Operativna varnost, je **aktivno varovanje omrežja ali njegovih storitev, s pomočjo up-to-date informacij o napadih** in stanju omrežja.

V glavnem ločimo pri operativni varnosti dva tipa dela: - Intrusion prevention - Intrusion detection Pri prvem skušamo vdor preprečiti na kakršenkoli način lahko, pri drugem pa, če je do vdora prišlo, ga skušamo zaznati in pravilno odreagirati.

Intrusion Prevention System je velikokrat implementiran v **požarni pregradi** na omrežju, kjer ta ščiti: - Notranjost pred zunanjostjo - Zunanjost pred notranjostjo Ta sistem filtrira ves promet, prepušča SAMO TISTI promet ki je dopusten glede na politiko in je IMUN na napade.

Požarna pregrada lahko deluje z večimi vrstami filtriranja: - Brezstanjsko filtriranje paketov (*stateless, traditional*) Filtriranje na *omrežni plasti* - Stanjsko filtriranje paketov (*stateful filter*) Filtriranje na *prenosni plasti* - Aplikacijski prehod (*application gateway*) Filtriranje na *aplikacijski plasti*

Brezstanjsko filtriranje paketov

Tega po navadi izvaja že router, pregleda posamezen paket in se odloči na podlagi: - IP izvornega/ponornega naslova - Številke IP protokola: TCP, UDP, ICMP, OSPF itd. - TCP/UDP izvornih in ciljnih vrat - Tip sporočila ICMP - TCP SYN in ACK bitov

Takšno filtriranje opisujemo s **dostopovnimi seznami** (Access Control List).

Stanjsko filtriranje paketov

Ta je bolj napreden saj moramo hraniti podatke o stanju recimo TCP povezave in lahko na podlagi stanja povezave in ali je veljavna ali ne.

Pač ga opisujemo **razširjenim dostopovnimi seznami** (Extended Access Control List).

Aplikacijsko filtriranje paketov

Še naprednejše filtriranje paketov, kjer požarna pregrada ne gleda samo TCP/IP paketov, temveč poskusi razumeti kaj te paketi pomenijo aplikacijski plasti.

IPS kot požarna pregrada zaznava zgolj podatke v glavah, lahko pa da se napad pojavi v podatkih paketa. Takrat pride v igro njegov komplement IDS, ki pa naredi poglobljeno analizo paketov. Na podlagi vstopa sumljivih podatkov lahko naprava njihov vstop ali razpošlje obvestila.

Te naprave IPS/IDS si gradijo profile prometa, ki analizirajo razne metrike in pomene, ter te profile lahko primerjajo z podatkovno bazo znanih napadov, kjer če ugotovijo podobnosti, lahko napovedo za gre za napad. Ali pa delujejo na podlagi atipičnega prometa, takšen, ki ni običajen za omrežje ipd; - *signature-based* oz. vzorci napada in profili - *anomaly-based*