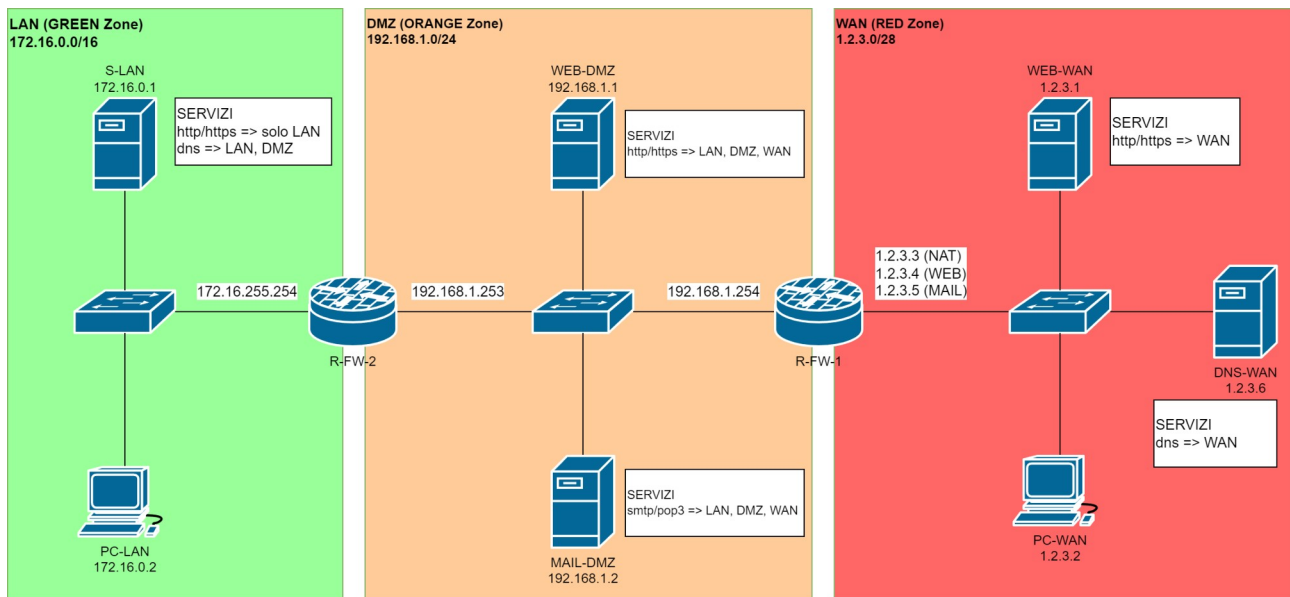


Realizzazione di una rete DMZ con Firewall Zone-Based su router Cisco 2901



Principali parametri di configurazione

RETE LAN (GREEN ZONE)

Network:	172.16.0.0/16
Server S-LAN:	172.16.0.1 Servizi erogati: http e https: solo per rete LAN; dns: reti LAN e DMZ
Client PC-LAN:	172.16.0.2
Gateway R-FW-2:	172.16.255.254

Record DNS caricati su S-LAN:

s-lan.abc.eu	A	172.16.0.1
services.abc.eu	CNAME	s-lan.abc.eu
web-dmz.abc.eu	A	192.168.1.1
www.abc.eu	CNAME	web-dmz.abc.eu

RETE INTERNET (RED ZONE)

Network:	1.2.3.0/28
Server WEB-WAN:	1.2.3.1 Servizi erogati: http e https: solo per rete WAN
Client PC-WAN:	1.2.3.2
Interfaccia R-FW-1:	1.2.3.3 (source NAT con overload) 1.2.3.4 (NAT statico per server WEB in DMZ) 1.2.3.5 (NAT statico per server MAIL in DMZ)
Server DNS-WAN:	1.2.3.6 Servizi erogati: dns: solo per rete WAN

Record DNS caricati su DNS-WAN:

mail.abc.eu	A	1.2.3.5
www.abc.eu	A	1.2.3.4

RETE DMZ (ORANGE ZONE)

Network:	192.168.1.0/24
Server WEB-DMZ:	192.168.1.1
Server MAIL-DMZ:	192.168.1.2
Gateway R-FW-2:	192.168.1.253
Default Gateway R-FW-1:	192.168.1.254

Configurazione IOS Firewall R-FW-2 a due interfacce (green, orange)

0. Caricamento della licenza "Securityk9" su router R-FW-2 (Cisco 2901)

```
enable
configure terminal
  license boot module c2900 technology-package securityk9
exit
write
reload
```

1. Definizione delle Access Control List su R-FW-2

```
!Password vuota
enable
configure terminal
  !Regole per il traffico proveniente dalla zona GREEN
  ip access-list extended REGOLE-GREEN
    permit icmp 172.16.0.0 0.0.255.255 any
    permit tcp 172.16.0.0 0.0.255.255 any
    permit udp 172.16.0.0 0.0.255.255 any
  exit

  !Regole per il traffico proveniente dalla zona ORANGE
  ip access-list extended REGOLE-ORANGE
    !Si consente solo l'accesso al servizio DNS (domain = 53)
    permit udp 192.168.1.0 0.0.0.255 host 172.16.0.1 eq domain
  exit
```

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

- 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.)
- policy-map:** associa un'azione (policy) specifica a ogni pacchetto individuato da class-map. Le principali azioni sono: *inspect*, *permit*, *drop*, *log*.
- service-map:** esegue le azioni contenute nella policy sull'interfaccia specificata.

2. Definizione delle classi su R-FW-2

```
class-map type inspect match-any CLASSE-GREEN
  match access-group name REGOLE-GREEN
  exit

class-map type inspect match-any CLASSE-ORANGE
  match access-group name REGOLE-ORANGE
  exit
```

3. Definizione delle policy su R-FW-2

```
policy-map type inspect POLICY-GREEN
  class type inspect CLASSE-GREEN
    !Stateful inspection su tutti i protocolli ammessi
    inspect
    exit
  !Azione di default = DROP
  class type inspect class-default
    drop
    exit
  exit

policy-map type inspect POLICY-ORANGE
  class type inspect CLASSE-ORANGE
    !Stateful inspection su tutti i protocolli ammessi
    inspect
    exit
  !Azione di default = DROP
  class type inspect class-default
    drop
    exit
  exit
```

4. Definizione delle zone e applicazione delle policy su R-FW-2

```
zone security GREEN
zone security ORANGE

zone-pair security GREEN-ORANGE source GREEN destination ORANGE
  service-policy type inspect POLICY-GREEN
  exit

zone-pair security ORANGE-GREEN source ORANGE destination GREEN
  service-policy type inspect POLICY-ORANGE
  exit
```

5. Configurazione delle interfacce di rete e associazione delle zone su R-FW-2

```
hostname R-FW-2
interface GigabitEthernet0/0
  ip address 172.16.255.254 255.255.0.0
  zone-member security GREEN
  no shutdown
```

```
exit

interface GigabitEthernet0/1
  ip address 192.168.1.253 255.255.255.0
  zone-member security ORANGE
  no shutdown
  exit

!Default route verso la rete WAN
ip route 0.0.0.0 0.0.0.0 192.168.1.254

exit
copy running-config startup-config
```

Configurazione IOS Firewall R-FW-1 a due interfacce (orange, red)

0. Caricamento della licenza "Securityk9" su router R-FW-1 (Cisco 2901)

```
enable
configure terminal
    license boot module c2900 technology-package securityk9
    exit
reload
```

1. Definizione delle Access Control List su R-FW-1

```
!Password vuota
enable
configure terminal
    !Regole per il traffico proveniente dalla zona ORANGE
    ip access-list extended REGOLE-ORANGE
        permit icmp 192.168.1.0 0.0.0.255 any
        permit tcp 192.168.1.0 0.0.0.255 any
        permit udp 192.168.1.0 0.0.0.255 any
        permit icmp 172.16.0.0 0.0.255.255 any
        permit tcp 172.16.0.0 0.0.255.255 any
        permit udp 172.16.0.0 0.0.255.255 any

        !In presenza di SOURCE NAT con overload, le regole devono
!fare riferimento anche all'indirizzo sorgente del router
!(il NAT viene eseguito prima del filtraggio del firewall)
        permit icmp host 1.2.3.3 any
        permit tcp host 1.2.3.3 any
        permit udp host 1.2.3.3 any
    exit
    !Regole per il traffico proveniente dalla zona RED
    ip access-list extended REGOLE-RED
        !Accesso limitato ai servizi HTTP,HTTPS, SMTP e POP3
        permit tcp any host 192.168.1.1 eq www
        permit tcp any host 192.168.1.1 eq 443
        permit tcp any host 192.168.1.2 eq smtp
        permit tcp any host 192.168.1.2 eq pop3
    exit
```

2. Definizione delle classi su R-FW-1

```
class-map type inspect match-any CLASSE-ORANGE
    match access-group name REGOLE-ORANGE
    exit

class-map type inspect match-any CLASSE-RED
    match access-group name REGOLE-RED
    exit
```

3. Definizione delle policy su R-FW-1

```
policy-map type inspect POLICY-ORANGE
```

```
class type inspect CLASSE-ORANGE
    inspect
    exit
class type inspect class-default
    drop
    exit
exit

policy-map type inspect POLICY-RED
    class type inspect CLASSE-RED
        inspect
        exit
    class type inspect class-default
        drop
        exit
exit
```

4. Definizione delle zone e applicazione delle policy su R-FW-1

```
zone security ORANGE
zone security RED

zone-pair security ORANGE-RED source ORANGE destination RED
    service-policy type inspect POLICY-ORANGE
    exit

zone-pair security RED-ORANGE source RED destination ORANGE
    service-policy type inspect POLICY-RED
    exit
```

5. Configurazione delle interfacce di rete e associazione delle zone su R-FW-1

```
hostname R-FW-1
interface GigabitEthernet0/0
    ip address 192.168.1.254 255.255.255.0
    ip nat inside
    zone-member security ORANGE
    no shutdown
    exit

interface GigabitEthernet0/1
    ip address 1.2.3.3 255.255.255.240
    ip nat outside
    zone-member security RED
    no shutdown
    exit

!Il traffico destinato alla rete LAN deve essere inoltrato
!a R-FW-2 (nessuna default route in questo esercizio)
ip route 172.16.0.0 255.255.0.0 192.168.1.253
```

6. Configurazione NAT su R-FW-1

```
ip access-list standard REGOLE-NAT
  permit 172.16.0.0 0.0.255.255
  permit 192.168.1.0 0.0.0.255
exit
```

!Source NAT con overload (IP Masquerading)

```
ip nat inside source list REGOLE-NAT interface GigabitEthernet0/1 overload
```

!NAT statico per i servizi erogati anche all'esterno dell'azienda

```
ip nat inside source static tcp 192.168.1.1 80 1.2.3.4 80
ip nat inside source static tcp 192.168.1.1 443 1.2.3.4 443
ip nat inside source static tcp 192.168.1.2 25 1.2.3.5 25
ip nat inside source static tcp 192.168.1.2 110 1.2.3.5 110
```

```
exit
copy running-config startup-config
```