Prendiamo in esame il caso in cui un’azienda ha bisogno di configurare una rete con i seguenti elementi: una zona internet, una zona DMZ con all’interno server web HTTP e un server di posta elettronica SMTP, una rete interna con almeno un server o nas e infine un firewall perimetrale posizionato tra le zone.

Per soddisfare la richiesta, ho trovato due principali possibili configurazioni, ognuna con i suoi punti di forza e debolezza: la prima prevede un firewall perimetrale posizionato al centro della rete che gestisca il traffico tra tutte e 3 le zone, la seconda implementa la DMZ in configurazione poit-to-point, andando meglio a separare la zona sensibile dalla DMZ e da internet.

Vediamo ora le due configurazioni nel dettaglio, con i rispettivi vantaggi e svantaggi.

**Configurazione A:** Single Firewall DMZ

Questa configurazione separa le tre zone in altrettanti livelli di sicurezza: la zona internet, non attendibile, la DMZ, semi-attendibile e la rete interna, zona attendibile.

Il server HTTP e SMPT sono posizionati nella DMZ perché devono essere acceduti dall’esterno, ma, proprio perché accessibili, non contengono dati sensibili dell’azienda, le porte aperte nel firewall coincideranno con i servizi offerti dai server, nello specifico: 80 e 443 per HTTP/HTTPS, 25 per SMPT e a seconda delle necessità, anche 110 e 995 per POP3/POP3S, 143 e 993 per IMAP/IMAPS.

Il server NAS viene posizionato nella rete interna per mantenere la massima protezione, poiché contiene dati aziendali sensibili, questa configurazione fa si che vi si possa accedere Esclusivamente dalla rete interna stessa, attraverso i Clients dei dipendenti che avranno un accesso a internet controllato e stringenti politiche di sicurezza.

Il firewall perimetrale avrà quindi una configurazione simile a questa:

**Traffico verso la DMZ**

**DALLA ZONA ALLA ZONA PORTA PROTOCOLLO AZIONE**

Internet Web Server 80,443 TCP PERMETTI

Internet Mail Server 25 TCP PERMETTI

Rete Interna Web Server 80,443 TCP PERMETTI

Rete Interna Mail Server ALL TCP PERMETTI

**Traffico verso Rete Internet**

**DALLA ZONA ALLA ZONA PORTA PROTOCOLLO AZIONE**

Internet Rete Interna ALL ALL NEGA

DMZ Rete Interna LIMITED TCP PERMETTI

Rete Interna DMZ ALL TCP PERMETTI

Rete Interna Internet ALL TCP PERMETTI

Si possono aggiungere misure di sicurezza aggiuntive alla DMZ, come IDS/IPS, web-app Firewall per il web server e hardening dei sistemi operativi. Per la rete interna si può implementare l’autenticazione a due fattori, un sistema di login centralizzato, backup regolari e password robuste.

**Pregi**:  
-Economico (richiede un solo firewall e una sola licenza)

-Facile da manutenere

-Configurazione semplice

-Troubleshooting rapido

-Gestione Centralizzata

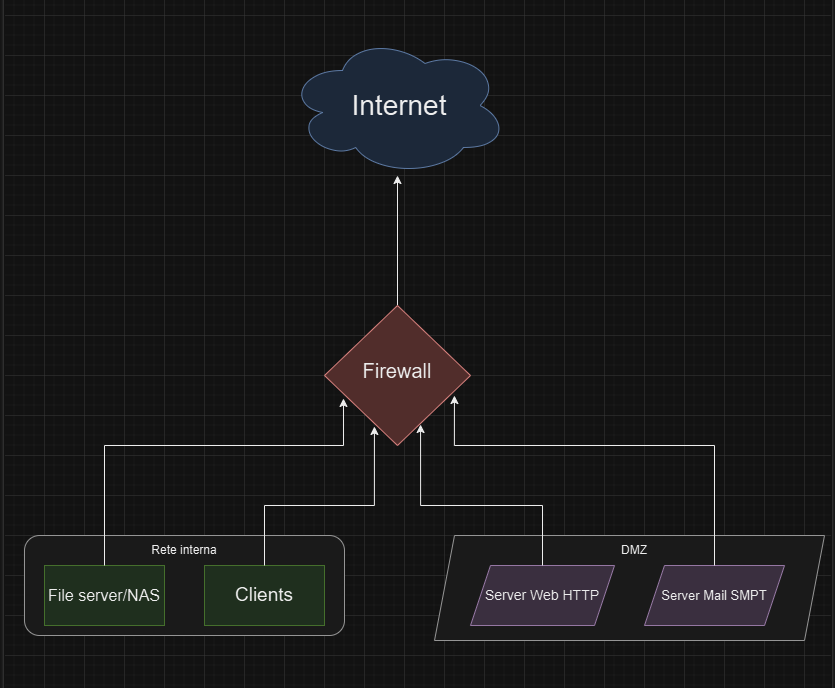
**Difetti:**

-Sicurezza ridotta (se è compromesso il firewall centrale, è compromessa l’intera rete)

-Performance ridotta (tutto il carico è su un singolo dispositivo)

-Possibili colli di bottiglia

**In sunto**: la configurazione single firewall è adatta ad aziende più piccole con capacità ridotta, poiché richiede un investimento iniziale minore e minori costi di manutenzione e gestione, offrendo una sicurezza sì ridotta rispetto alla point-to-point, ma comunque robusta.



**Configurazione B:** Point-to-point

Questa configurazione prevede l’utilizzo di due firewall: uno che regola il traffico da internet alla DMZ e e l’altro che regola il traffico dalla DMZ alla rete interna. Come nella configurazione A, i server HTTP e SMPT sono posizionati nella DMZ e il server NAS con i client nella rete interna. Permette un più facile utilizzo di VLAN per separare le reti ed è meno attaccabile, avendo diverse “camere stagne” isolate, rendendo più difficile il movimento orizzontale a un eventuale attaccante.

I due firewall avranno configurazioni differenti:

**Firewall esterno (Internet > DMZ)**

**DALLA ZONA ALLA ZONA PORTA PROTOCOLLO AZIONE**

Internet Web Server 80,443 TCP PERMETTI

Internet Mail Server 25 TCP PERMETTI

DMZ Internet 80,443 TCP PERMETTI

DMZ Internet 53 UDP PERMETTI (DNS)

Specifice: questo firewall protegge da attacchi esterni anche grazie all’integrazione di IDS/IPS, gestisce il NAT pubblico ed ha un Anti-DDoS protection

Firewall interno (DMZ > Rete interna)

**DALLA ZONA ALLA ZONA PORTA PROTOCOLLO AZIONE**

DMZ Interna 3306 TCP PERMETTI (MySQL)

DMZ Interna 53 UDP PERMETTI (DNS)

Interna DMZ ALL TCP PERMETTI

Interna Internet 80,443 TCP PERMETTI

Specifiche: Protegge la rete interna, ha policy più restrittive e un NAT interno

**Pregi:**

-Doppio controllo del traffico

-Trouble shooting più dettagliato

-Offre maggiore flessibilità di configurazione

**Difetti:**

-Maggiore investimento iniziale (richiede due firewall e due licenze)

-Maggiore costo di manutenzione

-Maggiore abilità tecnica richiesta

**In sunto:** questa configurazione offre una protezione maggiore e una più facile e precisa recovery nel caso di un attacco andato a segno, tuttavia, il maggiore costo iniziale e di manutenzione, limita l’opzione ad aziende più grandi, con estremo bisogno di proteggere efficacemente i loro dati sensibili.

