Technické specifikace - 2x Firewall v HA (požadavky níže jsou na jeden box FW)

HW požadavky	Nabízené zboží požadavek splňuje (ANO/NE)
HW appliance (VM appliance ani software řešení není akceptovatelné)	ANO
Režim vysoké dostupnosti minimálně jako active/active a active/passive, cluster o dvou fyzických zařízeních	ANO
Velikost 1 RU	ANO
Podpora duálního napájení (redundantní zdroj)	ANO
Minimálně 4x 10 GbE SFP+ síťová rozhraní	ANO
Minimálně 8x 1 GbE SFP síťová rozhraní	ANO
Minimálně 16x 1 GbE RJ45 síťová rozhraní	ANO
Management rozhraní 1 GbE RJ45 a sériový konzolový port	ANO
Výkonové požadavky	**Nabízené zboží požadavek splňuje (ANO/NE)**
Minimální propustnost firewallu pro IPv4 i IPv6 provoz 27 Gbps (měřeno na UDP komunikaci o paketech s velikostí 512 B).	ANO
Počet současně navázaných spojení firewallu min. 3 000 000, počet nových spojení za sekundu min. 250 000	ANO
Propustnost SSL VPN min. 2 Gbps	ANO
Propustnost IPSEC VPN (AES256/SHA256) min. 12 Gbps	ANO
Propustnost funkce SSL inspekce min. 4 Gbps	ANO
Počet CPS u spojení kontrolovaných pomocí SSL inspekce min. 3 000 (spojení za sekundu)	ANO
Propustnost funkce IPS min. 5 Gbps (reálná hodnota, měřeno na běžném provozu – real world traffic, včetně logování)	ANO
Propustnost funkcí next generation firewallingu (stavový firewall, IPS, analýza aplikací) min. 3 Gbps (reálná hodnota, měřeno na běžném provozu – real world traffic)	ANO
Propustnost funkcí ochrany před hrozbami (stavový firewall, IPS, analýza aplikací, ochrana před škodlivým kódem) min. 3 Gbps (reálná hodnota, měřeno na běžném provozu – real world traffic)	ANO
Udávaná latence firewallu (udp provoz) max. 5 µs	ANO
Min. počet současně připojených uživatelů SSL VPN 500	ANO
Min. počet site-to-site IPSEC tunelů 2 000	ANO
Min. počet dial up IPSEC spojení 15 000	ANO
Funkční požadavky	**Nabízené zboží požadavek splňuje (ANO/NE)**
Grafické konfigurační rozhraní (např. webový prohlížeč) a příkazový řádek bez omezení na počet administrátorů	ANO
Bezpečnostní funkce obecně označovaných jako Next Generation firewall	ANO
Podpora virtualizace na daném HW, vytváření a provozování tzv. virtuálních kontextů – min. 10 virtuálních kontextů v ceně zařízení; každý virtuální kontext musí pracovat izolovaně, možnost propojovat jednotlivé virtuální kontext pomocí interní virtuálních propojů bez nutnosti použití fyzických interface	ANO
Podpora stavového firewallingu pro IPv4 i IPv6, podpora nat 64/46	ANO
Možnost nasazení ve všech z následujících režimu (kombinace možné pomocí použití různých režimů pro různé virtuální kontexty): L2 bridge režim (inline), L3 router/NAT režim (inline), explicitní proxy (inline/out of path), transparentní proxy (inline)	ANO
Plnohodnotná správy z lokálního management rozhraní (a to i v případě využití nástroje centrální správy, neboť i v takovém případě musí být možné firewall, resp. firewall cluster, plnohodnotně konfigurovat ve chvíli, kdy z jakéhokoliv důvodu centrální správa nebude dostupná)	ANO

Ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign On	ANO
Podpora lokální databáze a vzdálené databáze (radius, ldap, tacacs+, saml, kerberos) pro ověřování uživatelů	ANO
Ověřování uživatelů pomocí SSO funkcionality pomocí Radius Single Sign On a AD pollingu	ANO
Funkce QoS, traffic shaping a SD-WAN miminálně v režimu vytvoření overlay a underlay virtuálních sítových rozhraní zahrnující fyzické propoje, IPSEC tunely či jiná rozhraní s možností definice pravidel pro řízení směrování, strategie využívání jednotlivých linek současně a monitorování stavu jednotlivých linek	ANO
Podpora funkcí VPN brány - IPSec VPN (dle platných standardů pro možnost propojení se zařízeními třetích stran); - SSL VPN pro klientský přístup s tunelovacím režimem včetně klienta pro osobní počítače i mobilní platformy, portálový režim pro bezklientský přístup;	ANO
VPN klient pro neomezený počet přistupujících zařízení součástí nabídky	ANO
Podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3	ANO
Antivirový engine musí být vybaven lokální databází vzorků škodlivého kódu a AI/ML enginem pro identifikaci podezřelých či neznámých vzorků	ANO
Funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (tzv. mobile malware), detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak), podpora sanitarizace aktivního obsahu běžných kancelářských dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby); podpora napojení na sandboxovací funkce včetně funkce akceptace lokálních signaturových databází generovaných sandboxem, vše bez nutnosti instalace pluginů do prohlížeče.	ANO
Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 4 000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace	ANO
Možnost definice zakázaných slov pro vyhledávání na internetu	ANO
Podpora funkce safe search pro populární vyhledavače	ANO
Funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), podpora definice časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit, výrobcem aktualizovaná a udržovaná databáze, vynikající pokrytí českého internetu; požadované akce – povolení stránky, logování stránky, brouzdání s proklikem, nutnost autentizace uživatele pro určitou kategorii, možnost definice časových kvót pro uživatele a kategorie webu	ANO
Podopra kategorizace stremovaných videí a kanálů min. pro platformu Youtube a Vimeo	ANO
Funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů	ANO
Možnost blokovat sítový provoz na základě URL, kategorie webové stránky, IP adresy (rozsah u), GeoIP databáze, data a času	ANO
Funkce ochrany před unikem citlivých dat (data leak prevention), která umí zachytit pokus o odeslaní/upload označeného dokumentu přes internet na základě vodoznaků, popisu regulárním výrazem atp.	ANO
Podpora dvoufaktorové autentizace pomocí HW nebo mobilních OTP tokenů, součástí nabídky musí být 2 testovací HW/mobilní tokeny a plně funkční řešení dvoufaktorového OTP ověřování uživatelů pro administrátory a uživatele VPN	ANO
Podpora a záruka výrobce na 5 let v režimu 24x7 (min. podpora výrobce, dopředná výměna HW, bezplatná aktualizace FW a subskripcí)	ANO
~~Dále je předmětem veřejné~~ zakázky **prodloužení technické podpory pro stávající FortiAnalyzer VM: FortiAnalyzer VM, SW podpora 24x7 FortiCare (for 1-6 GB Logs/Day) po dobu 60 měsíců.**	ANO