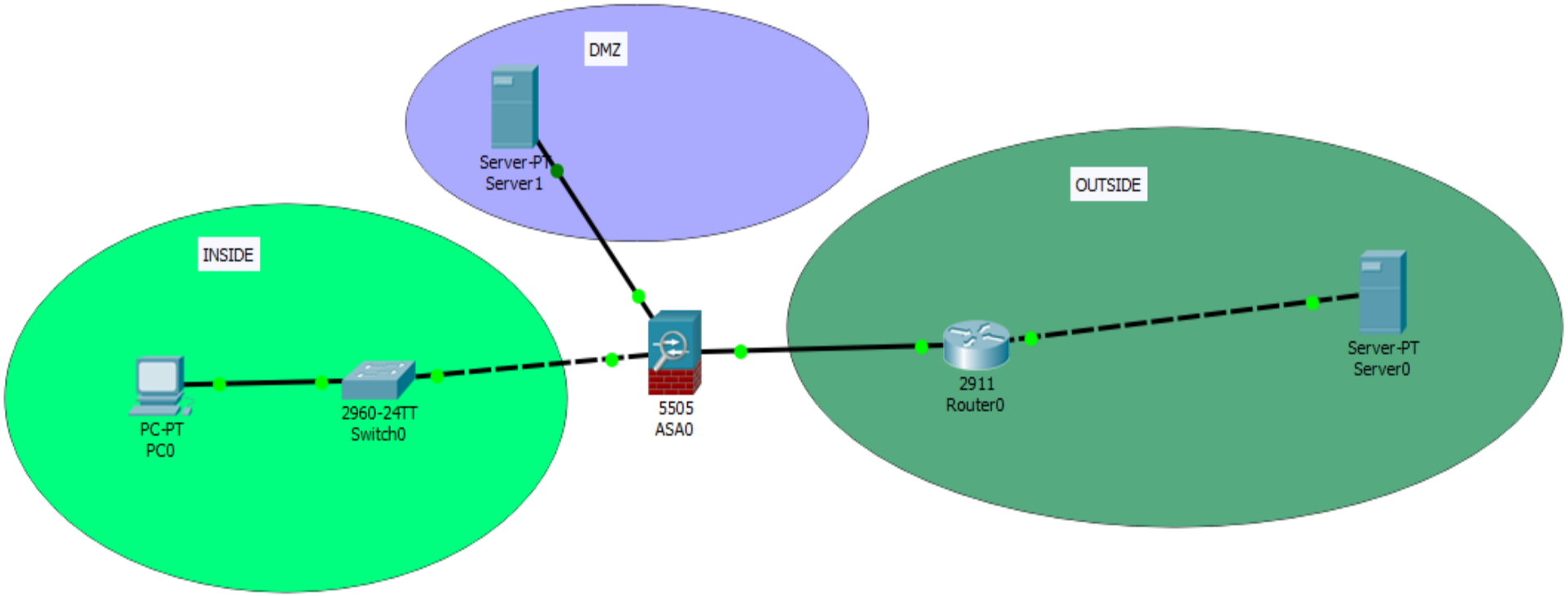
Configurazione firewall Cisco ASA5505

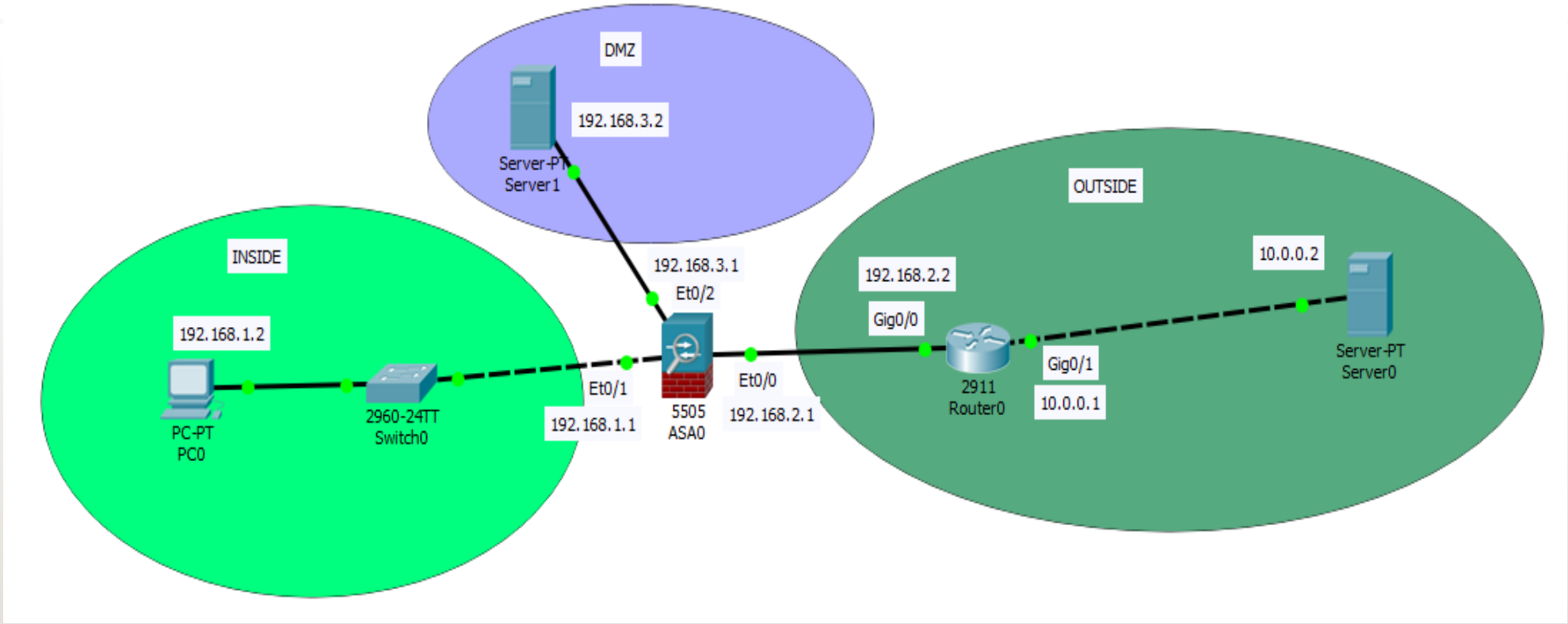
Argomenti da trattare:

- Creazione della rete
- Assegnazione indirizzi
- Modifica delle impostazioni di default delle vlan esistenti
- Assegnazione della vlan ad una interfaccia ethernet
- Impostare il dhcp e dns di una vlan
- Configurare le route
- Creazione dell'oggetto network e impostazione del NAT
- Creare ed impostare le regole di accesso(ACCESS LIST)
- Configurazione DMZ

Schema della rete:



Inseriamo gli indirizzi di rete:



Modifica delle impostazioni delle vlan:

Questi passi vanno fatti se si vogliono cambiare le impostazioni di default delle vlan già esistenti nella configurazione del firewall asa5505:

Per prima cosa vediamo la configurazione esistente.

Selezionare il terminale del asa5505.

Mandiamo in esecuzione il comando **show running-config**

Modifica delle impostazioni delle vlan:

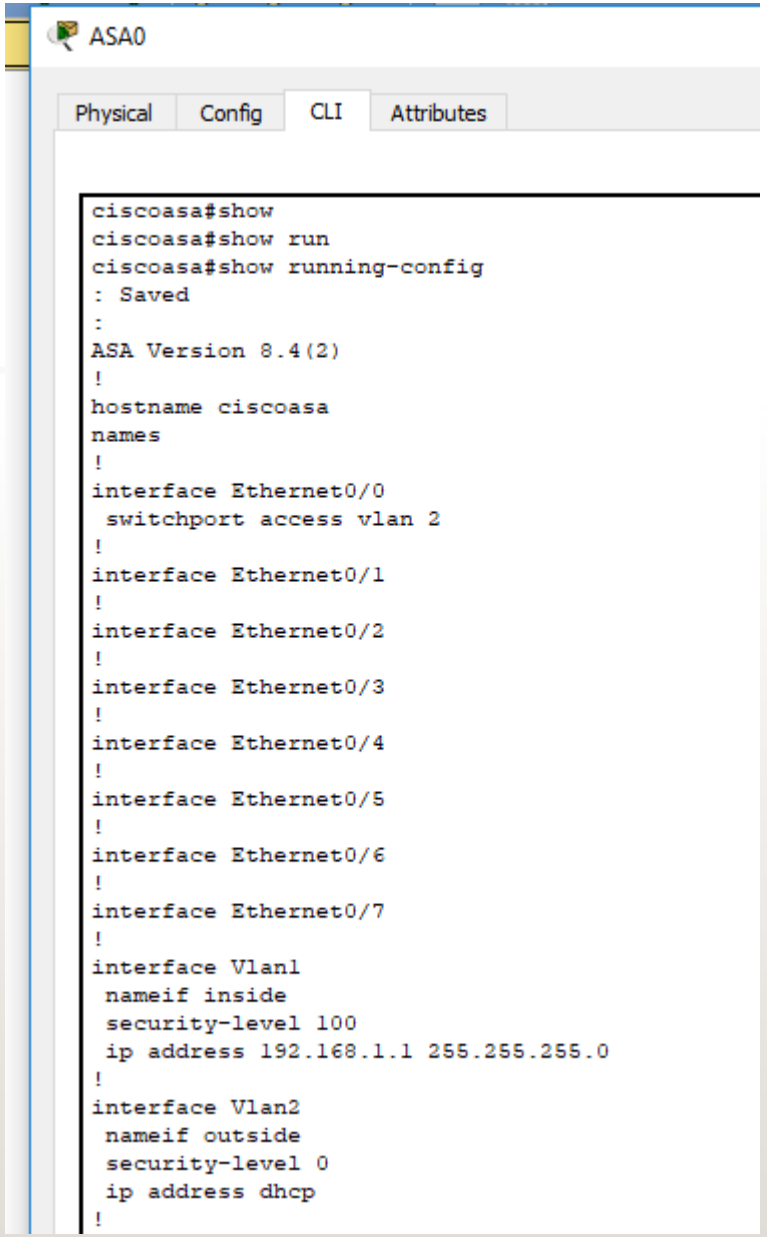
Possiamo vedere queste impostazioni:

Si nota che la **ethernet 0/0** è assegnata alla **vlan 2 (outside)**, mentre tutte le altre sono assegnate alla **vlan 1 (inside)**.

Ci mostra anche le impostazioni di default delle due vlan.

La **vlan 1** è chiamata **inside** e ha un **livello di sicurezza pari a 100**, appartiene alla rete **192.168.1.1 di maschera /24**

La **vlan 2** invece è chiamata **outside** ha un **livello di sicurezza pari a 0** e viene utilizzato il **dhcp** per identificare la rete



Modifica delle impostazioni delle vlan:

Continuando a scorrere le config troviamo:

```
!
!
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#
```

Viene utilizzato il **dhcpd** sulla rete **outside** con la **configurazione automatica** degli indirizzi,

mentre per la zona **inside** si ha un **dhcpd abilitato** sugli indirizzi che vanno da

192.169.1.5 all'indirizzo 192.168.1.36

Modifica delle impostazioni delle vlan:

Iniziamo a modificare le impostazioni di default:

Selezioniamo la vlan 1 da modificare tramite il comando:

interface vlan 1

Togliamo l'indirizzo di rete di default con il comando:

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#
```

Modifica delle impostazioni delle vlan:

Ora bisogna assegnare alla vlan 1 i nuovi parametri di rete che più ci piacciono:

Assegneremo queste impostazioni:

Ip e maschera: 192.168.1.1 255.255.255.0

Nome: inside

Livello di sicurezza: 100

Modifica delle impostazioni delle vlan:

Per assegnare i valori visti precedentemente, bisogna usare i seguenti comandi:

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)#
```

Modifica della vlan 2:

Ora andiamo a modificare le impostazioni della vlan 2, ripetiamo gli stessi passi fatti per la vlan 1. Andremo ad impostare queste specifiche:

Ip e maschera: 192.168.2.1 255.255.255.0

Nome: outside

Livello di sicurezza: 0

Si andrà ad assegnare questa vlan alla porta ethernet 0/0

Modifica delle impostazioni delle vlan:

Per assegnare i valori visti precedentemente, bisogna usare i seguenti comandi:

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)#
```

Impostare il dhcp e dns server di una vlan:

In questa sezione andremo a vedere come si può configurare un dhcp e un dns server su una vlan, così da assegnarlo a tutti terminali connessi senza configurarli manualmente.

Andremo ad impostare questi settaggi:

Intervallo ip dhcp: 192.168.1.10-192.168.1.41 (Massimo 32 host)

Dns server: 10.0.0.2

Interfaccia: inside

Impostare il dhcp e dns server di una vlan:

Questi sono i comandi:

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#
```

Fatto questo, controlliamo di nuovo le impostazioni del firewall con il commando: **show running-config**

Impostare il dhcp e dns server di una 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
!
```

Vediamo le configurazioni:

Possiamo vedere come la buona riuscita dei comandi. In particolare la configurazione del dhcp e dns sulla interfaccia inside e l'assegnazione degli indirizzi di rete alle due vlan.

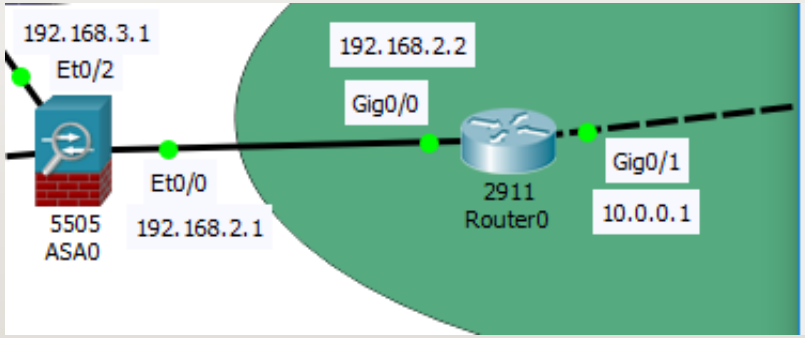
```
!
telnet timeout 5
ssh timeout 5
!
dhcpd auto_config outside
!
dhcpd address 192.168.1.10-192.168.1.41 inside
dhcpd dns 10.0.0.2 interface inside
dhcpd enable inside
!
```

Configurazione delle route:

Sempre sopra al terminale di configurazione del firewall asa5505, andiamo a eseguire il comando:

route outside 0.0.0.0 0.0.0.0 192.168.2.2

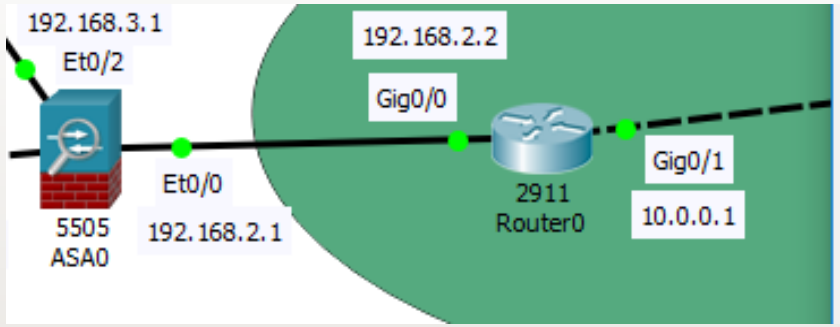
In questo modo il traffico verrà indirizzato all'esterno dal router di indirizzo 192.168.2.2




```
!
!
!
!
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)#
```

Configurazione delle route (parte del router):

Adesso, spostiamoci sul terminale di configurazione del router esterno.
Andiamo a configurare OSPF del router. Questo ci permette di inviare a tutti i router della rete(se presenti) di ricevere le configurazioni per le route.
Usiamo questi comandi:




```
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

Creazione dell'object network e configurazione NAT:

A questo punto torniamo sul terminale di configurazione del firewall asa5505 per creare l'ogetto network e per impostare il NAT. Eseguiamo questi comandi:

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#
```

Configurazione delle liste degli accessi(ACCESS LIST):

Ora non rimane che configurare le regole per le liste di accessi, ovvero bisogna specificare quali pacchetti far passare o quali bloccare.

Come esempio vogliamo far passare solo i pacchitti del protocollo tcp (per un eventuale server web) e i pacchetti ICMP per verificare lo stato degli host con dei semplici ping.

Andremo ad usare il comando **access-list**. Possiamo anche vedere una eventuale definizione:

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

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

Configurazione delle liste degli accessi(ACCESS LIST):

Eseguiamo questi comandi:

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

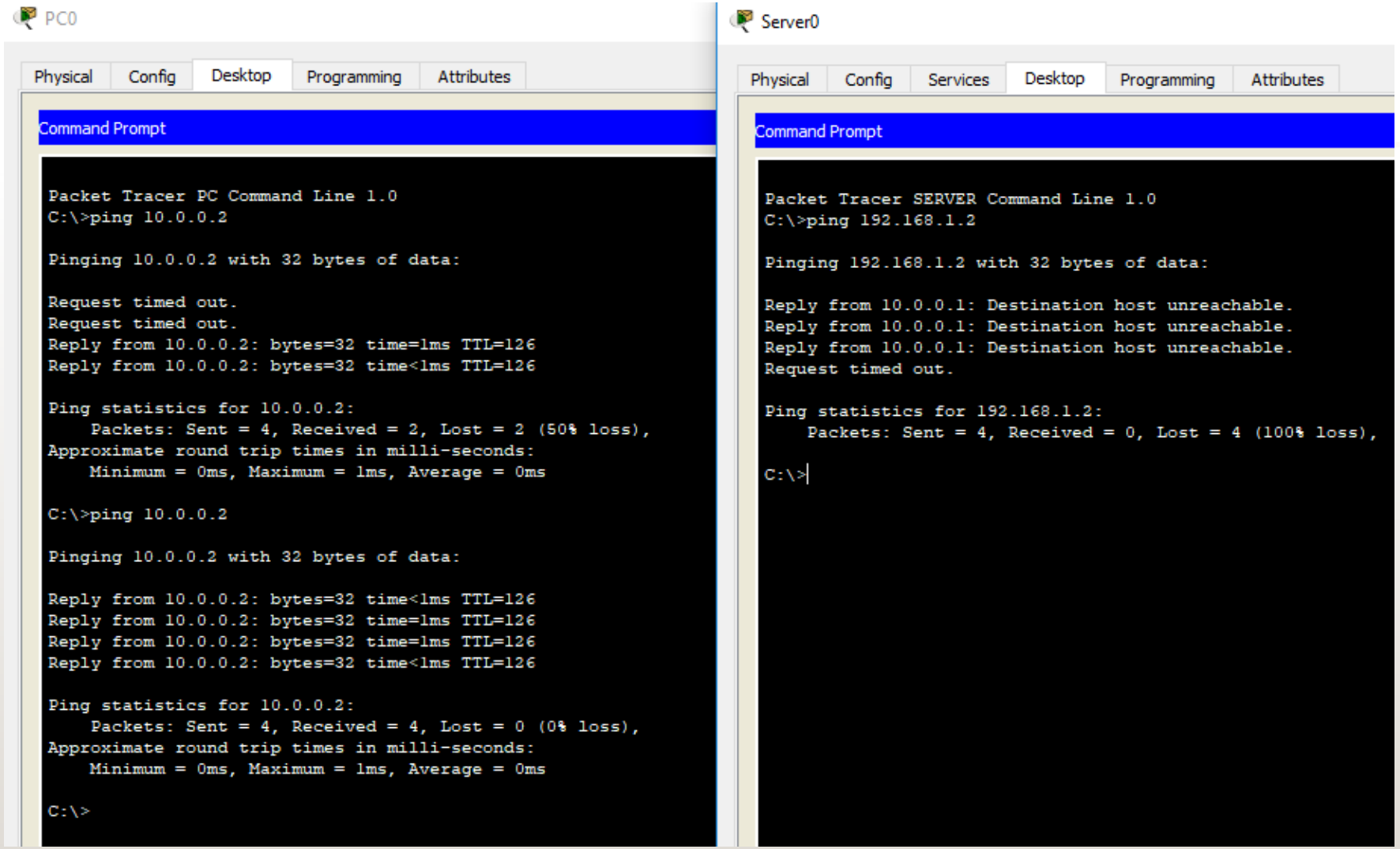
```
ciscoasa(config)#
ciscoasa(config)#access-list in_to_internet extended permit tcp any any
ciscoasa(config)#access-list in_to_internet extended permit icmp any any
ciscoasa(config)#access-group in_to_internet in interface outside
ciscoasa(config)#
```

Fine impostazioni reti interne ed esterne:

Con questo abbiamo concluso la configurazione delle reti interne ed esterne. Volendo si possono usare impostazioni differenti per quanto riguarda gli indirizzi e configurare reti più complesse. Si possono mettere anche delle regole più restrittive usando anche il numero di porta come altro parametro per le access list, oppure permettere solo a determinati host di comunicare con l'esterno e negarlo agli altri.

Per concludere questa parte possiamo vedere un esempio di ping tra il pc nella rete esterna e il server situato sulla rete internet. Si noterà il passaggio dei pacchetti. Se proviamo ad eseguire il ping dal server esterno verso l'interno, vedremo che l'host non può essere raggiunto.

Fine impostazioni reti interne ed esterne:



Configurazione DMZ:

In questa sezione vedremo come si può configurare una zona demilitarizzata (DMZ).

Richiamando la configurazione della rete presente all'inizio, abbiamo questo:

Il server ha ip: 192.168.3.2

L'interfaccia dmz è sulla porta ethernet 0/2 con ip: 192.168.3.1 e maschera /24

La prima cosa da fare è creare una nuova vlan per la DMZ, dopodiché assegnarla alla interfaccia ethernet ed impostare le access list. Si possono sfruttare i passi già eseguiti per le configurazioni delle altre vlan.

Configurazione DMZ:

Iniziamo creando la vlan 3 identificata da questi parametri:

Indirizzo ip e maschera: 192.168.3.1 255.255.255.0

Nome: DMZ

Livello di sicurezza: 70 (1-99)

In più possiamo dire di non avere nessuna interfaccia diretta con la vlan 1

Configurazione DMZ:

Eseguiamo i seguenti comandi dal terminale del firewall asa5505:

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)#
```

Configurazione DMZ:

Assegniamo la nuova vlan alla interfaccia ethernet 0/2.

Ecco i comandi:

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)#
```

Configurazione DMZ:

Creiamo l'oggetto network e configuriamo il NAT come già fatto per le altre 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 questo modo l'host 192.168.3.2(il server) viene visto dall'esterno tramite l'indirizzo 192.168.2.10. in poche parole questo oggetto traduce il suo indirizzo interno in quello esterno.

Configurazione DMZ:

Come ultimo passo, configuriamo le access list.

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 questo modo si configurano le **access list** in modo tale che **ogni persona** possa raggiungere il server dmz **dall'esterno** attraverso ai protocolli **icmp** e **tcp** sulla **porta 80**, per il solo host **192.168.3.2**(il server)

Configurazione DMZ:

Ecco i comandi dati sul terminale.

```
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 questo modo si configurano le **access list** in modo tale che **ogni persona** possa raggiungere il server dmz **dall'esterno** attraverso ai protocolli **icmp** e **tcp** sulla **porta 80**, per il solo host **192.168.3.2**(il server).

Per accedere dall'esterno al server si utilizza l'indirizzo dichiarato prima 192.168.2.10, poi il firewall asa converte questo ip in quello privato(192.168.3.2) e applica le regole delle ACLs.

Configurazione DMZ:

Come possiamo vedere nella schermata successiva, il **server dmz**(interno), può **pingare o raggiungere l'esterno**.

Al contrario il **server esterno**(internet) **non** può raggiungere il **server dmz**(interno) direttamente mettendo il suo indirizzo privato della rete.

Però se si utilizza l'**ip pubblico** del server dmz(interno) da un terminale nella rete internet, lo si può raggiungere.

Per quanto riguarda la rete **vlan 1**, ossia quella interna, **non** può vedere la rete DMZ perchè lo abbiamo impostato tramite il comando **no forward vlan 1** quando configuravamo la **vlan 3**.

Configurazione DMZ: