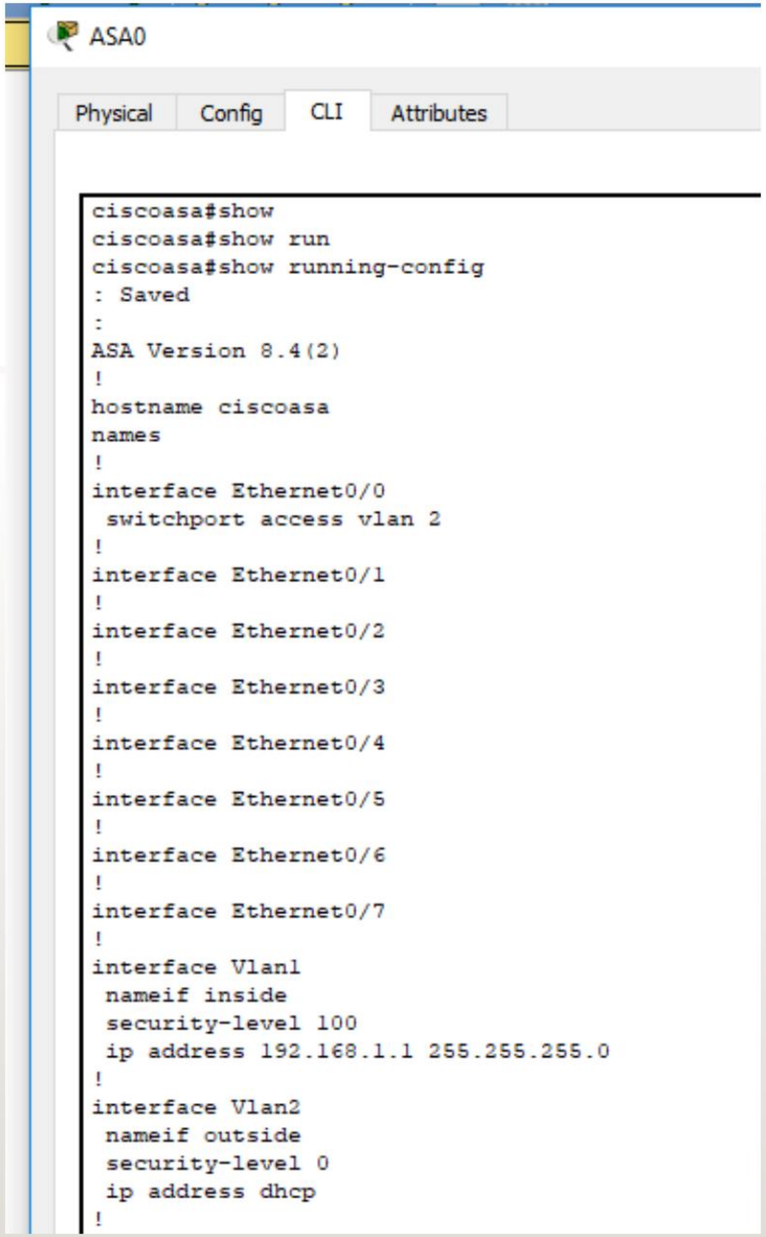
We can see these settings:

Note that **ethernet 0/0** is assigned to **vlan 2 (outside),** while all the others are assigned to **vlan 1 (inside).**

It also shows us the default settings of the two vlans.

Vlan **1** is called **inside** and has a **security level equal to 100,** it belongs to the **192.168.1.1 network of mask / 24**

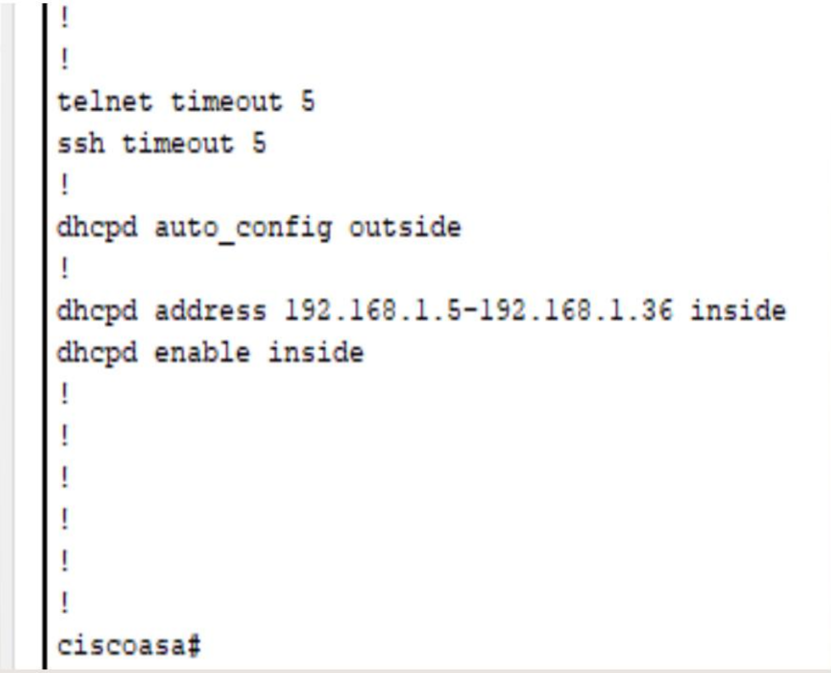
The **vlan 2** instead is called **outside** has a **level of security equal to 0** and **dhcp** is used to identify the network



```
ciscoasa#show
ciscoasa#show run
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
!
```

Changing the vlan settings:

Continuing to scroll through the config we find:



```
!
!
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#
```

The **dhcpd** on the **outside** network is used with automatic address **configuration ,**

while for the **inside** zone you have a **dhcpd enabled** on the addresses that go from

192.169.1.5 at the address 192.168.1.36

Changing the vlan settings:

Let's start changing the default settings:

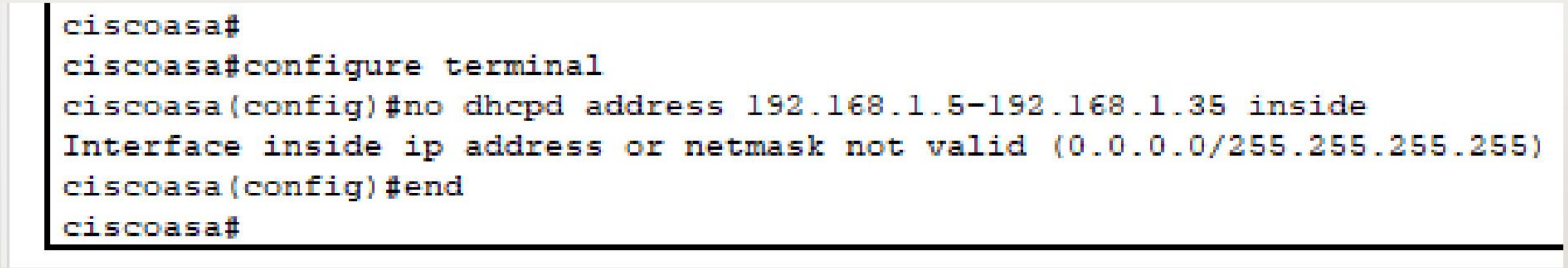
We select the vlan 1 to modify using the command:

interface vlan 1

We remove the default network address with the command:

no ip address

exit



```
ciscoasa#
ciscoasa#configure terminal
ciscoasa(config)#no dhcpd address 192.168.1.5-192.168.1.35 inside
Interface inside ip address or netmask not valid (0.0.0.0/255.255.255.255)
ciscoasa(config)#end
ciscoasa#
```

Changing the vlan settings:

Now we need to assign the new network parameters that we like most to vlan 1:

We will assign these settings:

Ip and mask: 192.168.1.1 255.255.255.0

Name: inside

Security level: 100

Changing the vlan settings:

To assign the values seen above, you need to use the following commands:

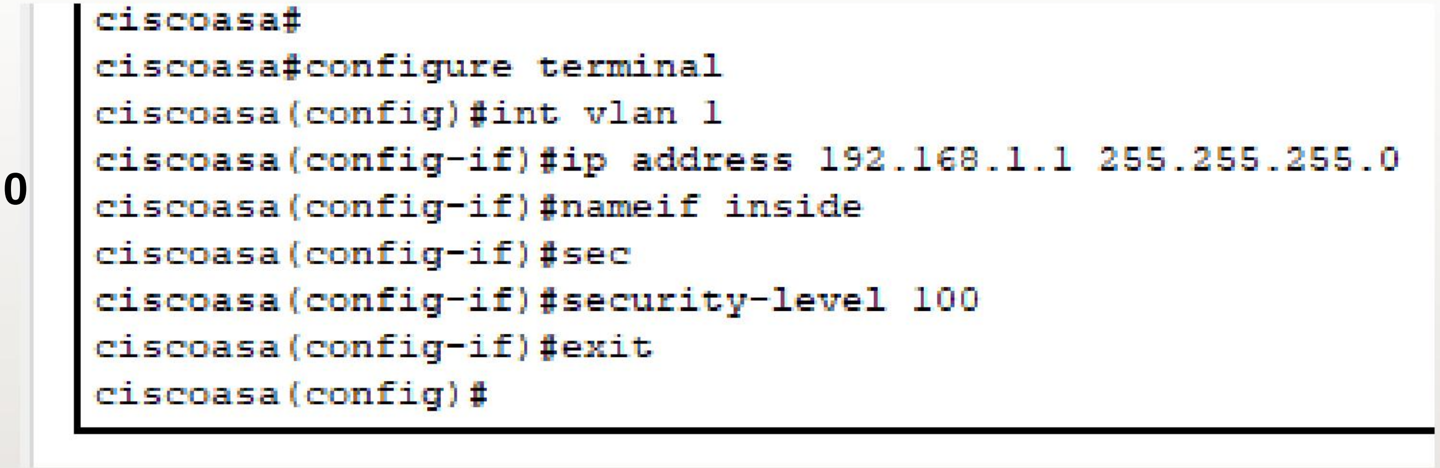
int vlan 1

ip address 192.168.1.1 255.255.255.0

nameif inside

security-level 100

exit



```
ciscoasa#
ciscoasa#configure terminal
ciscoasa(config)#int vlan 1
ciscoasa(config-if)#ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)#nameif inside
ciscoasa(config-if)#sec
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#exit
ciscoasa(config)#
```

Changing the vlan 2:

Now we are going to change the settings of vlan 2, repeat the same steps we did for vlan 1. We are going to set these specifications:

Ip and mask: 192.168.2.1 255.255.255.0

Name: outside

Security level: 0

This vlan will be assigned to the 0/0 ethernet port

Changing the vlan settings:

To assign the values seen above, you need to use the following commands:

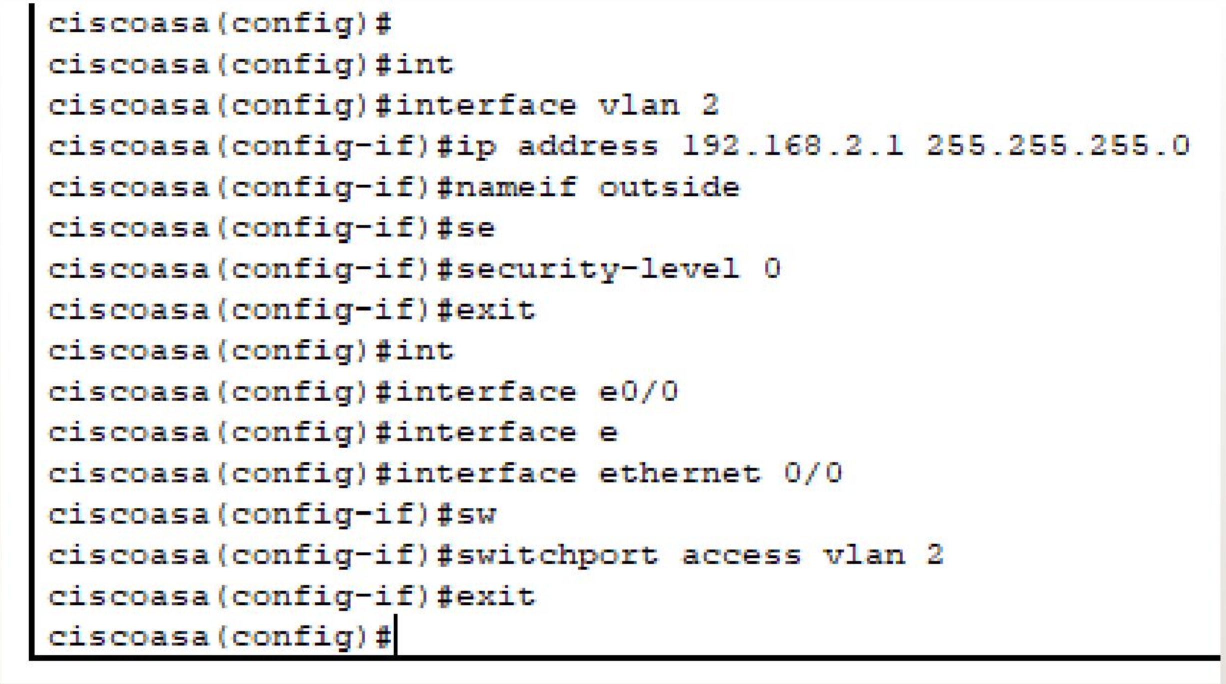
int vlan 2

ip address 192.168.2.1 255.255.255.0

nameif outside

security-level 0

exit



```
ciscoasa(config)#
ciscoasa(config)#int
ciscoasa(config)#interface vlan 2
ciscoasa(config-if)#ip address 192.168.2.1 255.255.255.0
ciscoasa(config-if)#nameif outside
ciscoasa(config-if)#se
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#exit
ciscoasa(config)#int
ciscoasa(config)#interface e0/0
ciscoasa(config)#interface e
ciscoasa(config)#interface ethernet 0/0
ciscoasa(config-if)#sw
ciscoasa(config-if)#switchport access vlan 2
ciscoasa(config-if)#exit
ciscoasa(config)#
```

Set up the dhcp and dns server of a vlan:

In this section we will see how you can configure a dhcp and a dns server on a vlan, so as to assign it to all connected terminals without configuring them manually.

We are going to set these settings:

Ip dhcp range: 192.168.1.10-192.168.1.41 (Maximum 32 hosts)

Dns server: 10.0.0.2

Interface: inside

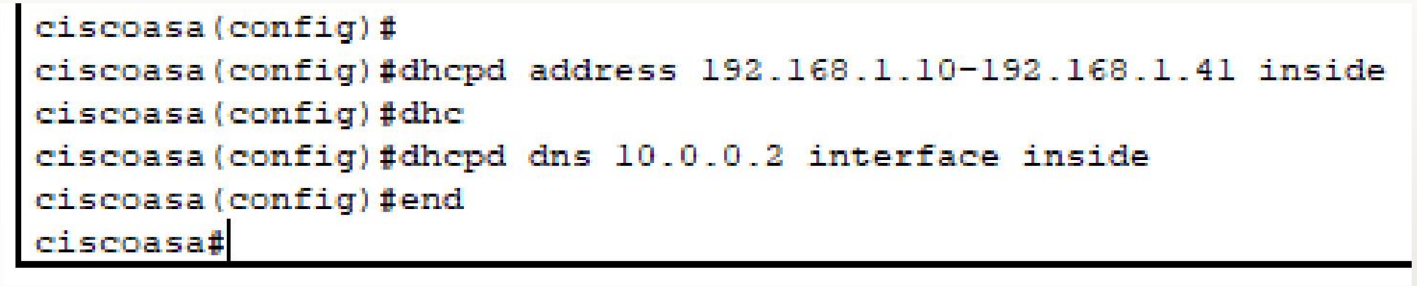
Set up the dhcp and dns server of a vlan:

These are the commands:

dhcpd address 192.168.1.10-192.168.1.41 inside

dhcpd dns 10.0.0.2 interface inside

end

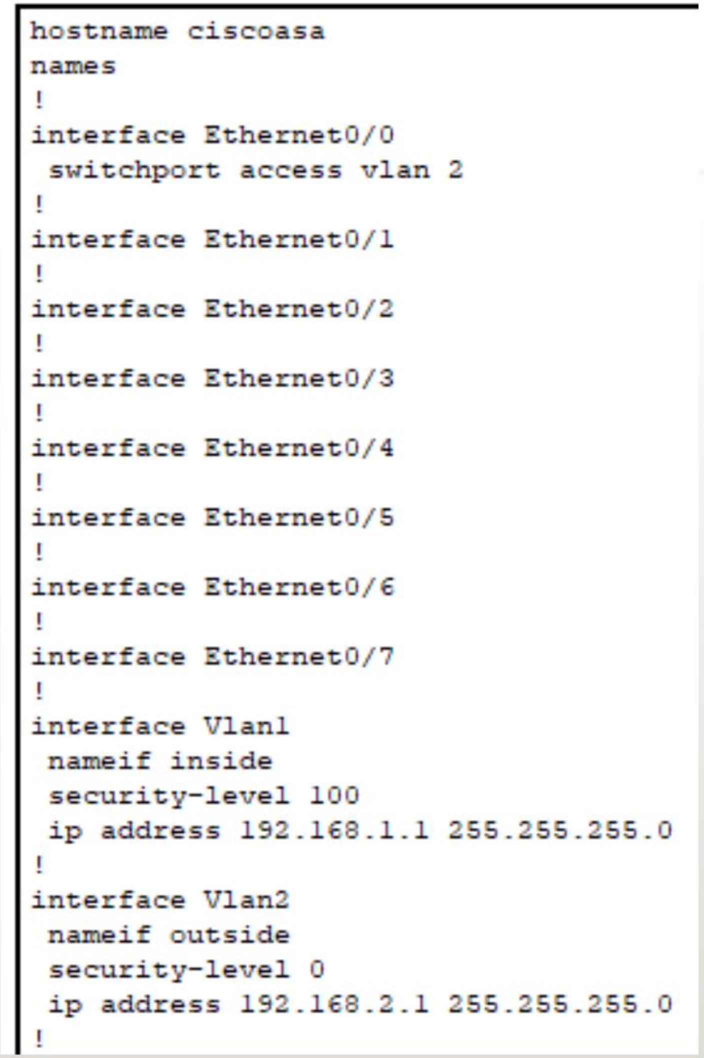


```
ciscoasa(config)#
ciscoasa(config)#dhcpd address 192.168.1.10-192.168.1.41 inside
ciscoasa(config)#dhc
ciscoasa(config)#dhcpd dns 10.0.0.2 interface inside
ciscoasa(config)#end
ciscoasa#
```

Once this is done, let's check the firewall settings again with the command:

show running-config

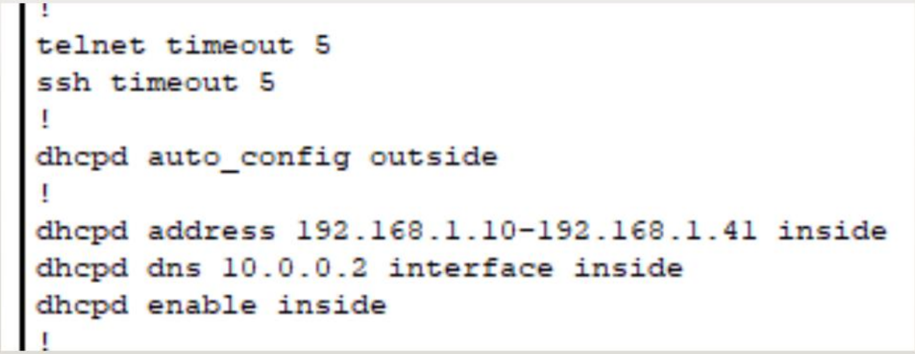
Set up the dhcp and dns server of a vlan:



```
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 192.168.2.1 255.255.255.0
!
```

Let's see the configurations:

We can see how the success of the commands. In particular, the configuration of dhcp and dns on the inside interface and the assignment of network addresses to the two vlan.



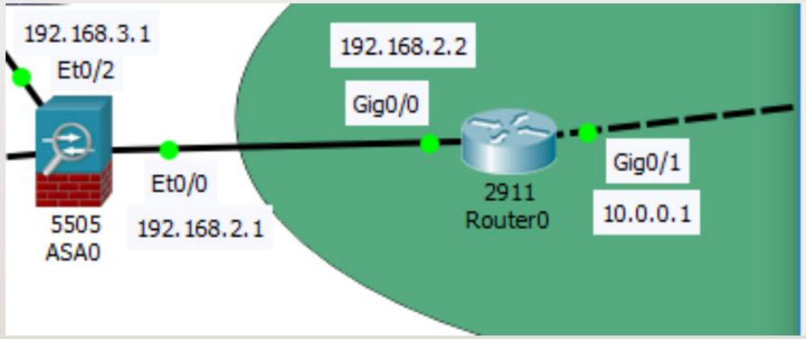
```
!
telnet timeout 5
ssh timeout 5
!
dhcpd auto_config outside
!
dhcpd address 192.168.1.10-192.168.1.41 inside
dhcpd dns 10.0.0.2 interface inside
dhcpd enable inside
!
```

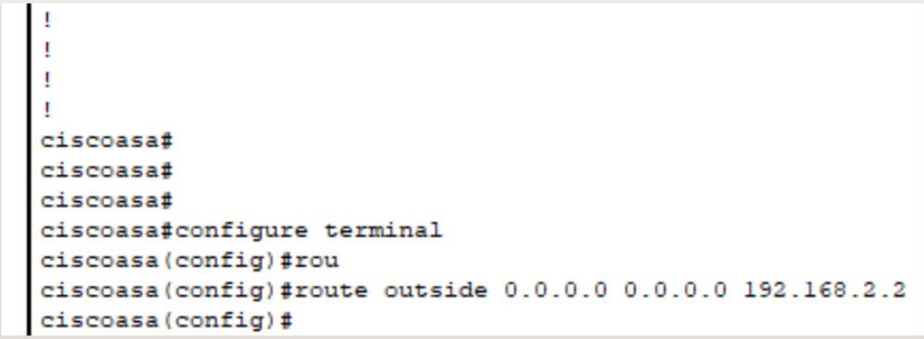
Route configuration:

Always above the asa5505 firewall configuration terminal, let's run the command:

route outside 0.0.0.0 0.0.0.0 192.168.2.2

In this way the traffic will be directed outside by the router with address 192.168.2.2





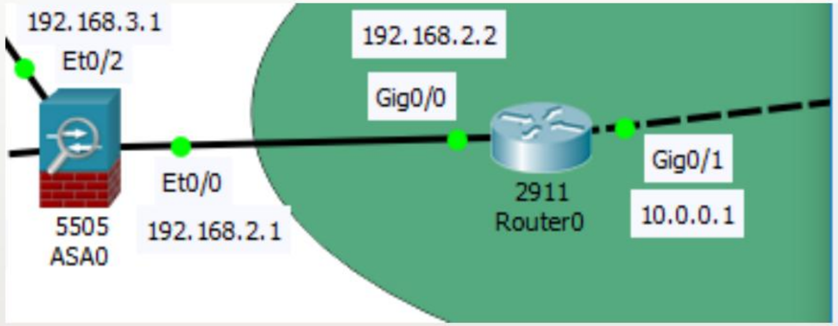
```
!
!
!
!
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#configure terminal
ciscoasa(config)#rou
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 192.168.2.2
ciscoasa(config)#
```

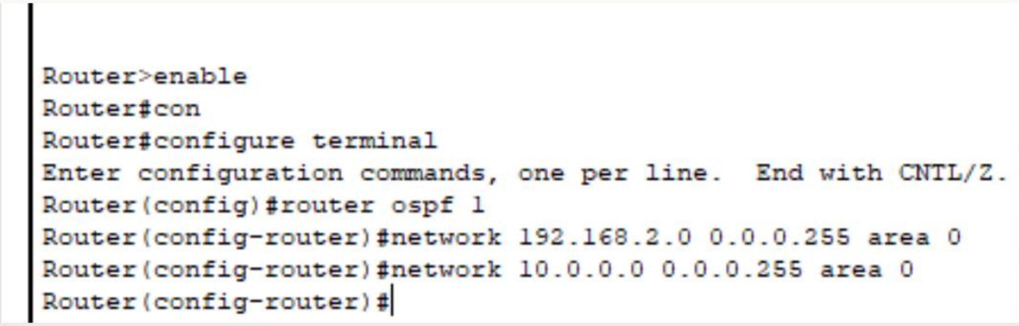
Route configuration (part of the router):

Now, let's move on to the configuration terminal of the external router.

Let's go to configure the router's OSPF. This allows us to send all routers on the network (if any) to receive the configurations for the routes.

We use these commands:





```
Router>enable
Router#con
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.2.0 0.0.0.255 area 0
Router(config-router)#network 10.0.0.0 0.0.0.255 area 0
Router(config-router)#
```

router ospf 1

network 192.168.2.0 0.0.0.255 area 0

network 10.0.0.0 0.0.0.255 area 0

Creation of the object network and NAT configuration:

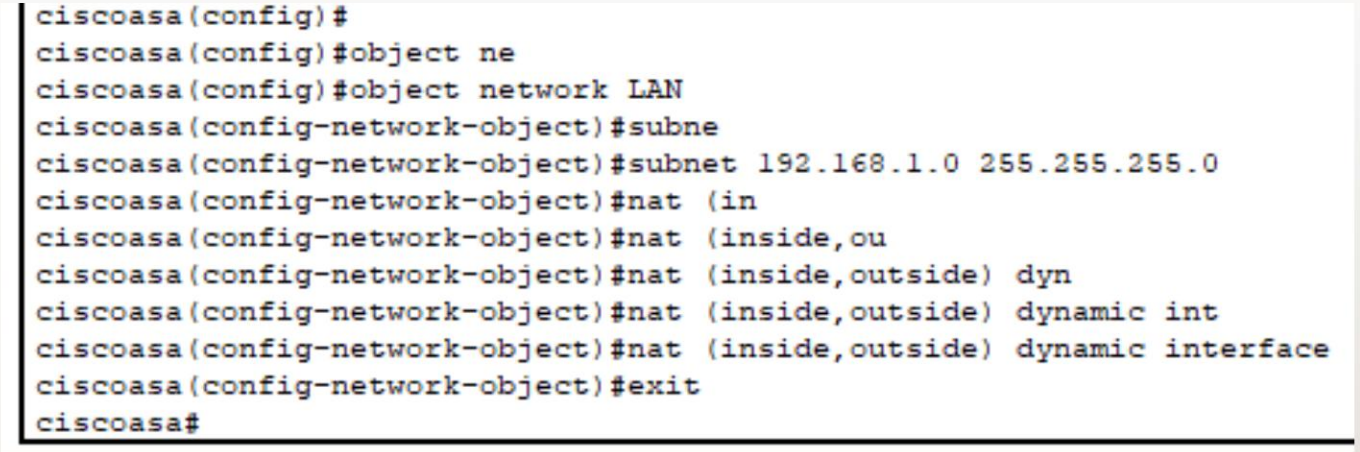
At this point we return to the configuration terminal of the firewall asa5505 to create the network object and to set the NAT. We run these commands:

object network LAN

subnet 192.168.1.0 255.255.255.0

nat (inside,outside) dynamic interface

exit



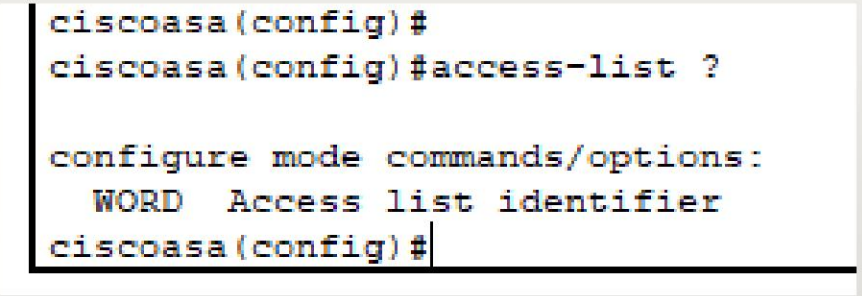
```
ciscoasa(config)#
ciscoasa(config)#object ne
ciscoasa(config)#object network LAN
ciscoasa(config-network-object)#subne
ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)#nat (in
ciscoasa(config-network-object)#nat (inside,ou
ciscoasa(config-network-object)#nat (inside,outside) dyn
ciscoasa(config-network-object)#nat (inside,outside) dynamic int
ciscoasa(config-network-object)#nat (inside,outside) dynamic interface
ciscoasa(config-network-object)#exit
ciscoasa#
```

Configuring the access lists (ACCESS LIST):

Now all that remains is to configure the rules for the access lists, that is, you have to specify which packets to pass or which ones to block.

As an example we want to pass only the packets of the tcp protocol (for a possible web server) and the ICMP packets to check the status of the host with simple pings.

We're going to use the **access-list** command . We can also see one possible definition:



```
ciscoasa(config)#
ciscoasa(config)#access-list ?

configure mode commands/options:
  WORD  Access list identifier
ciscoasa(config)#
```

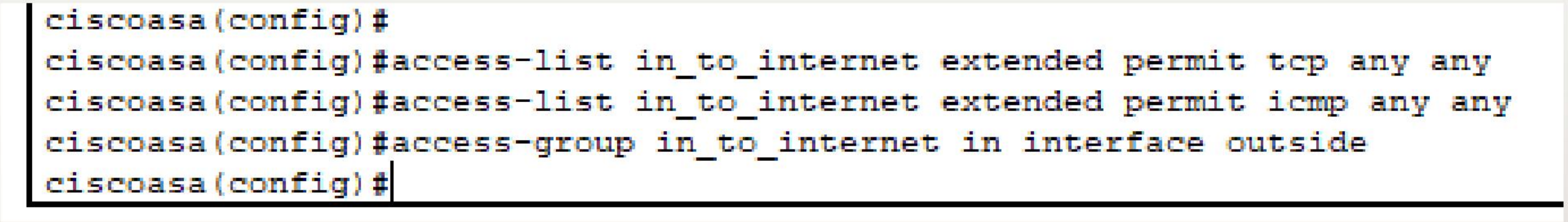
Configuring the access lists (ACCESS LIST):

We run these commands:

access-list in_to_internet extended permit tcp any any

access-list in_to_internet extended permit icmp any any

access-group in_to_internet in interface outside



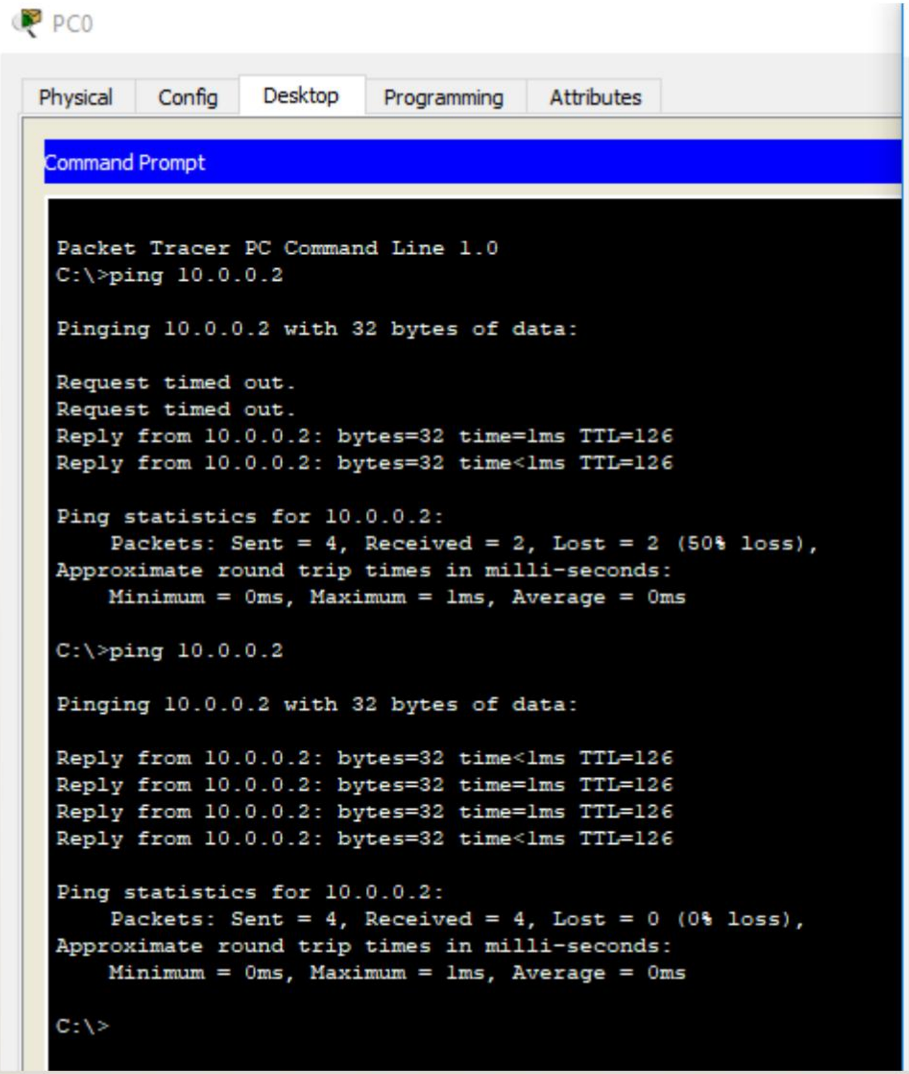
```
ciscoasa(config)#
ciscoasa(config)#access-list in_to_internet extended permit tcp any any
ciscoasa(config)#access-list in_to_internet extended permit icmp any any
ciscoasa(config)#access-group in_to_internet in interface outside
ciscoasa(config)#
```

End of internal and external network settings:

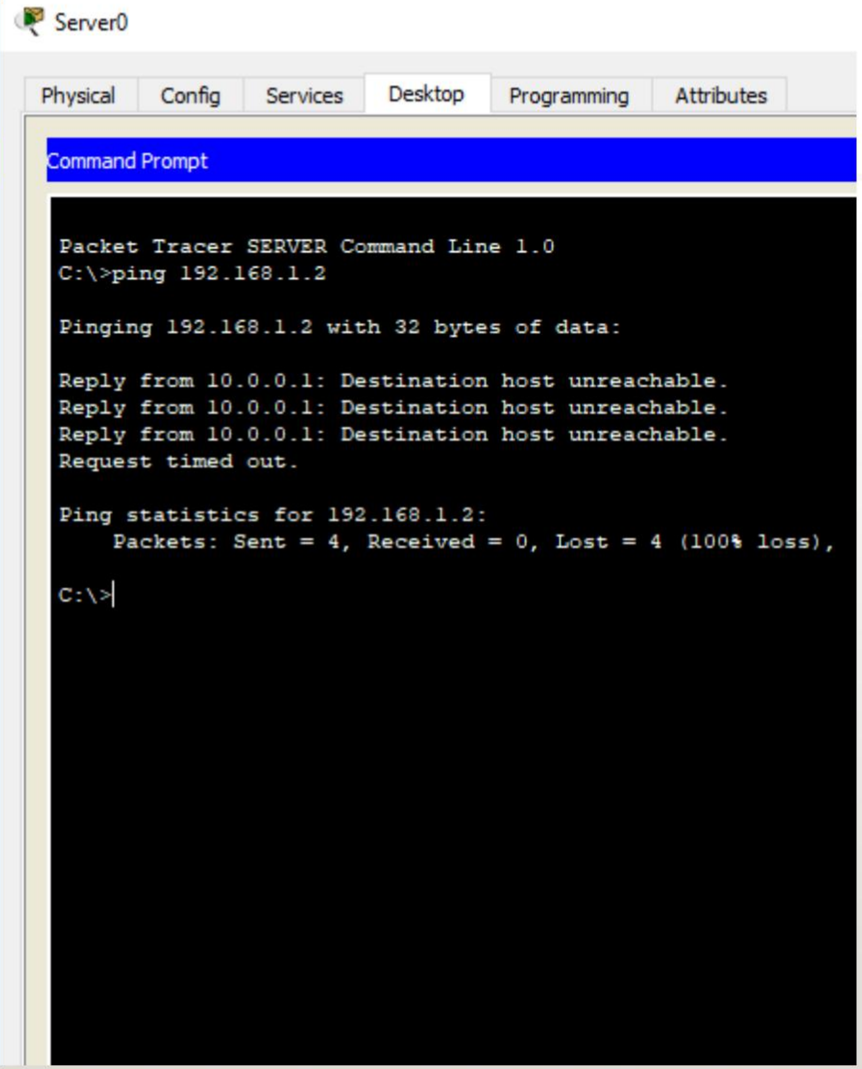
With this we have concluded the configuration of the internal and external networks. If you want you can use different settings for how much it's about addresses and configuring more complex networks. You can also put more restrictive rules using the port number as another parameter for the access lists, or allow only certain hosts to communicate with the outside and deny it to others.

To conclude this part we can see an example of ping between the pc in the external network and the server located on the internet. You will notice the passage of packages. If we try to ping from the external server to the extension, we will see that the host cannot be reached.

End of internal and external network settings:



```
Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 10.0.0.2: bytes=32 time=1ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time=1ms TTL=126
Reply from 10.0.0.2: bytes=32 time=1ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```



```
Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

DMZ configuration:

In this section we will see how a demilitarized zone (DMZ) can be configured.

Recalling the network configuration present at the beginning, we have this:

The server has ip: 192.168.3.2

The dmz interface is on the 0/2 ethernet port with ip: 192.168.3.1 and mask / 24

The first thing to do is to create a new vlan for the DMZ, then assign it to the ethernet interface and set the access lists. You can take advantage of the steps already performed for the configurations of the other vlan.

DMZ configuration:

Let's start by creating the vlan 3 identified by these parameters:

IP address and mask: 192.168.3.1 255.255.255.0

Name: DMZ

Security level: 70 (1-99)

In addition we can say that we have no direct interface with vlan 1

Machine Translated by Google

DMZ configuration:

We run the following commands from the asa5505 firewall terminal:

interface vlan 3

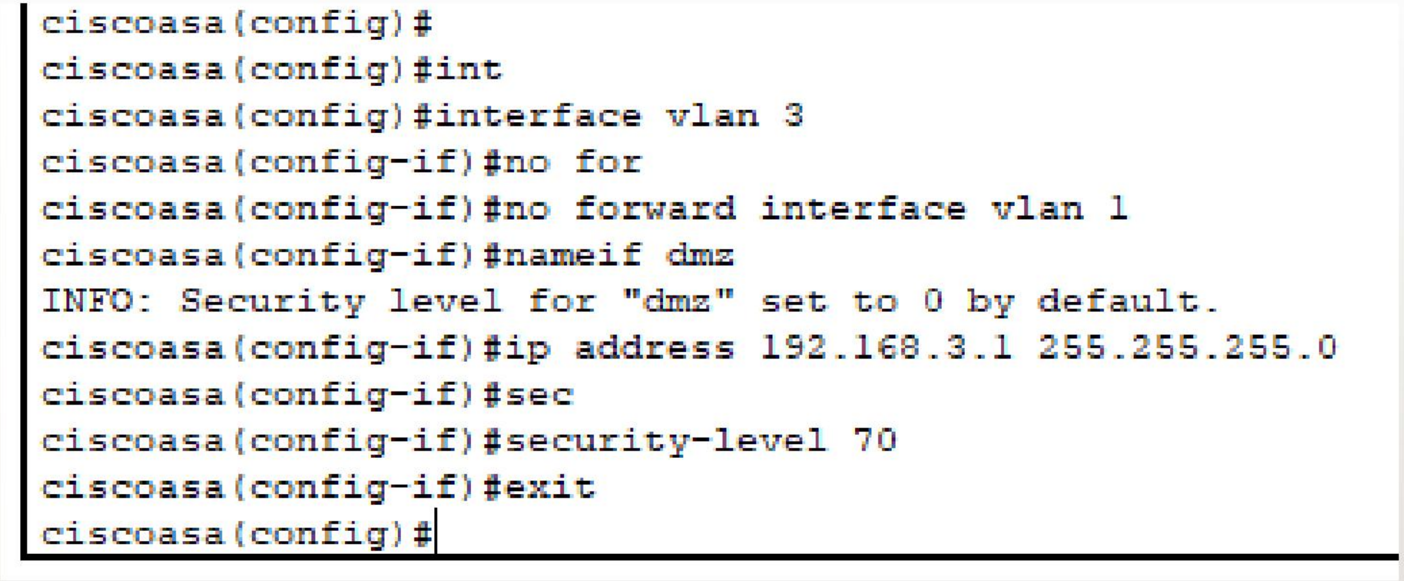
no forward interface vlan 1

nameif dmz

ip address 192.168.3.1 255.255.255.0

security-level 70

exit



```
ciscoasa(config)#
ciscoasa(config)#int
ciscoasa(config)#interface vlan 3
ciscoasa(config-if)#no for
ciscoasa(config-if)#no forward interface vlan 1
ciscoasa(config-if)#nameif dmz
INFO: Security level for "dmz" set to 0 by default.
ciscoasa(config-if)#ip address 192.168.3.1 255.255.255.0
ciscoasa(config-if)#sec
ciscoasa(config-if)#security-level 70
ciscoasa(config-if)#exit
ciscoasa(config)#
```

DMZ configuration:

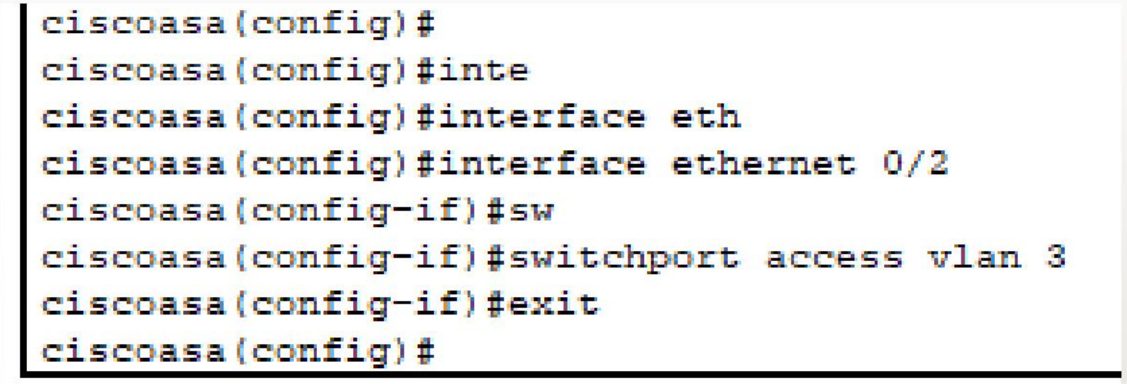
We assign the new vlan to the 0/2 ethernet interface.

Here are the commands:

interface ethernet 0/2

switchport access vlan 3

exit



```
ciscoasa(config)#
ciscoasa(config)#inte
ciscoasa(config)#interface eth
ciscoasa(config)#interface ethernet 0/2
ciscoasa(config-if)#sw
ciscoasa(config-if)#switchport access vlan 3
ciscoasa(config-if)#exit
ciscoasa(config)#
```

DMZ configuration:

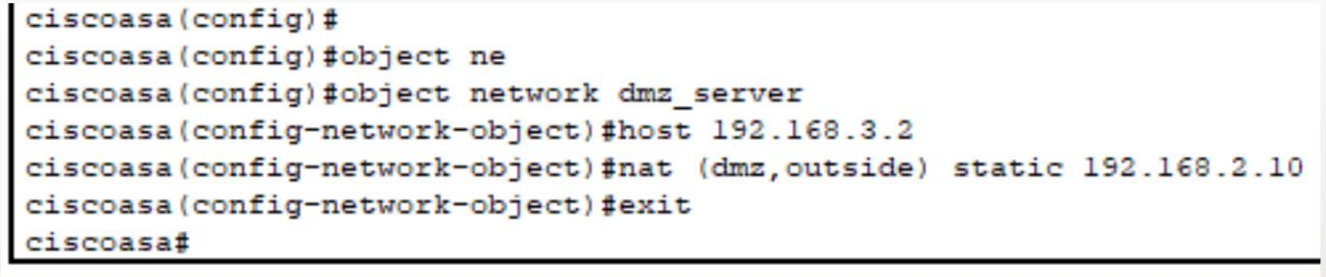
We create the network object and configure the NAT as already done for the other vlan:

object network dmz_server

host 192.168.3.2

nat (dmz, outside) static 192.168.2.10

exit



```
ciscoasa(config)#
ciscoasa(config)#object ne
ciscoasa(config)#object network dmz_server
ciscoasa(config-network-object)#host 192.168.3.2
ciscoasa(config-network-object)#nat (dmz,outside) static 192.168.2.10
ciscoasa(config-network-object)#exit
ciscoasa#
```

In this way the host 192.168.3.2 (the server) is seen from the outside through the address 192.168.2.10. in short, this object translates its internal address into the external one.

DMZ configuration:

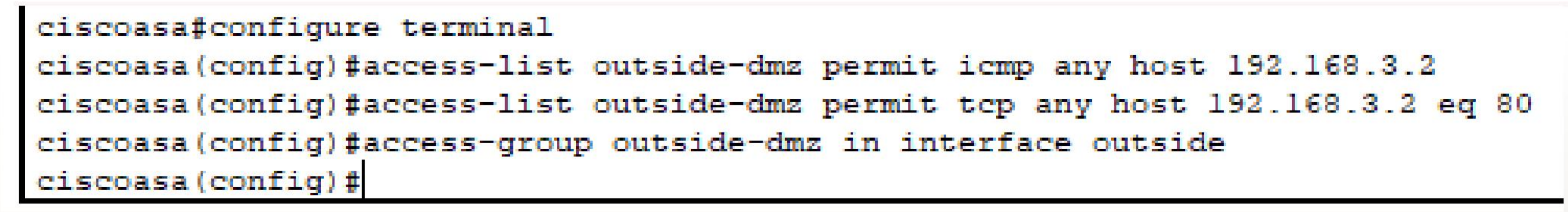
As a last step, let's set up the access lists.

```
access-list outside-dmz permit icmp any host 192.168.3.2
access-list outside-dmz permit tcp any host 192.168.3.2 eq 80
access-group outside-dmz in interface outside
```

In this way, the **access lists** are configured so that **each person** can reach the dmz server from the **outside** through the **icmp** and **tcp** protocols on **port 80,** only for the host **192.168.3.2 (the** server)

DMZ configuration:

Here are the commands given on the terminal.



```
ciscoasa#configure terminal
ciscoasa(config)#access-list outside-dmz permit icmp any host 192.168.3.2
ciscoasa(config)#access-list outside-dmz permit tcp any host 192.168.3.2 eq 80
ciscoasa(config)#access-group outside-dmz in interface outside
ciscoasa(config)#
```

In this way, the **access lists** are configured in such a way that **each person** can reach the dmz server from the **outside** through the **icmp** and **tcp** protocols on **port 80,** only for the host **192.168.3.2 (the** server).

To access the server from the outside, use the address declared first 192.168.2.10, then the asa firewall converts this ip into the private one (192.168.3.2) and applies the rules of the ACLs.

DMZ configuration:

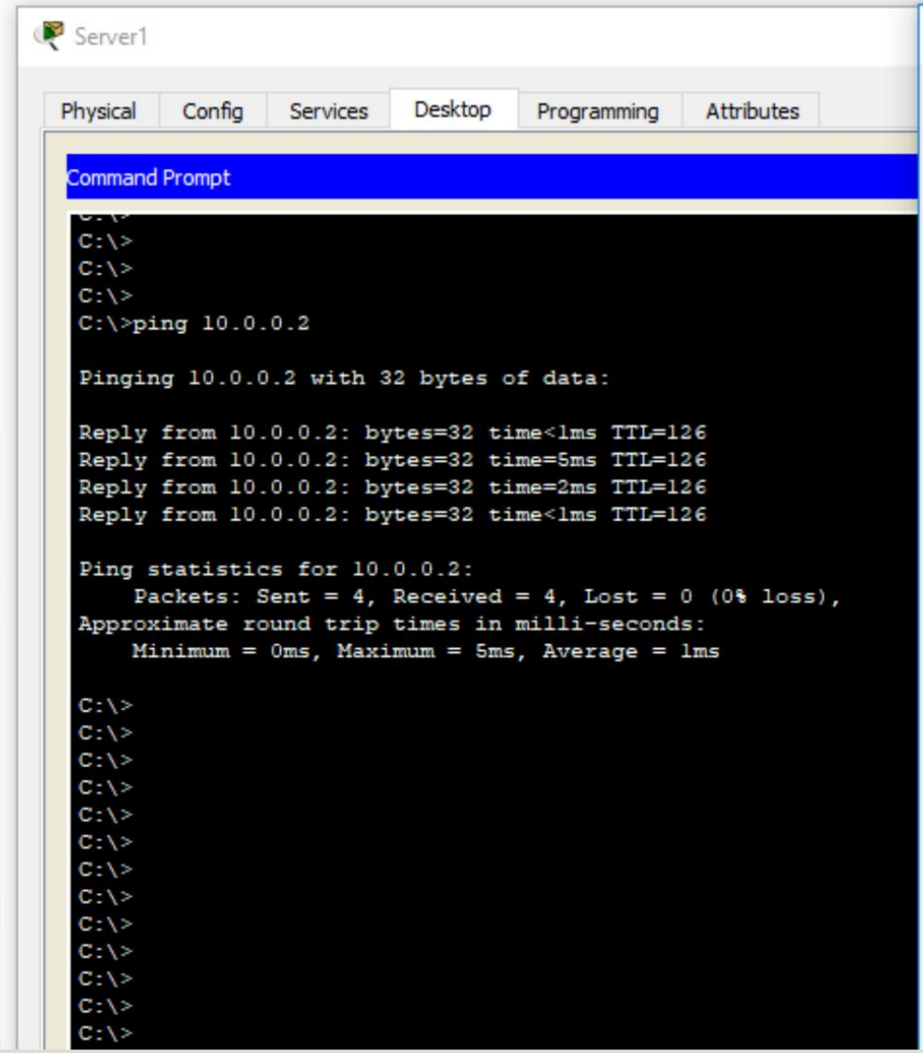
As we can see in the next screenshot, the dmz **server** (internal), can **ping or reach the external.**

On the contrary, the external (internet) **server** can **not** reach the dmz (internal) server directly by entering its private network address .

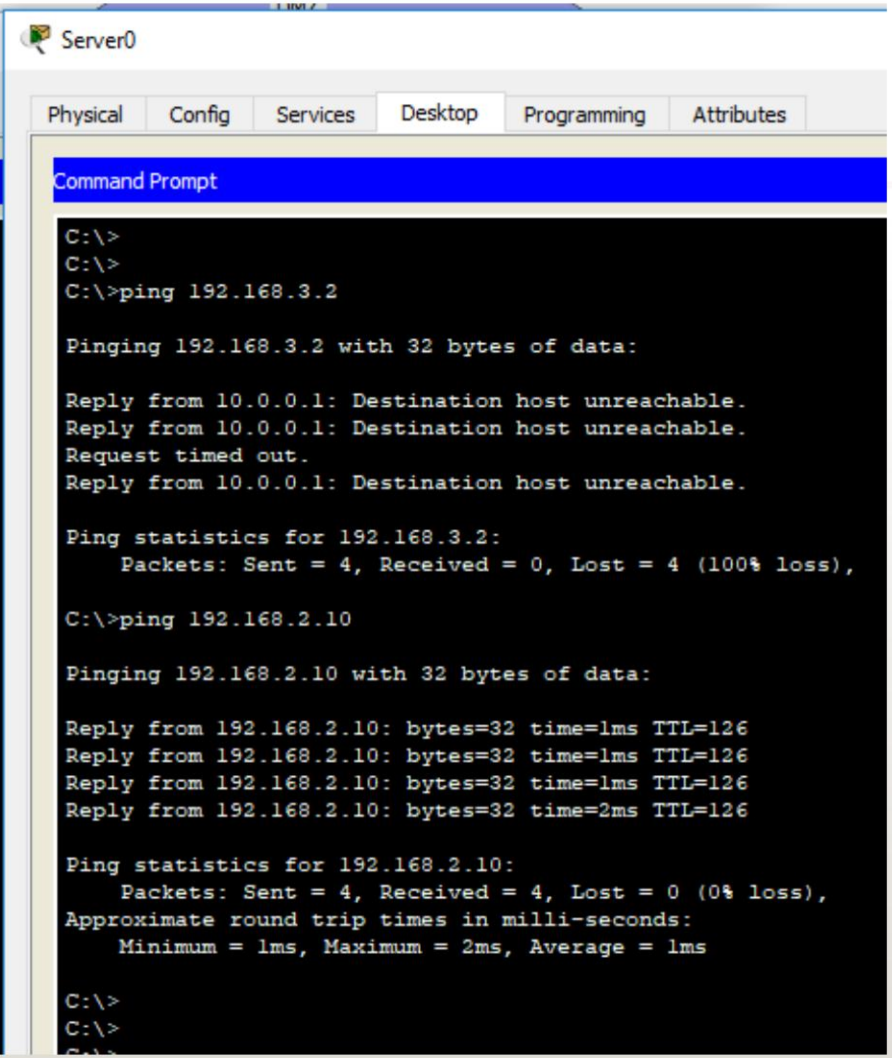
But if you use **the public ip** of the dmz server (internal) from a terminal in the internet, you can reach it.

As for the **vlan** network 1, i.e. the internal one, **it** cannot see the DMZ network because we have set it through the **no forward vlan 1** command when we configured la **vlan** 3.

DMZ configuration:



```
C:\>
C:\>
C:\>
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time=5ms TTL=126
Reply from 10.0.0.2: bytes=32 time=2ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 5ms, Average = 1ms

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
```



```
C:\>
C:\>
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.
Request timed out.
Reply from 10.0.0.1: Destination host unreachable.

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Reply from 192.168.2.10: bytes=32 time=1ms TTL=126
Reply from 192.168.2.10: bytes=32 time=1ms TTL=126
Reply from 192.168.2.10: bytes=32 time=1ms TTL=126
Reply from 192.168.2.10: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
C:\>
```