# Služba Web Application Firewall (WAF)

Ochrana perimetru počítačové sítě bude realizována dvěma Next Generation Firewally (dále jen NGFW), boxy běžící v HA (vysoká dostupnost) clusteru v režimu active/passive. Tuto problematiku řeší aktivita „Realizace perimetrového a centrálních firewallů“. Na toto, ucelené řešení, navazuje služba Web Application Firewall (WAF), která bude provozována na zmíněných NGFW.

Služba WAF bude mít nakonfigurované Web aplikační profily, které budou detekovat a blokovat známé útoky webových aplikací. Dále tyto profily WAF budou nakonfigurovány tak, aby používaly signatury a omezení pro kontrolu webového provozu. V neposlední řadě budou vynucovány zásady metody HTTP/HTTPS, která řídí metodu HTTP/HTTPS, která odpovídá zadanému vzoru.

Jednotlivé WAF profily, pro omezení protokolu http/https, budou aplikovány přímo na NGFW, při nastaveném režimu kontroly na proxy.

Aktualizace produktu, servisní podpora a aktualizace používaných signatur je požadována na dobu minimálně 2 let.

## Specifikace minimálních požadavků technického řešení

Klíčové vlastnosti Web aplikačních profilů služby WAF na NGFW:

1. **Detekce a blokování útoků**: WAF profily budou detekovat a blokovat známé útoky na webové aplikace pomocí signatur a omezení.
2. **Politika http/https metod**: Umožňují vynucení politiky http/HTTPS metod, což kontroluje, které http/https metody odpovídají specifikovanému vzoru.
3. **Přizpůsobitelné profily**: Umožní přizpůsobit výchozí profil nebo vytvořit vlastní profil pro aplikaci přístupových pravidel a omezení http/HTTPS protokolu na provoz.
4. **Proxy-based inspekce**: WAF profily půjdou aplikovat na firewall politiky při inspekčním režimu na proxy-based.
5. **Ochrana proti SQL Injection a obecným útokům**: Konfigurace WAF profilu bude zahrnovat ochranu proti SQL Injection a obecným útokům.
6. **SSL inspekce**: Pro ochranu webového serveru bude možné nastavit SSL inspekci s hlubokou inspekcí a ochranou serveru.