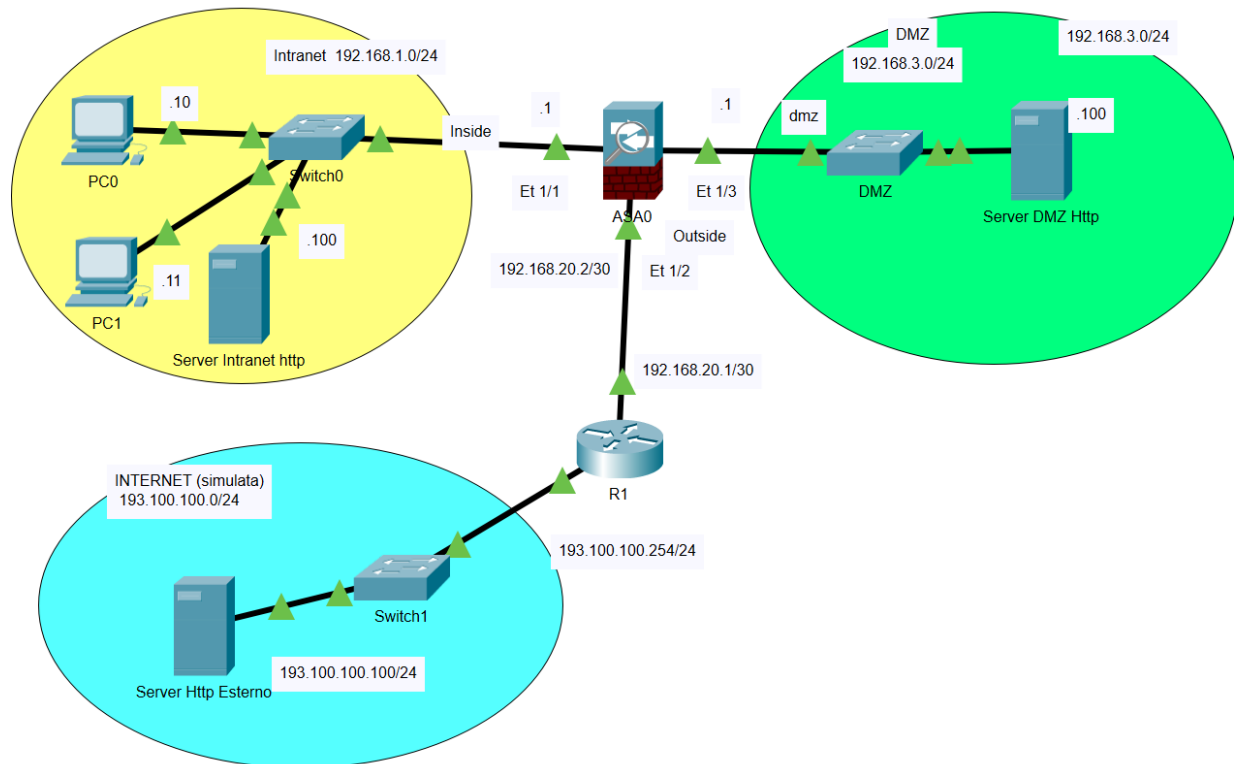


## DMZ con ASA (Adaptive Security Appliances)

Il seguente progetto utilizza la rete illustrata nel progetto Dmz gtramite ACL. Tutti i dispositivi di rete rimangono invariati anche nella loro configurazione ad eccezione di R2 che viene sostituito con un dispositivo ASA 5506. Le interfacce collegate sono descritte nello schema seguente.



### Configurazione di default

Osserviamo la configurazione preesistente del dispositivo ASA0 attraverso la visualizzazione del running-config.

```
ciscoasa#show running-config

: Saved
:
ASA Version 9.6(1)
!
hostname ciscoasa
names
!
interface GigabitEthernet1/1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet1/2
nameif outside
security-level 0
ip address dhcp
!
interface GigabitEthernet1/3
no nameif
no security-level
```

```

no ip address
shutdown
!
interface GigabitEthernet1/4
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/5
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/6
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/7
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/8
no nameif
no security-level
no ip address
shutdown
!
interface Management1/1
management-only
no nameif
no security-level
no ip address
!
!
telnet timeout 5
ssh timeout 5
!
!

```

Alla GigabitEthernet1/1 è assegnato il nome inside con livello di sicurezza 100 mentre alla GigabitEthernet1/2 è assegnato il nome outside con livello di sicurezza 0.

Il security-level è un numero compreso tra 0 e 100 che definisce la credibilità della rete a cui è collegata l'interfaccia; maggiore è il numero, maggiore è la fiducia che si ha nella rete. Ad esempio, la rete più sicura, come la LAN interna, dovrebbe avere il livello di sicurezza 100. La rete esterna connessa a una rete non attendibile (come Internet) dovrebbe avere il livello 0. L'interfaccia connessa alla DMZ dovrebbe avere il livello di sicurezza impostato su un valore compreso tra 1 e 99 (solitamente 50).

Per impostazione predefinita, il traffico può passare dall'interfaccia di livello di sicurezza superiore a quella inferiore mentre viene negato dal livello di sicurezza inferiore a quello superiore. Per modificare questo comportamento è necessario utilizzare gli ACL.

## Impostazione delle GigabitEthernet 1/1

La configurazione di default dell'interfaccia è già adatto alla nostra rete.

## Impostazione delle GigabitEthernet 1/2

```
ciscoasa# configure terminal
ciscoasa(config)# interface gigabitEthernet 1/2
ciscoasa(config-if)# ip address 192.168.20.2 255.255.255.252
```

Lasciamo invariato il livello di sicurezza.

## Impostazione delle GigabitEthernet 1/3

```
ciscoasa(config)# interface gigabitEthernet 1/3
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 192.168.20.2 255.255.255.252
ciscoasa(config-if)# no shutdown
```

## Impostazione Route

Definiamo una rotta statica per indirizzamento traffico verso l'esterno.

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 192.168.2.2
```

## Impostazione ACL

```
ciscoasa(config)# access-list in-to-internet extended permit icmp any any echo-
reply
ciscoasa(config)# access-list in-to-internet extended permit tcp any 192.168.1.0
255.255.255.0 gt 1024
ciscoasa(config)# access-list in-to-internet extended permit tcp any host
192.168.3.100 eq 80
```

*A differenza delle ACL impostata nei router la wildcard mask presente negli indirizzi è sostituita da una subnet mask.*

Associamo l'ACL denominata in-to-internet all'interfaccia outside in ingresso

```
ciscoasa(config)# access-group in-to-internet in interface outside
```