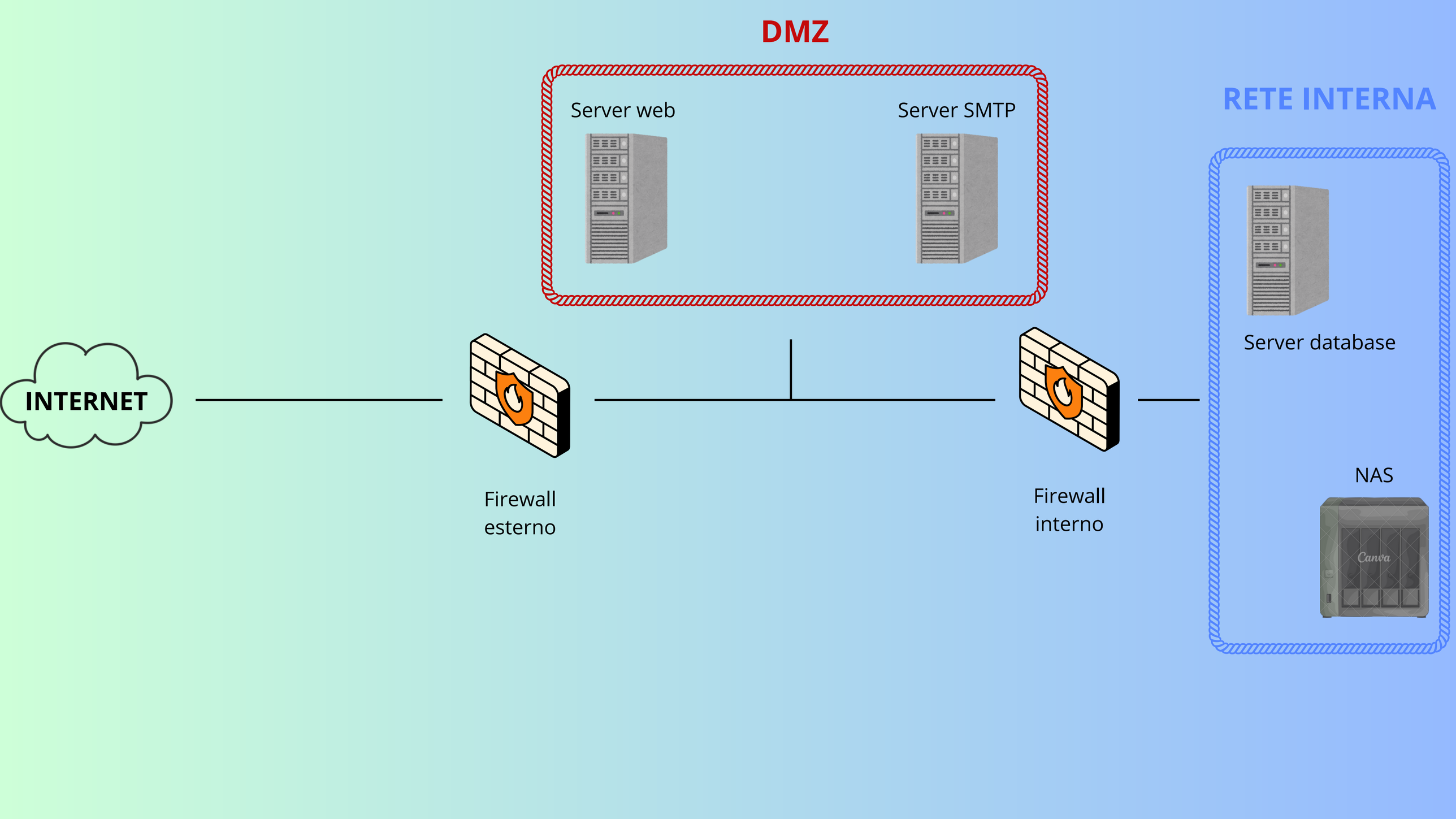

DMZ
Server web
Server SMTP
RETE INTERNA
Server database
INTERNET
Firewall
esterno
Firewall
interno
NAS
Canva

1. Il firewall esterno protegge la DMZ. In questo caso, avendo un server web ed un server SMTP, filtra il traffico consentendo solo le connessioni HTTP e HTTPS sulle porte 80 e 443, e il traffico SMTP sulla porta 25 e 587.

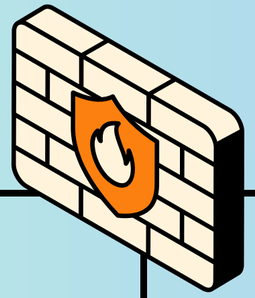
2. La DMZ, separata dalla rete interna, ospita ed isola i server pubblici come il server web e il server SMTP che sono accessibili da internet. Cosi si evita che eventuali attacchi a questi servizi compromettano la rete interna.

3. Il firewall interno è un’ulteriore barriera che si trova tra la DMZ e la rete interna. Il suo compito principale è quindi quello di controllare e filtrare il traffico tra la DMZ e la rete interna. Potrebbe essere configurato per consentire connessioni verso il server o il nas solo su determinate porte.

4. La rete interna ospita le risorse sensibili come un server database o un nas. Il firewall interno gestisce e filtra anche il traffico tra dispositivi interni e server/nas interni.

INTERNET

Firewall perimetrale



Server database

NAS

PC/LAPTOP

DMZ

Server web

Server SMTP

In questa rete più semplice (e quindi con costi ridotti), il firewall:

1. Blocca le connessioni non autorizzate che provengono da internet verso la DMZ o la rete interna
2. Consente solo il traffico autorizzato in base alle regole configurate verso la DMZ (in questo caso richieste HTTP/HTTPS al server web e SMTP al server mail)
3. Impedisce connessioni dirette dalla DMZ alla rete interna, eccetto quelle autorizzate su determinate porte (ad esempio il protocollo IMAP per l’inoltro delle mail dal server SMTP al server interno)