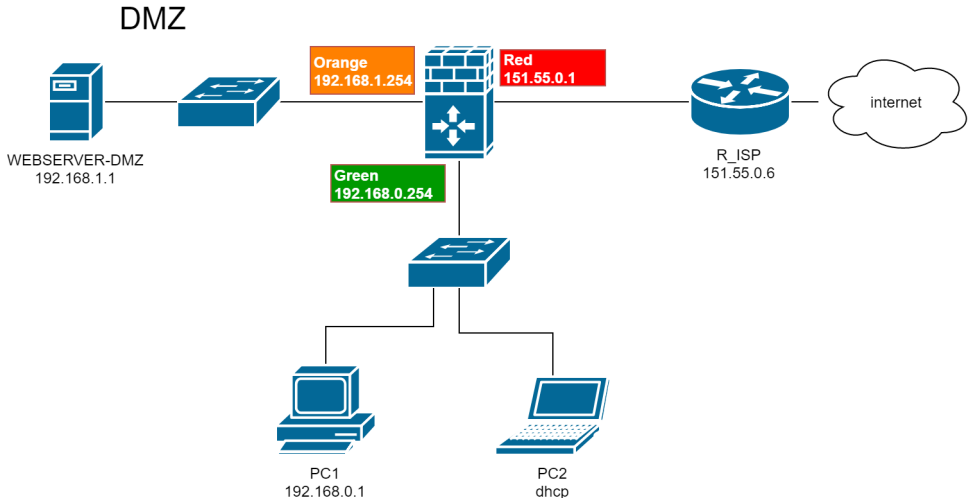
# Realizzazione di una DMZ con firewall ASA 5506X a tre interfacce




## Principali parametri di configurazione

**RETE LAN (GREEN ZONE)**

| | | |
|---|---|---|
| Network: | 192.168.0.0/24 | |
| Server DNS: | 200.1.1.1 | (server pubblico) |
| Pool DHCP: | da 192.168.0.201 a 192.168.0.230 | |
| Gateway: | 192.168.0.254 | |

**RETE INTERNET (RED ZONE)**

L’azienda dispone di otto indirizzi IPV4 pubblici.

| | | |
|---|---|---|
| Network: | 151.55.0.0/29 | |
| Indirizzi disponibili: | 151.55.0.1 | (assegnato all’interfaccia del firewall) |
| | 151.55.0.2 | (utilizzato per accedere da internet al web server posto in DMZ) |
| | 151.55.0.3 | |
| | 151.55.0.4 | |
| | 151.55.0.5 | |
| | 151.55.0.6 | (gateway dell’ISP) |

**RETE DMZ (ORANGE ZONE)**

| | | |
|---|---|---|
| Network: | 192.168.1.0/24 | |
| Server DNS: | 200.1.1.1 | (server pubblico) |
| Server WEB: | 192.168.1.1 | |
| Gateway: | 192.168.1.254 | |

## 1. Configurazione delle interfacce di rete del firewall ASA 5506X e del servizio DHCP

```
!Password vuota
enable
```

```
configure terminal
      hostname FW

      !Interfaccia green
      interface GigabitEthernet1/1
             nameif inside
             description Interfaccia collegata alla green zone (Inside)
             ip address 192.168.0.254 255.255.255.0
             security-level 100
             no shutdown
             exit

      !Interfaccia red
      interface GigabitEthernet1/2
             nameif outside
             description Interfaccia collegata alla red zone (outside)
             no ip address dhcp
             ip address 151.55.0.1 255.255.255.248
             security-level 0
             no shutdown
             exit

      !Interfaccia orange
      interface GigabitEthernet1/3
             nameif dmz
             description Interfaccia collegata alla orange zone (dmz)
             ip address 192.168.1.254 255.255.255.0
             security-level 50
             no shutdown
             exit

      !Default route (inoltra i pacchetti in uscita sull'interfaccia outside al router dell'ISP)
      route outside 0.0.0.0 0.0.0.0 151.55.0.6

      !Configurazione del servizio DHCP
      dhcpd address 192.168.0.201-192.168.0.230 inside
      dhcpd dns 200.1.1.1 interface inside
      !L’opzione 3 DHCP mposta il default gateway
      dhcpd option 3 ip 192.168.0.254
      dhcpd enable inside

      exit
```

## 2. Configurazione dei processi NAT

La configurazione è realizzata mediante gli “object network” presenti nel firewall.

```
!Source NAT dinamico per gli host della rete GREEN che accedono a internet
configure terminal
      object network RETE-GREEN
             subnet 192.168.0.0 255.255.255.0
             nat (inside,outside) dynamic interface
             exit

!Source NAT dinamico per gli host della rete ORANGE che accedono a internet
configure terminal
```

```
      object network RETE-ORANGE
             subnet 192.168.1.0 255.255.255.0
             nat (dmz,outside) dynamic interface
             exit

!Source NAT statico per l’accesso a internet per il web server posto in DMZ
configure terminal
      object network SERVER-DMZ
             host 192.168.1.1
             nat (dmz,outside) static 151.55.0.2
             exit
```

## 3. Impostazione delle attività di controllo sui pacchetti (configurazione delle policy)

Per configurare le attività di controllo da eseguire sui pacchetti in transito, è necessario configurare:

1. **class-map**: seleziona il tipo di pacchetto da controllare in base al protocollo di livello 4 (TCP, UDP, ICMP) o livello 7 (HTTP, DNS, ecc.)
2. **policy-map**: associa un’azione (policy) specifica a ogni pacchetto individuato da class-map. Le principali azioni sono: *inspect*, *permit*, *drop*, *log*.
3. **service-map**: esegue le azioni contenute nella policy sull’interfaccia specificata.

```
configure terminal
      class-map inspection_default
             !Seleziona i principali protocolli utilizzati sulla rete
             match default-inspection-traffic
             exit

      policy-map global_policy
             class inspection_default
                    inspect dns
                    inspect ftp
                    inspect http
                    inspect icmp
                    exit

      service-policy global_policy global
      exit
```

## 4. Definizione delle access-list

Per impostazione predefinita, i pacchetti provenienti da una rete meno sicura di quella a cui sono destinati (esempio: da internet a LAN) sono bloccati dal firewall. Per consentirne il transito, è necessario impostare apposite access-list.

```
configure terminal
      !ACL per i pacchetti che transitano da DMZ a LAN
      access-list DMZ-INSIDE extended permit icmp any any echo-reply
      access-list DMZ-INSIDE extended permit icmp any any unreachable

      access-group DMZ-INSIDE in interface dmz

      !ACL per i pacchetti che transitano da INTERNET a LAN
```

```
      access-list OUTSIDE-INSIDE extended permit icmp any any echo-reply
      access-list OUTSIDE-INSIDE extended permit icmp any any unreachable
      access-list OUTSIDE-INSIDE extended permit udp any eq 53 any

      access-group OUTSIDE-INSIDE in interface outside

      !ACL per i pacchetti che transitano da INTERNET a DMZ
      access-list OUTSIDE-DMZ extended permit tcp any host 151.55.0.2 eq 80
      access-list OUTSIDE-DMZ extended permit tcp any host 151.55.0.2 eq 443

      access-group OUTSIDE-DMZ in interface outside

      exit

copy running-config startup-config
reload
```