č. položky	Vlastnosti HW IPS sondy	Popis nebo přesný odkaz na dokumetací, vč. kapitoly, čísla stránky apod.
1	Propustnost zařízení 8Gps, 2x 10GE SFP+ port, 6x 1GE port RJ45 nebo SFP	
2	Minimální garantovaná propustnost SSL 3Gps, velikost klíče min. 2048, počet spojení za sekundu min. 5000	
3	Minimální počet spojení za sekundu 200.000 v nežném provozu(SSL provoz min. 10%)	
4	Podporované nasazení senzoru (také podpora pro port clustering nebo High-availability): - SPAN nebo Hub - Tap - Inline, fail-closed - Inline, fail-open	
5	Externí fail-over 10 Gbic porty zabudované fail-over, na straně zadavatel jsou SFP+(Cisco) sloty, optický přenos stačí MM(může být i SM...)	
6	Interní fail-over pro metalické porty	
7	DoS profily: 300	
8	Latence méně než 100 mikrosekund v běžném provozu	
9	Senzor využívá dedikovaný LAN Management port pro komunikaci s "Manager serverem", podpora IPv4 a IPv6	
10	Oddělený managment SW od sondy nebo garance, že management nebude mít dopad na výkon sondy	
11	Možnost "High Availability" řešení, obnovy po havárii a balancování zátěže pro nepřetržitý vysoký výkon	
12	Zařízení Intrusion Prevention System (IPS) filtruje v reálném čase síťový provoz a podle stanovené politiky blokuje nebo upozorňuje na provoz, který by mohl být hrozbou pro vnitřní stroje a infrastrukturu.	
13	Chrání prostředí před známými i neznámými hrozbami pomocí hloubkové inspekční technologie (kombinace úplné analýzy protokolu, reputačního hodnocení hrozeb a behaviorální analýzy podezřelého chování), ochrana proti útokům typu callbacks, Dos, Zero-day aj.	
14	Jako reakce na vzniklou událost je možné použít zaslání záznamu do syslogu.	
15	V IPS jsou obsaženy/aktualizovány signatury pro pokrytí OWASP top 10 útoků.	
16	Ochrana virtuálního prostředí	
17	Pravidelné aktualizace IPS signatur od výrobce (automatické nebo manuální)	
18	Analýza provozu a signatury vztahující se na detekci a prevenci komunikace botnetů. Tyto signatury jsou minimálne 1x denne aktualizovány.	
19	V případě budoucího použití více sond možnost jednotné správy těchto IPS sond	
20	Podpora integrace se skenermi zranitelností a následné využití jejich analýz	
21	Přehled o konkrétních aplikacích	
22	Nepřetržitá aktualizace systému díky globální síti laboratoří	
23	Odlišné politiky na základě směru provozu	
24	Rozpoznávaní jednotlivých aplikací a vizualizace	
25	Ochrana webových serverů na úrovni serverové i samotné webové aplikace. IPS chrání konkrétní webové aplikace na základě jejich názvu (Apache, IIS, Facebook,...).	
26	Možnost integrace s malware sandboxem	
27	Možnost blokování vybraného provozu na základě odchylek/anomálií od statistického profilu.	
28	Funkcionalita SYN cookies pro zajištění ochrany proti nadměrnému navazování spojení.	
29	Inspekce Q v Q provozu	
30	ochrana ARP spoofing	
31	ochrana IP spoofing	
32	Inspekce MPLS provozu	
33	Inspekce IPv6 provozu	
34	Inspekce tunelovaného provozu (včetně provozu GRE)	
35	Podpora dekomprese odezvy HTTP	
36	Monitoring latence obecně	
37	Inspekce dvojitého provozu VLAN	
38	Monitorování výkonu senzoru	
39	Možnost Whitelistů a Blacklistů	
40	Zobrazení událostí protokolu monitorování senzorů CLI v manageru	
41	Zabezpečený přenos souborů ze senzoru CLI	
42	Možnost integrace s produkty třetích stran pro další analýzu	
43	možnost nastavení QoS politik	
44	Inspekce SSL provozu	
45	Firewall politiky	
46	Pravidla přístupu firewall (ACL na L3, L4)	
47	Rozpoznávání a ochrana na aplikační vrstvě 7 OSI modelu (například detekce shellcode v přenášených souborech a jejich hodnocení pomocí online anti-malware služby, kategorizace webů podle URL)	
48	Sběr dat a akcí z aplikační 7. vrstvy OSI modelu (minimálně pro http, ftp, netbios-ss nebo smtp)	
49	Možná anti-malware kontrola dat procházejících sondou po známych protokolech (např. Http, smtp) s následní real-time blokaci nebo identifikaci viru a vytvoření události.	
50	DNS DoS ochrana	
51	IPS politiky pro exploit útoky	
52	IPS poskytuje podporu proti DoS/DDoS útokům (Skrz předdefinované politiky nebo možnosti vytvářet vlastní na základě aktuálního provozu).	
53	Průzkumné vlastní politiky	
54	Dedikované politiky určené pro blokaci průzkumných útoků (tzv.: Reconnaissance Attacks)	
55	Politiky pro omezení síťového provozu	
56	Možnost vytváření vlastních IPS signatur a importu Snort signatur	
57	Možnost integrace s globální reputační databází (reputací IP a souborů) a integrace s geolokační databází. IPS umí na daný hodnocený provoz reagovat či využít reputaci/geolokaci jako atribut pro vytvoření pravidel.	

58	Karanténa (automatická, k dispozici skrz IPS politiky, z logu, samostatné záložky konzole). Podporovaná také karanténa skrz bezpečnostní tagy z NSX.	
59	SmartBlocking(časově omezené blokování) útoků včetně možnosti použití IP Reputation pro rozšíření SmartBlocking	
60	Kontrola informací X-Forwarder-For Header. Vyhledání pověsti a karanténa IP adres klienta v hlavičce XFF.	
61	Simulace blokování (možnost funkce simulace blokování, která umožňuje umístit senzor do neblokujícího režimu, kdy útoky nejsou blokovány, i když je k tomu nakonfigurovaná aplikovaná politika IPS.)	
62	Zachycení datových paketů s možností zobrazení (pro kliknutím z GUI na externí program WireShark nebo analogický produkt/funkcionalitu pro analýzu obsahu paketů)	
63	Řízení přístupu (podpora například TACACS)	
64	Ochrana webového serveru před útoky DoS	
65	Stanovení priority provozu	
66	Generování a export Netflow v9 nebo IPFIX na vybrané zařízení pro analýzu	
67	Ochrana vůči útokům za použití evasion techniky.	
68	Detekce Zero-Day javascript hrozeb v PDF souborech	
69	**Základní zaškolení formou instalace a nastavení sondy s min. 5 politikami dle dohody, některé politiky vyjdou z aktuálních politik na stavající IPS sondě McAffe M-2950 (v případě neznalosti správy této sondy bude ze strany zadavatele zajištěna součinnost).**	
70	**5 let podpory, nárok na nové verze SW, bezpečnostní signatury, servis HW**	
71	**Požadujeme dodávku sondy formou HW appliance (SW+HW od jednoho výrobce, záruka a servis od jednoho výrobce na celek po dobu 5 let NBD on-site) vč. managemntu. Pro stávající sondu management máme a lze do něj přidat další sondu od stejného výrobce**	
72	**Telefonická a mailová podpora v pracovních dnech od 8.00 do 16.00 hod. v českém jazyce**	