Počet	Oblast	Popis funkce/vlastnosti	Splňuje
	Vlastnosti UTM/NG firewall - obecně		
		Konzolový a management port.	ANO/NE
		Podpora VLAN, podpora LACP.	ANO/NE
	Vytvoření virtuálního kontextu s omezeným počtem zdrojů, po jejich vyčerpání bude ovlivněn pouze daný virtuální kontext, nikoli celý box.	Virtualizace v HW/OS pro min. 10 virtuálních kontextů, s možností definování maximálních povolených zdrojů(Při překročení přidělených zdrojů bude ovlivněn pouze daný virtuální kontext).	ANO/NE
	Založení izolovaného administrátorského účtu pro jeden či více konkrétních virtuálních kontextů, takový účet pak nemá přístup k ostatním virtuálním kontextům, které mu nebyly přiděleny.	Podpora izolovaných administrátorských účtů pro jednotlivé virtuální kontexty.	ANO/NE
		Možnost funkce v L2 režimu (transparentní inspekční režim) nebo v L3 režimu (router).	ANO/NE
	Vytvořit spojení přes SSL VPN za užití VPN klienta na stanici a dvoufaktorové autentizace.	Funkce SSL VPN v tunelovém režimu a režimu přístupu ke vnitřním službám přes webovou proxy s podporou aplikací RDP, SSH a HTTP; součástí nabídky VPN klient pro neomezený počet uživatelů, podpora dvoufaktorové autentizace uživatelů; jsou-li funkce SSL VPN licencovány na počet uživatelů, součástí nabídky v současné době musí být licence pro 500 uživatelů s možností rozšíření na 5000 uživatelů.	ANO/NE
		Požadované bezpečnostní funkce (pokryté licencí): antivirová inspekce, kategorizace webu/web filtering, L7 analýza aplikací, detekce narušení (IPS/IDS), ochrana před únikem citlivých dat (DLP), DNS filtr , vše s podporou výrobce na 5 let.	ANO/NE
	Otestování antivirové inspekce za pomocí využití lokálního sandbox zařízení.	Podpora antivirové inspekce: signatury automaticky aktualizované výrobcem, s možností rozšíření o inspekci tzv. sandbox technikou, která nesmí být poskytována formou cloud služby, ale jako lokální VM/HW appliance.	ANO/NE
		Funkce rozlišování aplikací pomocí L7 charakteristiky, možnost definovat vlastní aplikace pomocí signatur, automatická aktualizace od výrobce.	ANO/NE
		Funkce kategorizace webových stránek a web filtering s podporou českých a slovenských stránek	ANO/NE
		Funkce ochrany úniku citlivých dat (DLP).	ANO/NE
		Funkce Loadbalancingu provozu.	ANO/NE
		Funkce transparentního ověřování uživatelů komunikujících skrz NGFW pomocí domény (MS Active Directory).	ANO/NE
		Funkce ověřování uživatelů pomocí LDAP, RADIUS, SSO, Kerberos… s možností práce se skupinami uživatelů.	ANO/NE
		Funkce GEO IP databáze, možnosti definování politiky pomocí geolokační databáze.	ANO/NE
		Funkce reputační databáze IP adress a blokace známých botnet C&C center.	ANO/NE
		Funkce překladu IP adres (NAT).	ANO/NE
	Vytvořit logy pomocí syslog protokolu s podporou TCP a TLS (dle RFC 5425) a uložit je na předem určený cíl.	Musí splňovat požadavky na logování podle vyhlášky 316/2014 §21 jako kritický informační systém. Pro logování podporovat Syslog protokol s podporou TCP a TLS (podle RFC 5425) s možností volby cíle pro logy.	ANO/NE
		Logy musí být ve strukturovaném, zdokumentovaném tvaru.	ANO/NE
		Funkce hloubkové analýzy provozu (packet capture) pro případ řešení problému v provozu (Debug mod).	ANO/NE
	Přeposílat dešifrovaný provoz, který prošel SSL inspekcí na externí IP adresu.	Funkce přeposílání dešifrovaného provozu, který prošel SSL inspekcí na externí IP adresu.	ANO/NE
	Doplňující požadavky na firewally		
	FW cluster bude odpojen od centrálního managementu, a stále jej lze plnohodnotně spravovat pomocí lokálního GUI/CLI přímo na FW platformě. Pro lokální správu není nutné instalovat speciálního klienta - lze spravovat přes běžný webový prohlížeč, či terminál přes SSH.	FW cluster musí být možné v případě nedostupnosti centrálního managementu plnohodnotně spravovat pomocí lokálního GUI a CLI provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici.	ANO/NE
		Funkce explicitní proxy přímo na firewallu (včetně autentizace uživatelů, proxy-chainingu, podpora inspekčních mechanismů a bezpečnostních funkcí (AV, IPS, Webfilter) s kapacitou pro 1000 uživatelů.	ANO/NE
	Vytvořit pravidlo, které se vztahuje k určité aplikaci na sedmé vrstvě ISO/OSI modelu. Toto pravidlo se pak využije na správný tok a zachová se podle nastavené akce - buď provoz povolí, či zakáže.	Možnost definice FW pravidel v tzv. NGFW režimu (tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace (definované v rámci funkce rozlišování aplikací dle L7 charakteru (AppControl), nikoliv pouhý TCP/UDP port), resp. kategorie URL filteringu (nikoliv jako AppControl resp. URL filtering profil aplikovaný na dané pravidlo).	ANO/NE
		Funkce reverzní proxy (publikování webových serverů) s funkcionalitou WAF (detekce Cross Site Scripting, SQL injection, generických útoků, detekce Information Disclosure a známých exploitů, detekce Bad Botů, možnost definice a omezení parametrů (Constraint) u tolerované délky hlavičky či těla, počtu URL parametrů, Cookie), podpora manipulace s HTTP metodami (get/put/post/head/connect/options) včetně funkce Load Balancingu (round robin, static, váha, nejkratší odezva, nejmenší počet spojení) a funkce SSL offloadingu (včetně definice použitého certifikátu).	ANO/NE
		Podpora režimu redundatní IPSEC VPN se statickým routingem (bez nutnosti použití dynamického routingu).	ANO/NE
		Podpora vytváření virtuálních sítových propojů mezi jednotlivými virtuálními kontexty firewallu a to včetně akcelerace HW moduly.	ANO/NE
6x	**UTM/NG firewall geo cluster HW appliance**		
	V režimu vysoké dostupnosti musí být zachována kompletní funkčnost FW i při výpadku jednoho boxu, a to v jakémkoliv módu - Active-Active/Active-Pasive/Cluster.	Pracují v režimu vysoké dostupnosti v módu Active-Active/Active-Pasive/Cluster.	ANO/NE
	Při výpadku jednoho ze zdrojů, musí okamžitě převzít napájení zdroj druhý, zároveň musí umožňovat výměnu zdrojů za běhu boxu, aniž by to narušilo jeho funkčnost.	Redundantní napájení s funkcí Hotswap.	ANO/NE
		Min. 8x 10 GE SFP+ rozhraní na každém firewallu.	ANO/NE
		Min. 10x 1 GE SFP rozhraní na každém firewallu.	ANO/NE
		Min. 10x 1 GE RJ45 rozhraní na každém firewallu.	ANO/NE
		Propustnost firewallu min. 50 Gbps pro IPv4 (UDP pakety 64 B) i IPv6 (UDP pakety 86B).	ANO/NE
		Počet spojení na firewallu minimálně 10 miliónů celkem v jeden okamžik, min. 280 000 nových spojení za sekundu (nárůst).	ANO/NE
	Umožňuje sestavit funkční IPSec tunel s jiným FG zařízením, které tuto funkci podporuje.	Propustnost IPSEC VPN min. 40 Gbps.	ANO/NE
		Propustnost funkce IPS min. 12 Gbps.	ANO/NE
		Podpora funkce inspekce SSL provozu s propustností min. 10 Gbps v rámci jedné lokality.	ANO/NE
		Latence firewallu < 8 µs (udp pakety 64 B).	ANO/NE
		Řešení stavového firewallu a celého šifrování na HW modulech(hlavní šifrování a dešifrování provádí zabudované nebo dodané HW moduly).	ANO/NE
		Osazení všech rozhraní moduly (konektory) tj. 16xSFP SR, 8xSFP+ SR, a zbytek RJ45 pomocí originálních komponent.	ANO/NE
		Splňovat minimální požadavky na všechny kryptografické funkcionality podle zákona 181/2014 a jeho platných vyhlášek.	ANO/NE
		Podpora na 5 let v režimu 8x5xFix-time 48 h.	ANO/NE
1x	**UTM/NG firewall HW appliance**		
	V režimu vysoké dostupnosti musí být zachována kompletní funkčnost FW i při výpadku jednoho boxu, a to v jakémkoliv módu - Active-Active/Active-Pasive/Cluster.	Pracují v režimu vysoké dostupnosti v módu Active-Active/Active-Pasive/Cluster.	ANO/NE
	Při výpadku jednoho ze zdrojů, musí okamžitě převzít napájení zdroj druhý.	Redundantní napájení součástí nabídky včetně všech napájecích a propojovacích napájecích kabelů.	ANO/NE
		Min. 2x 10 GE SFP+ rozhraní na každém firewallu.	ANO/NE
		Min. 8x 1 GE SFP rozhraní na každém firewallu.	ANO/NE
		Min. 8x 1 GE RJ45 rozhraní na každém firewallu.	ANO/NE
		Propustnost firewallu min. 24 Gbps pro IPv4 (UDP pakety 64 B) i IPv6 (UDP pakety 86B).	ANO/NE
		Počet spojení firewallu minimálně 5,5 miliónů celkem v jeden okamžik , min. 250 000 nových spojení za sekundu (nárůst).	ANO/NE
		Propustnost IPSEC VPN min. 15 Gbps.	ANO/NE
		Propustnost funkce IPS min. 5 Gbps.	ANO/NE
		Podpora funkce inspekce SSL provozu s propustností min. 3,5 Gbps.	ANO/NE
		Latence firewallu < 8 µs (udp pakety 64 B).	ANO/NE
		Řešení stavového firewallu a celého šifrování na HW modulech(hlavní šifrování a dešifrování provádí zabudované nebo dodané HW moduly).	ANO/NE
		Osazení všech rozhraní moduly (konektory), tj. 8xSFP SR, 2xSFP+ SR a zbytek RJ45 pomocí originálních komponent.	ANO/NE

		Splňovat minimální požadavky na všechny kryptografické funkcionality podle zákona 181/2014 a jeho platných vyhlášek.	ANO/NE
		Podpora na 5 let v režimu 8x5xFix-time 48 h.	ANO/NE
	Centrální management		
	Všechny prvky - FW, sandbox + prvky zadavatele (Fortinet 310B) lze spravovat z centrálního managementu.	Možnost centrální správy prvků (firewally, sandbox) včetně existujících HW prvků zadavatele (Fortinet 310B).	ANO/NE
		Podpora pro správu min. 10 HW boxů a min. 30 virtuálních kontextů. Možnost rozšíření na min. 15 HW boxů a 50 virtuálních kontextů.	ANO/NE
		Dodání v podobě virtuální appliance na technologii VMware.	ANO/NE
		Podpora na 5 let v režimu 24x7xFix-time 8 h.	ANO/NE
400x	**Software pro pracovní stanice (end-point security)**		
		Podporované systémy (end-point security) MS Windows XP, 7, 8/8.1, 10, Server 2008, 2012 a 2016; Mac OSX.	ANO/NE
		Management software pro Windows Server 2008, 2012 a 2016.	ANO/NE
		Zabezpečení pracovní stanice formou antivirové inspekce, webového filtru s funkcí kategorizace, aplikační firewall.	ANO/NE
		VPN připojení s funkcí ověřování uživatele personálním certifikátem a dvoufaktorovou autentizací.	ANO/NE
		Obousměrná spolupráce s nabízenou UTM/NG firewall platformou.	ANO/NE
		Podpora výrobce a subskripce na 5 let.	ANO/NE
250x	**Generátor jednorázových hesel (tokeny)**		
		OTP se skládá z min šesti číslic, OATH TOTP (RFC6238).	ANO/NE
	Klient se přihlásí k VPN s využitím dvoufaktorové autentizace pomocí SW/HW tokenu.	Integrace s nabízenou UTM/NG firewall platformou a end-point softwarem pro VPN připojení uživatel (např. Radius server nebo integrovaná podpora).	ANO/NE
		Mobilní aplikace pro SW token musí být podporována systémy Windows Mobile,Android,iOS.	ANO/NE
		Počet SW tokenů - 200x	ANO/NE
		HW token s dobře čitelným LCD displejem a životností baterie na min. 2 roky.	ANO/NE
		Počet HW tokenů - 50x	ANO/NE
2x	**Sandboxing**		
		Analýza podezřelých souborů formou sandboxingu (spuštění, otevření podezřelého souboru v izolovaném prostředí příslušného operačního systému s reálným vyhodnocením chování daného souboru).	ANO/NE
	Výsledky kontrol sandboxu budou dostupné na centrálním managementu.	Plnohodnotná a obousměrná integrace s nabízenou firewall platformou, informace o výsledcích kontrol na sandboxu dostupné v centrálním managementu.	ANO/NE
		Dodání formou virtuální appliance nasazené v existujícím prostředí zadavatele (vSphere verze 6.5).	ANO/NE
		Požadovaná VM appliance s možností škálování výkonu licenčním navyšováním počtu běžících instancí sanboxovaného OS.	ANO/NE
		Podpora skenování souborů v režimu online nebo na span portu.	ANO/NE
		Funkce reportingu nalezených problémů.	ANO/NE
		Podporované OS MS Windows 10.	ANO/NE
		Podpora Android(výhodou, volitelně).	ANO/NE
		Počet instancí MS Windows 10 – 8x (Licenci pro OS může dodat zadavatel).	ANO/NE
		Počet instancí pro inspekci MS Office dokumentů – 4x (Licence může dodat zadavatel).	ANO/NE
		Podpora inspekce minimálně: spustitelných souborů, MS Office souborů, Adobe Flash souborů, PDF, JAR souborů, skriptů (nap. vbs) a multimediálních soborů a to včetně podpory běžně používaných archivů.	ANO/NE
		Zařízení disponuje API, pomocí kterého lze obousměrně propojit sandboxovací inspekci s aplikací zákazníka za účelem zkoumání potencionálně nebezpečných vzorků, počet takto připojených aplikací nesmí být omezován.	ANO/NE
		Součástí nabídky musí být provázání sandbox zařízení s portálem elektronické podatelny za účelem analýzy vkládaných souborů včetně potřebné implementace.	ANO/NE
		Podpora v režimu 24x7 na dobu 5 let.	ANO/NE
	Doplňující požadavky na sandboxy		
	Sandbox automaticky prohledá cílový adresář umístěný na síti, kde budou infikované soubory, které odhalí.	Podpora automatizovaného scannování potencionálně nebezpečných souborů na sdílených síťových discích přes protokol CIFS/SMB a NFS.	ANO/NE
	Do sandboxu bude naimportována custom image pracovní stanice, kterou dodá zákazník, na této image lze testovat soubory a aplikace.	Podpora zákazníkem připravené verze OS (custom VM image) - možnost importovat do sandbox prostředí image pracovní stanice (OS Windows XP, 7, 8, 8.1 a 10 + další používané aplikace) či serveru (OS Windows Server 2008,2012 a 2016).	ANO/NE
	Do sandboxu bude nasazen infikovaný/škodlivý soubor, který sandbox musí identifikovat a přidat ho do lokální AV/URL databáze, kterou sdílí s NGFW platformou.	V případě identifikace škodlivého kódu, sandbox okamžitě vytváří lokální AV/URL databázi, kterou okamžitě sdílí s NGFW platformou.	ANO/NE
	Na koncové stanici bude nainstalován patřičný SW, který funguje jako sandbox agent. Pomocí tohoto SW lze "integrovat" sandbox a využívat ho z koncové stanice pro testování souborů a aplikací.	Možnost integrace sandboxu s endpoint SW, který funguje jako Sandbox Agent.	ANO/NE
		Možnost navýšení kapacity sandboxingu rozšířením o další appliance.	ANO/NE
	Implementace		
		implementace	ANO/NE