I firewall sono di massima importanza affinché la rete aziendale rimanga sicura. Qui di seguito mostriamo alcune configurazioni che sono state implementate nel firewall:

Nella prima immagine vediamo come possiamo configurare le interfacce del firewall assegnando impostazioni come IP, il nome scelto e il livello di sicurezza da aggiungere in base all’affidabilità dei dispositivi. Data la suddivisione della rete in tre zone è importante settare le interfacce in ordine di sicurezza: ad esempio l’intranet verrà utilizzata da impiegati quindi avrà un livello di sicurezza alto(100).

Nella seconda immagine vediamo una lista di ACL. Le ACL (Access Control Lists) sono regole configurate per controllare il flusso del traffico di rete in base a criteri specifici. Queste regole definiscono quali pacchetti di rete possono passare attraverso il firewall e quali devono essere bloccati e possono essere basate su vari criteri, come indirizzi IP sorgente e destinazione, numeri di porta, protocolli di rete e altro ancora. Le ACL nei firewall sono fondamentali per la sicurezza della rete, poiché consentono di limitare l'accesso alle risorse di rete solo a quelle persone o sistemi autorizzati, proteggendo così la rete da accessi non autorizzati o minacce esterne. Le ACL impostate nel firewall-Theta permettono protocolli quali icmp, udp o tcp di navigare in base alle proprie preferenze e di arrivare anche a specifiche porte. Le ACL si avvieranno una volta mandato il tipico comando “access-group” con il nome scelto della regola configurata.

In questo firewall, e anche in altri dispositivi, abbiamo impostato tutto il necessario per una rete professionale come dhcp DNS e un NAT ; nei router abbiamo implementato anche un OSPF(protocollo di routing per determinare l’instradamento dei pacchetti all’interno di una rete..