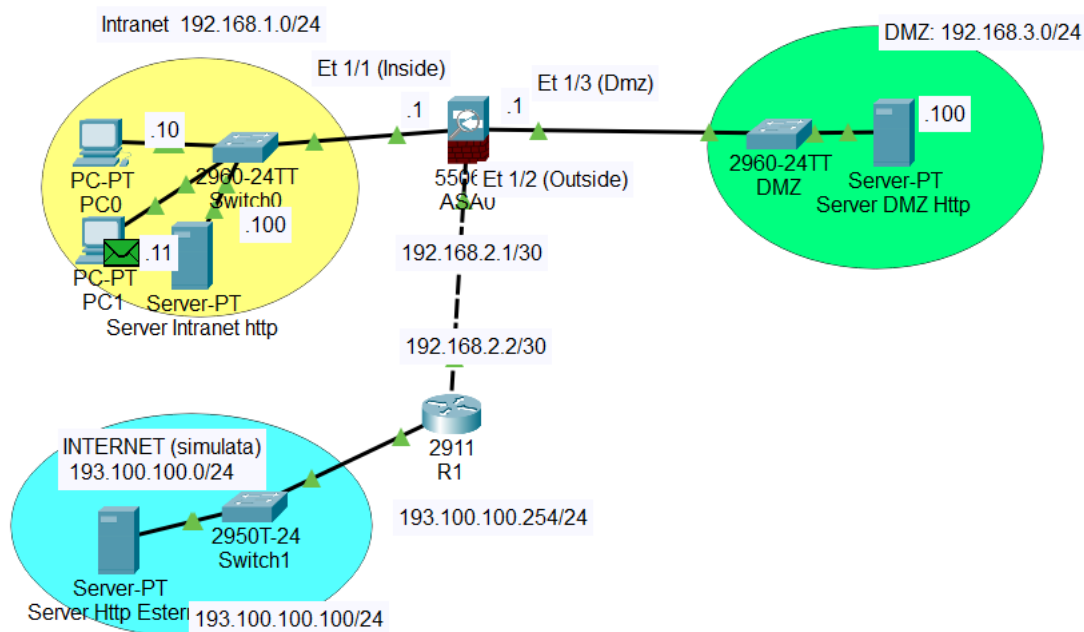


DMZ con ASA (Adaptive Security Appliances)

Introduzione al Progetto

Questo progetto illustra la configurazione di una DMZ utilizzando un dispositivo Cisco ASA 5506, che sostituisce il router R2 del precedente progetto "DMZ tramite ACL". La topologia di rete rimane invariata, mentre la configurazione si adatta alle specifiche funzionalità dell'ASA.

Topologia di Rete



Il dispositivo ASA 5506 gestisce tre zone di sicurezza:

- **Inside:** Rete interna (LAN aziendale)
- **Outside:** Rete esterna (connessione Internet)
- **DMZ:** Zona demilitarizzata (server pubblici)

Analisi della Configurazione di Default

Prima di procedere con le modifiche, esaminiamo la configurazione preesistente del dispositivo ASA:

```
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
!
[Altre interfacce disabilitate...]

```

Comprensione dei Security Level

Il security-level è un parametro fondamentale dell'ASA che definisce il livello di fiducia di ciascuna interfaccia:

- **100:** Massima fiducia (rete interna)
- **0:** Nessuna fiducia (Internet)
- **1-99:** Fiducia intermedia (tipicamente 50 per la DMZ)

Regola di default del traffico:

- Il traffico può transitare da un'interfaccia con security-level superiore verso una con security-level inferiore
- Il traffico è bloccato nella direzione opposta (da security-level inferiore a superiore)

Configurazione delle Interfacce

Interfaccia Inside (GigabitEthernet1/1)

La configurazione di default è già appropriata per la nostra rete:

- Nameif: inside
- Security-level: 100
- IP: 192.168.1.1/24

```

ciscoasa(config)# interface gigabitEthernet 1/1
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# exit

```

Interfaccia Outside (GigabitEthernet1/2)

Configuriamo l'interfaccia per la zona Outside:

- Nameif: outside
- Security-level: 0
- IP: 192.168.2.1/30

```
ciscoasa# configure terminal
ciscoasa(config)# interface gigabitEthernet 1/2
ciscoasa(config)# security-level 0
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 192.168.2.1 255.255.255.252
ciscoasa(config-if)# exit
```

Interfaccia DMZ (GigabitEthernet1/3)

Configuriamo l'interfaccia per la zona DMZ:

- Nameif: dmz
- Security-level: 50
- IP: 192.168.3.1/24

```
ciscoasa(config)# interface gigabitEthernet 1/3
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# ip address 192.168.3.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# exit
```

Configurazione del Routing

Definiamo la rotta di default per il traffico verso Internet:

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

Questa rotta indirizza **tutto** il traffico destinato a reti non note verso 192.168.2.2 cioè il router R1 attraverso l'interfaccia outside.

Configurazione delle Access Control List (ACL)

Le ACL sull'ASA utilizzano la subnet mask invece della wildcard mask utilizzata sui router Cisco.

Subnet Mask vs Wildcard Mask nelle ACL

Introduzione

Una delle differenze più importanti tra router Cisco e ASA riguarda il modo in cui vengono specificate le reti nelle Access Control List (ACL). Comprendere questa differenza è cruciale per evitare errori di configurazione.

Cisco ASA - Subnet Mask

L'ASA utilizza la **subnet mask tradizionale** nella definizione delle ACL:

- **1** = bit significativo (deve corrispondere)
- **0** = bit non significativo (ignorato)

Stessi Esempi con Subnet Mask (ASA)

Esempio 1: Host Singolo

ASA - Specificare l'host 192.168.1.100

```
access-list OUTSIDE-IN extended permit tcp host 192.168.1.100 any eq 80
```

OPPURE

```
access-list OUTSIDE-IN extended permit tcp 192.168.1.100 255.255.255.255 any eq 80
```

Subnet mask 255.255.255.255 = tutti i bit devono corrispondere

Esempio 2: Rete /24

ASA - Rete 192.168.1.0/24

```
access-list OUTSIDE-IN extended permit tcp 192.168.1.0 255.255.255.0 any eq 80
```

Confronto Diretto

Scenario	Router (Wildcard)	ASA (Subnet Mask)
Host singolo	192.168.1.100 0.0.0.0	192.168.1.100 255.255.255.255
Rete /24	192.168.1.0 0.0.0.255	192.168.1.0 255.255.255.0
Rete /28	192.168.1.16 0.0.0.15	192.168.1.16 255.255.255.240
Qualsiasi host	any oppure 0.0.0.0 255.255.255.255	any oppure 0.0.0.0 0.0.0.0

Consigli Pratici

1. Memorizzazione

- **ASA:** Usa le stesse subnet mask che useresti per configurare le interfacce
- **Router:** Pensa "al contrario" - dove la subnet ha 0, la wildcard ha 1

2. Verifica

Usa sempre i comandi di show per verificare:

```
show access-list
```

ACL per Controllo del Traffico con Gestione delle Sessioni

IMPORTANTE: L'ASA è un firewall stateful, quindi gestisce automaticamente il traffico di ritorno per le connessioni stabilite dall'interno verso l'esterno. Le ACL sono necessarie principalmente per:

1. Traffico da livelli di sicurezza inferiori verso superiori
2. Traffico tra interfacce con stesso livello di sicurezza
3. Controllo granulare del traffico permesso

ACL minima per Traffico da Outside verso Inside/DMZ con Controllo delle Sessioni (Outside → Inside/DMZ)

```
//ICMP
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

//HTTP
ciscoasa(config)# access-list in-to-internet extended permit tcp any host
192.168.3.100 eq 80

//HTTPS
ciscoasa(config)# access-list in-to-internet extended permit tcp any host
192.168.3.100 eq 443
```

ACL per permettere il ritorno delle richieste http da DMZ → Inside

```
ciscoasa(config)# access-list dmz-to-inside extended permit tcp any
192.168.1.0 255.255.255.0 gt 1024
```

Spiegazione Dettagliata delle Regole

1. Traffico Inside → Outside

- Permesso automaticamente (security-level 100 → 0)
- Return traffic gestito automaticamente dallo stateful firewall
- Nessuna ACL necessaria

2. Traffico Inside → DMZ

- Permesso automaticamente (security-level 100 → 50)
- ACL per autorizzare il ritorno delle richieste http da DMZ ????

3. Traffico DMZ → Outside

- Permesso automaticamente (security-level 50 → 0)
- Return traffic gestito automaticamente
- Nessuna ACL necessaria

4. Traffico Outside → Inside/DMZ

- Bloccato di default (security-level 0 → 100/50)
- ACL necessaria per permettere servizi specifici
- Solo servizi pubblici (web server)

5. Traffico DMZ → Inside

- Bloccato di default (security-level 50 → 100)

Applicazione delle ACL

Applica ACL solo dove necessario

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

```
ciscoasa(config)# access-group dmz-to-inside out interface inside
```

Verifica della Configurazione

Comandi di Verifica Utili

Visualizzare le interfacce e i loro stati

```
ciscoasa# show interface ip brief
```

Verificare le ACL applicate

```
ciscoasa# show access-list
```

Controllare le rotte

```
ciscoasa# show route
```

Monitorare le connessioni attive

```
ciscoasa# show conn
```

Visualizzare i security level

```
ciscoasa# show nameif
```