Specifikace plnění

Obecné požadavky na celé řešení	Splnění ANO/NE	Komentář ke způsobu plnění požadavku (pokud je relevantní)
Na základě bezpečností strategie Zadavatele, Zadavatel z důvodu použití "Dual Vendor" strategie výslovně vylučeje použití technologie od výrobce Fortinet, jehož bezpečnostní řešení je použito v IT částí infrastruktury Zadavatele	ANO	[redacted]
Zadavatel si v případě nejasnosti technických parametrů vyhrazuje právo otestovat jakýkoliv z požadavků v rámci PoC testu, který bude proveden před uzavřením kupní smlouvy na náklady Uchazeče, a to v rozsahu nezbytně nutném	ANO	
Na každou část řešení musí být poskytnuta podpora výrobce jak na software tak hardware, všechny licence a související po dobu 5 let od předání. Výměna vadného hardware musí být v režimu 8x5 NBD. Při nedodržení parametru výměny vadného hardware ŘSD náleží sankce 1 ‰ z ceny zařízení za každý započatý den zpoždění	ANO	
Veškeré komponenty celého řešení musí být nezávislé na virtualizačním prostředí zadavatele. Musí tak být dodány jako HW appliance	ANO	[redacted]
U každé požadované funkcionality musí být uveden odkaz do veřejně dostupné dokumentace, případně do dokumentace vytvořené dodavatelem, kde je jasně popsán způsob plnění daného parametru. Tyto informace budou využity zadavatelem ke kontrole plnění tohoto parametru	ANO	

Požadavky na Centrální management (CM)	Splnění ANO/NE	Komentář ke způsobu plnění požadavku (pokud je relevantní)
Výrobce a model nabízeného produktu:		[redacted]
P/N a další specifikace nabízeného produktu:		[redacted]
Obecné požadavky	**Splnění ANO/NE**	**Komentář ke způsobu plnění požadavku (pokud je relevantní)**
CM musí být pro prvky typu FW NG	ANO	[redacted]
Velikost každé CM appliance je maximálně 2U a rozměrově kompatibilní s 19" rozvaděčem	ANO	2U
Součástí dodávky je sada pro instalaci do 19" rozvaděče	ANO	
Hardware požadavky	**Splnění ANO/NE**	**Komentář ke způsobu plnění požadavku (pokud je relevantní)**
CM musí být typu HW appliance	ANO	[redacted]
CM musí obsahovat jeden dedikovaný port pro správu pomocí konzole - OOB management	ANO	
CM disponuje minimálně 4 datovými porty o rychlosti 1G (metalické)	ANO	2x RJ-45 100Mbps/1Gbps/10Gbps + 2x SFP+ 10Gbps ports
CM disponuje dvěma nezávislými redundantními zdroji napájení AC 230V	ANO	Dual power supplies, hot swap redundant configuration 800 / 1200W
High Availability požadavky (HA)	**Splnění ANO/NE**	**Komentář ke způsobu plnění požadavku (pokud je relevantní)**
CM musí být dodán v režimu HA v módu Active-Active nebo Active-Standby složený alespoň ze dvou zařízení	ANO	Active/Passive
CM musí podporovat režim HA i v geograficky oddělených lokalitách	ANO	[redacted]
Funkční požadavky	**Splnění ANO/NE**	**Komentář ke způsobu plnění požadavku (pokud je relevantní)**
Řešení slouží pro centrální správu všech nabízených firewallů v režimu vysoké dostupnosti (tedy dvě HW appliance v režimu Active-Active nebo Active-Standby)	ANO	Active/Passive
Součástí dodávky musí být případné licence pro centrální správu tak, aby bylo možné centrálně spravovat všechny dodané FW NG HW appliance včetně všech virtuálních kontextů až do celkového počtu 100ks fyzických zařízení	ANO	Součástí nabídky
CM musí podporovat sběr logových záznamů, analýzu logových záznamů, správu veškerých bezpečnostních a síťových konfigurací, korelaci logových záznamů, analýzu hrozeb a korelaci hrozeb v jediné instanci	ANO	[redacted]
CM musí podporovat sběr minimálně 20 000 logových záznamů za vteřinu	ANO	[redacted]
Administrátor musí mít možnost úpravy veškeré síťové a bezpečnostní konfigurace přímo na grafickém rozhraní FW NG, a zároveň přes grafické rozhraní centrálního managementu	ANO	[redacted]
Administrátor musí mít možnost importovat FW NG spravovaný lokálně do centrálního managementu bez toho, aby došlo k výpadku provozu procházejícího daným FW NG	ANO	[redacted]
CM musí pro autentizaci a autorizaci administrátorů podporovat protokoly SAML, LDAP, Radius a lokální databázi	ANO	[redacted]
CM musí podporovat dodatečnou Multi-factor Authentication pro dodatečnou autentizaci administrátorů pro GUI, CLI i API. Multi-factor Authentication pro administrátory bude již součástí nabízeného řešení	ANO	[redacted]
CM musí podporovat definování různých administrátorských rolí povolující přístupy do jednotlivých částí konfigurace	ANO	[redacted]
CM musí podporovat vytváření šablon pro zjednodušení společné konfigurace na více firewallech	ANO	[redacted]
CM musí podporovat vytváření seskupování zařízení pro zjednodušení společné konfigurace na více firewallech a přiřazení jednotné politiky	ANO	[redacted]
Centrální dohledová konzole musí být schopna vytvářet reporty manuálně a podle časového harmonogramu	ANO	[redacted]
V grafickém rozhraní dohledové konzole lze definovat uživatelské dashboardy	ANO	[redacted]
CM firewallů musí umožňovat korelaci bezpečnostních událostí generovaných jednotlivými firewally (IPS, apod.), bez nutnosti instalace další HW nebo VM appliance.	ANO	[redacted]

CM musí podporovat integraci s autentizačními systémy pro možnost mapování uživatelských identit na ip adresy (získané uživatelské identity je možné použít pro vytváření bezpečnostních politik a monitoring událostí)	ANO	[redacted]
CM musí podporovat redistribuci získaných uživatelských identit na všechny spravované NFGW	ANO	[redacted]
CM musí podporovat auditní logování konfiguračních změn	ANO	[redacted]
CM musí zobrazit rozdíl mezi stávající a novou konfigurací na jednotlivých firewallech (před instalací FW politiky)	ANO	[redacted]
CM musí umožňovat kopírování politik z jednoho FW (z jedné politiky) na jiný FW (do jiné politiky) (v rámci jednoho centrálního managementu)	ANO	[redacted]
CM umožňuje pravidelné zálohy konfigurace nebo částí konfigurace (FW pravidla, objekty, routing…) na externí úložiště pomocí protokolu SFTP nebo SCP	ANO	[redacted]
CM musí umožnovat uložení minimálně 40TB logů	ANO	48 TB
CM musí umožňovat zálohování logů na externí úložiště logů z důvodů archivace logů zabezpečeným protokolem s autorizací, například SFTP, SCP	ANO	[redacted]

Požadavky na Firewally NG shodné pro všechny typy (FW NG)		
Obecné požadavky	**Splnění ANO/NE**	**Komentář ke způsobu plnění požadavku (pokud je relevantní)**
Typ zařízení Next-generation firewall	ANO	[redacted]
FW NG musí podporovat licenční model nezávislý na počtu ochraňovaných koncových systémů	ANO	bez licenčního omezení
Zařízení typu next-generation firewall (dále pouze FW NG) je jako celek složen z komponent jednoho výrobce a to i včetně všech dalších poskytovaných bezpečnostních funkcionalit typu IPS, AV, AS signatur, databází pro URL fitering sanbox funkcionality apod. Zároveň je výrobcem zajištěna podpora minimálně po dobu plánované životnosti FW NG, tedy pěti let od data dodání.	ANO	[redacted]
Pokud je pro jakoukoliv popisovanou funkcionalitu třeba licence, tak tato licence musí být součástí nabídky	ANO	všechny potřebné subscribce/licence jsou součástí nabídky
V případě expirace licence, nebo podpory, nesmí být omezena funkcionalita bezpečnostního systému s výjimkou čerpání aktuálních bezpečnostních dat (analýza bude probíhat z poslední uložené databáze na zařízení). V žádném případě nesmí být omezena schopnost plnohodnotně spravovat zařízení.	ANO	[redacted]
Všechny požadované funkcionality musí být možné zapnout v jednom časovém okamžiku, bez nutnosti přepínat zařízení nebo porty mezi jednotlivými módy apod. Tento požadavek se netýká funkcionalit, které se vzájemně logicky vylučují, např. HA v režimu Active-Active či Active-Passive. V případě, že některé funkcionality nejsou vzájemně kompatibilní, nebo nejsou dostupné v jednom módu, je vyžadováno, aby tato skutečnost byla výslovně popsána	ANO	[redacted]
Pokud jsou požadované funkcionality dostupné pouze ve specifickém módu zařízení, je požadováno, aby veškeré udávané hodnoty propustnosti byly měřeny právě v tomto módu. Pokud jsou hodnoty v oficiálních datasheetech udávány v jiném módu, dodavatel je povinen dodat vlastní měřící protokoly. V tomto módu bezpečnostního systému bude též prováděno měření propustnosti v rámci PoC.	ANO	[redacted] nepodporuje vícero módů provozu. Hodnoty v datasheetech jsou uváděné v tomto jediném módu
Pokud nabízený FW NG některou z požadovaných funkcionalit nesplňuje, je možné tuto funkcionalitu doplnit bezpečnostním systémem jiného výrobce. Pokud k takovému doplnění dojde, je požadováno uvést, která funkcionalita je poskytována jiným nástrojem, než FW NG.	ANO	viz. poznámky
Pokud je dodán bezpečnostní nástroj nad rámec FW NG, je požadováno provést jeho integraci do dodávaného centrálního managementu tak, aby bylo možné všechny bezpečnostní události analyzovat v jednotném rozhraní. Požadovaná integrace musí být součástí dodávky.	ANO	Do nabídky je zahrnutý centrální management
Hardware požadavky	**Splnění ANO/NE**	**Komentář ke způsobu plnění požadavku (pokud je relevantní)**
FW NG je typu HW appliance stejně jako všechny doplňkové systémy	ANO	[redacted]
FW NG obsahuje jedno dedikované rozhraní serial console pro kompletní lokální správu zařízení (RJ-45 nebo USB)	ANO	[redacted]
FW NG obsahuje jedno dedikované rozhraní sloužící jako Out-of-Band management - 1GbE RJ45	ANO	[redacted]
FW NG musí obsahovat alespoň jeden dedikovaný OoB management port pro správu FW NG pomocí protokolu IP. Tento port musí splňovat: - možnost využít jej pro správu FW NG (nastavení interface, routingu, bezpečnostních pravidel apod.) pomocí API, CLI a GUI - použít jej pro monitoring stavu FW NG (SNMP apod.) - použít jej pro čerpání služeb NG-firewallem (NTP, DNS apod.) - kompletní oddělení od datových interfaců tak, že jeho nastavení žádným způsobem nezasahuje do směrovací tabulky určené pro manipulaci s daty procházejícími FW NG	ANO	[redacted]
Modul pro zpracování dat (tzv. data-plane) musí být v architektuře FW NG hardwarově oddělen od řídícího modulu (tzv. control-plane) tak, aby nemohlo dojít k jejich vzájemnému ovlivnění	ANO	[redacted]
FW NG pracuje s aktivní a kandidátskou konfigurací, při rekonfiguraci je měněna pouze kandidátská konfigurace, zařízení podle ní začne pracovat po dokončení konfigurace a po nahrání konfigurace administrátorem do aktivní konfigurace	ANO	[redacted]
FW NG podporuje agregaci portů pomocí protokolu 802.3ad (LACP)	ANO	[redacted]
FW NG umožňuje napájení ze dvou nezávislých větví napájení AC 230V. Pokud jsou v zařízení zdroje AC 230V musí být vyměnitelné za běhu (hot swap)	ANO	[redacted]
Velikost FW NG je maximálně 2U a rozměrově kompatibilní s 19" rozvaděčem	ANO	1U
Součástí dodávky je sada pro instalaci do 19" rozvaděče	ANO	

High Availability požadavky (HA)	Splnění ANO/NE	Komentář ke způsobu plnění požadavku (pokud je relevantní)
FW NG podporuje režim HA v módu active-standby a active-active skládající se alespoň ze dvou uzlů	ANO	[redacted]
Každý HA uzel disponuje informacemi o probíhajícím provozu a jsou synchronizovány tak, aby při výpadku jednoho FW NG nedošlo ke ztrátě informací NAT a k přerušení aktivních spojení provozu TCP & UDP procházejícího skrze FW NG	ANO	[redacted]
Každý HA uzel, nezávisle na své funkci (Active-Passive) musí být současně spravovatelný a monitorovatelný pomocí SNMP	ANO	[redacted]
Na HA řešení je možné provést failover na základě nedostupnosti druhého FW NG, up/down stavu interface, nebo nedostupnosti specifikované IP adresy, nebo více IP adres	ANO	[redacted]
Výkonnostní požadavky	**Splnění ANO/NE**	**Komentář ke způsobu plnění požadavku (pokud je relevantní)**
Všechny parametry propustnosti jsou měřeny v enterprise mixu, při nastavení FW NG v takovém módu, který umožňuje splnění všech požadovaných parametrů uvedených v technické specifikaci	ANO	[redacted]
Síťová funkcionalita	**Splnění ANO/NE**	**Komentář ke způsobu plnění požadavku (pokud je relevantní)**
FW NG plně podporuje IPv4 a IPV6	ANO	[redacted]
FW NG musí podporovat zapojení v režimech L2 (s virtuálním L3 rozhraním), L3, transparent a TAP	ANO	[redacted]
FW NG podporuje konfiguraci DHCP server a DHCP relay na externí DHCP server včetně podpory DHCP options a to i pod úrovní virtual routeru a routing instance	ANO	[redacted]
FW NG musí podporovat směrování typu Static route, OSPFv2, OSPFv3, BGP a PBR (Policy Based Routing)	ANO	[redacted]
PBR musí být možno nakonfigurovat na základě všech dostupných metrik typu interface, IP adresa, protokol a port, uživatel	ANO	[redacted]
FW NG musí podporovat aplikační detekci a kontrolu jako svou nativní funkcionalitu	ANO	[redacted]
FW NG podporuje konfiguraci Bidirectional Forwarding Detection (BFD) pro protokoly BGP a OSPF	ANO	[redacted]
FW NG podporuje možnost oddělení provozu do routing-instancí a to i pod úrovní virtuálního systému	ANO	[redacted]
FW NG podporuje konfigurace GRE tunelů	ANO	[redacted]
FW NG podporuje import/export route mezi routing instancemi (route leaking) a mezi logickými systémy (logický vnitřní interface) v rámci jednoho firewallu bez použití externího routeru, nebo externího propoje	ANO	[redacted]
Z důvodu zapojení systému do kritické infrastruktury musí být FW NG schopen čerpat čas z autentizovaného NTP serveru.	ANO	[redacted]
FW NG podporuje Multicast PIM-SM, PIM-SSM, IGMP v1, v2, and v3	ANO	
Firewall funkcionalita	**Splnění ANO/NE**	**Komentář ke způsobu plnění požadavku (pokud je relevantní)**
FW NG musí obsahovat integrovaný systém ochrany proti zranitelnostem (virtual patching) a síťovým útokům (IPS). Databáze IPS signatur musí být uložena přímo ve FW. Aplikace IPS profilu musí být granulární, na úrovni bezpečnostního pravidla	ANO	[redacted]
FW NG podporuje tvorbu bezpečnostních politik se specifikací source IP, destination IP , application, user/user group	ANO	[redacted]
Při instalaci firewall politik nedojde k výpadku navázaných spojení	ANO	[redacted]
FW NG podporuje konfiguraci ochrany firewallu na síťových rozhraních – podpora IP spoofing a UDP, ICMP a SYN floods	ANO	[redacted]
FW NG podporuje překlady adres ve formě: Statický NAT, Destination NAT, Source NAT (za jednu nebo vice IP adres), obousměrné překlady IPv4 a IPv6. Persistence překladu v rámci NAT poolu na úrovni IP.	ANO	[redacted]
FW NG podporuje konfigurace route-based site-to-sice IPsec VPN	ANO	[redacted]
FW NG poskytuje možnost prioritizace provozu a omezení využívané šířky pásma na základě zdrojové a cílové IP adresy, portu, uživatelské identity, aplikace a času (od – do, den v týdnu + čas apod.) nadbytečná komunikace je zahozena, nebo frontována	ANO	[redacted]
FW NG podporuje prioritizaci provozu na základě DSCP	ANO	[redacted]
FW NG podporuje prioritizaci provozu na základě identifikované aplikace	ANO	[redacted]
Požadavky na dešifrování	**Splnění ANO/NE**	**Komentář ke způsobu plnění požadavku (pokud je relevantní)**
FW NG nebo jiné dekrypční zařízení musí podporovat dešifrování odchozího SSL/TLS provozu, za pomoci podvržení serverového certifikátu klientům reverse proxy	ANO	[redacted]
FW NG nebo jiné dekrypční zařízení musí podporovat dešifrování příchozího SSL/TLS provozu, za pomoci naimportovaného privátního klíče interního serveru forward proxy	ANO	[redacted]

FW NG nebo jiné dekrypční zařízení musí podporovat dešifrování Secure Shell (SSH proxy) a kontrolovat tunelované aplikace	ANO	[redacted]
Dešifrovaný provoz musí být možno definovat na základě URL kategorií, i všech dalších typických parametrů, jako jsou zdrojová a cílová IP adresa, port, uživatelská identita	ANO	[redacted]
FW NG nebo jiné dekrypční zařízení poskytuje možnost dešifrovat pouze provoz spadající do rizikových skupin definovaných výrobcem FW NG nebo jiného dekrypčního zařízení	ANO	[redacted]
FW NG nebo jiné dekrypční zařízení musí podporovat dešifrování za pomocí ECC (Elliptical Curve Cryptography), včetně DHE a ECDHE pro příchozí i odchozí provoz	ANO	[redacted]
FW NG nebo jiné dekrypční zařízení musí podporovat dešifrování protokolu TLS verze 1.2 i 1.3	ANO	[redacted]
FW NG nebo jiné dekrypční zařízení musí podporovat přeposílání dešifrovaného provozu na jiné skenovací zařízení (např. DLP, analýza provozu a souborů apod.)	ANO	[redacted]
FW NG nebo jiné dekrypční zařízení musí být schopno dekryptovat TLS obecně, tedy i protokoly LDAPS, FTPS, apod., nikoliv pouze HTTPS	ANO	[redacted]
Aplikační firewall	**Splnění ANO/NE**	**Komentář ke způsobu plnění požadavku (pokud je relevantní)**
Detekce aplikace musí být součástí základní funkcionality FW NG	ANO	[redacted]
Zadání aplikace je standardním kritériem při tvorbě bezpečnostního pravidla, aplikace není přidávána jako profil	ANO	[redacted]
Definovaná aplikace je jedním "match" kritériem při policy lookup společně se source a destination IP	ANO	[redacted]
Plná podpora logování pravidel s definovanými aplikacemi a viditelný název aplikace/kategorie v zaslaném logu	ANO	[redacted]
FW NG obsahuje mimo definovaných jednotlivých aplikací i aplikační kategorie	ANO	[redacted]
FW NG detekuje aplikaci nezávisle na protokolu a portu, na kterém je provozována	ANO	[redacted]
FW NG podporuje identifikaci aplikací na nestandardních portech	ANO	[redacted]
Identifikace aplikace musí probíhat přímo v FW NG	ANO	[redacted]
FW NG musí umět pracovat s neznámými aplikacemi - upozornit na ně a mít možnost je zakázat	ANO	[redacted]
FW NG musí umožňovat tvorbu plnohodnotných, uživatelsky definovaných aplikací bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele. Tyto uživatelsky definované aplikace nejsou omezeny na specifický protokol (např. HTTP, HTTPS)	ANO	[redacted]
FW NG podporuje logování přenesených souborů aplikacemi v upload/download směru	ANO	[redacted]
FW NG podporuje blokace přenesených souborů aplikacemi v upload/download směru	ANO	[redacted]
Kontrola na základě uživatelských identit	**Splnění ANO/NE**	**Komentář ke způsobu plnění požadavku (pokud je relevantní)**
FW NG musí podporovat vytváření bezpečnostních pravidel na základě uživatelských identit	ANO	[redacted]
Uživatelská identita, nebo uživatelská skupina, do které uživatelé patří je jedním "match" kritériem při policy lookup společně s a aplikací a případně source/destination IP	ANO	[redacted]
Identitu je možno přidat do pravidla jako jednotlivý uživatel, nebo jako skupina uživatelů vytvořená staticky na FW NG, nebo získaná ze všech následujících externích adresářových služeb: - On-Premise AD - Azure AD	ANO	[redacted]
FW NG podporuje získávání vazby IP adresa-uživatelské jméno bez nutnosti instalace klienta na koncové zařízení	ANO	[redacted]
FW NG podporuje získávání vazby IP adresa-uživatelské jméno bez nutnosti instalace klienta na doménový kontroler	ANO	[redacted]
FW NG musí podporovat získávání vazby IP adresa a uživatelské jméno bez nutnosti instalace dalších komponent mimo samotné HW appliance	ANO	[redacted]
FW NG musí podporovat získávání vazby IP adresa a uživatelské jméno z VPN agenta	ANO	[redacted]
FW NG musí umožňovat automaticky přesun uživatele do jiné skupiny na základě bezpečnostního incidentu vztahujícímu se k danému uživateli, bez nutnosti manuální intervence, např. pomocí API	ANO	[redacted]
Bezpečnostní funkcionality	**Splnění ANO/NE**	**Komentář ke způsobu plnění požadavku (pokud je relevantní)**
FW NG disponuje Intrusion detection and prevention a databáze IPS signatur je uložena přímo ve FW NG a pravidelně aktualizována výrobce po celou dobu životního cyklu zařízení	ANO	[redacted]
Aplikace IPS profilu lze nastavit granulárně na úrovni bezpečnostní politiky	ANO	[redacted]

FW NG umožňuje tvorbu uživatelsky definovaných IPS signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	ANO	[redacted]
FW NG disponuje systémem ochrany proti virům a škodlivého kódu, databáze AV signatur je uložena přímo ve FW NG a pravidelně aktualizována výrobce po celou dobu životního cyklu zařízení	ANO	[redacted]
Aplikace AV profilu lze nastavit granulárně na úrovni bezpečnostní politiky	ANO	[redacted]
Antivirus je schopen kontrolovat provoz v minimálně těchto aplikacích: SMTP, POP3, IMAP, HTTP, HTTPS, HTTP/2, FTP a SMB	ANO	[redacted]
FW NG podporuje v bezpečnostních pravidlech použití externích dynamických seznamů	ANO	[redacted]
FW NG musí umožňovat tvorbu uživatelsky definovaných IPS signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	ANO	[redacted]
FW NG musí obsahovat integrovaný systém ochrany proti přítomnosti virů a škodlivého kódu. Databáze AV signatur musí být uložena přímo v FW NG. Aplikace AV profilu musí být granulární, na úrovni bezpečnostního pravidla	ANO	[redacted]
FW NG musí umožňovat tvorbu uživatelsky definovaných spyware signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	ANO	[redacted]
FW NG musí podporovat možnost zablokování útoku využívajícího známá C&C centra i v případě, že je provoz šifrován a není možné provádět SSL dekrypci	ANO	[redacted]
FW NG musí poskytovat funkci k ochraně proti tzv. drive-by downloadům; způsob ochrany musí být pro uživatele interaktivní s možností volby akceptace rizika a stažení souboru	ANO	[redacted]
FW NG musí obsahovat nativní službu pro ochranu proti útoku typu DoS pomocí limitace počtu spojení na úrovni zdrojová a cílová IP adresa a uživatelská identita	ANO	[redacted]
Lokální management zařízení	**Splnění ANO/NE**	**Komentář ke způsobu plnění požadavku (pokud je relevantní)**
Jednotlivé FW NG musí obsahovat plnohodnotné grafické rozhraní (GUI) pro správu síťových a bezpečnostních funkcí bez nutnosti používání centrálního management serveru. Připojení ke GUI musí podporovat šifrování	ANO	[redacted]
Jednotlivé FW NG musí obsahovat plnohodnotné textové rozhraní (CLI) pro správu a čtení logových záznamů bez nutnosti používání centrálního management serveru. Vzdálené připojení k CLI musí podporovat šifrování	ANO	[redacted]
GUI obsahuje offline kontextovou nápovědu	ANO	[redacted]
CLI rozhraní umožňuje zobrazení konfigurace ve formátu, který je možné mírně upravit a následně dávkově vložit pro replikaci části konfigurace (např. hromadné vytvoření objektů, statických route apod.)	ANO	[redacted]
GUI musí podporovat čtení a vyhledávání v logových záznamech bez nutnosti používání centrálního management serveru	ANO	[redacted]
FW NG podporuje pro autentizaci a autorizaci administrátorů protokoly LDAP, Radius, SAML a osobní certifikát	ANO	[redacted]
FW NG podporuje Multi-factor Authentication pro dodatečnou autentizaci administrátorů do management rozhraní	ANO	[redacted]
Možnost vlastní definice administrátorských rolí a možnost omezování přístupů do jednotlivých částí konfigurace	ANO	[redacted]
FW NG disponuje nástrojem pro odchycení provozu pro analýzu (Packet capture)	ANO	[redacted]
Nástroj pro odchycení provozu musí být schopen odchytit provoz jak na datových, tak na OOB management interfacech	ANO	[redacted]
Nástroj pro odchycení provozu musí být schopen odchytit provoz jak na vstupním, tak na výstupním interface a porovnáním času zjistit latenci daného paketu	ANO	[redacted]
FW NG musí obsahovat nativní nástroje pro debugging problémových situací v úrovni L2 – L7 ISO/OSI modelu	ANO	[redacted]
Jednotlivé HW appliance musí obsahovat plnohodnotné API rozhraní pro čtení a konfiguraci síťových nastavení, bezpečnostních a dalších pravidel, nastavení síťových rozhraní a směrování.	ANO	[redacted]
API musí být důkladně popsáno ve veřejně přístupné dokumentaci	ANO	[redacted]
FW NG musí být možné spravovat z administrátorských stanic s OS Windows, Linux a MacOS X (včetně HW s čipem Apple Silicon)	ANO	Z webového rozhraní
FW NG management musí podporovat práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem	ANO	[redacted]
FW NG musí podporovat kontrolu čtyř očí tak, že jeden administrátor připraví změny a druhý je následně schválí a aplikuje	ANO	[redacted]
Logování	ANO	
FW NG musí obsahovat lokální úložiště logů	ANO	[redacted]

FW NG musí obsahovat nástroj pro analýzu logů bez nutnosti využití dalšího systému mimo GUI	ANO	[redacted]
FW NG musí podporovat agregované zobrazení logů na základě jednoho filtrovacího pravidla, napříč jednotlivými typy logů, jako jsou provozní logy, logy bezpečnostních incidentů a logy přístupů na URL	ANO	[redacted]
FW NG musí podporovat přeposílání logů na zařízení třetích stran, minimálně SysLog ve formátu CEF	ANO	[redacted]
FW NG musí umožňovat výběr přeposílaných logů na úrovni bezpečnostního pravidla, tedy nastavit, která bezpečnostní pravidla mají logovat a která ne	ANO	[redacted]
FW NG musí mít možnost detailně definovat, které typy logů jsou zasílány, do jakých cílových lokací (email, SNMP Trap, SysLog atd.)	ANO	[redacted]

Požadavky na Firewally NG typ A	Splnění ANO/NE	Komentář ke způsobu plnění požadavku (pokud je relevantní)
Výrobce a model nabízeného produktu:		[redacted]
P/N a další specifikace nabízeného produktu:		[redacted]
Minimální počet portů 10Gbit SFP+ - 6 portů	ANO	1G/10G SFP/SFP+ (10)
Minimální počet portů 25Gbit SFP28 - 4 porty	ANO	25G SFP28 (4)
Minimální počet portů 100Gbit QSFP28 - 2 porty	ANO	40G/100G QSFP/QSFP28 (2)
Požadovaná propustnost v režimu FW NG (zapnutá aplikační kontrola bez kontroly IPS, AV apod.) je minimálně 20 Gbps.	ANO	29 Gbps
Požadovaná propustnost v režimu Threat Protection (zapnutá aplikační kontrola a všechny požadované bezpečnostní funkce, včetně všech signaturových ochran) je minimálně 15 Gbps	ANO	15 Gbps
Minimální počet souběžných spojení musí dosahovat hodnoty alespoň 2 000 000	ANO	2.5M
Minimální počet nových spojení za sekundu musí dosahovat hodnoty alespoň 200 000	ANO	240000
FW NG umožňuje vytvořit minimálně 10 plnohodnotných virtuálních domén (kontextů)	ANO	11
Jednotlivé virtuální domény musí mít možnost sdílet jeden interface bez nutnosti vyčerpat na tuto funkci jeden z požadovaných 10 virtuálních kontextů. Pokud je třeba pro tuto funkci nezbytné použít separátní kontext, je vyžadováno navýšení počtu dodaných kontextů na 11.	ANO	11
FW NG musí být schopen ukládat logové údaje na interní SSD disk o velikosti minimálně 400 GB	ANO	480 GB SSD

Požadavky na Firewally NG typ B	Splnění ANO/NE	Komentář ke způsobu plnění požadavku (pokud je relevantní)
Výrobce a model nabízeného produktu:		[redacted]
P/N a další specifikace nabízeného produktu:		[redacted]
Minimální počet portů 1Gbit RJ45 - 6 portů	ANO	10/100/1000 (4)
Minimální počet portů 10Gbit SFP+ - 6 portů	ANO	1G/10G SFP/SFP+ (8)
Požadovaná propustnost v režimu FW NG (zapnutá aplikační kontrola bez kontroly IPS, AV apod.) je minimálně 9 Gbps.	ANO	9.5 Gbps
Požadovaná propustnost v režimu Threat Protection (zapnutá aplikační kontrola a všechny požadované bezpečnostní funkce, včetně všech signaturových ochran) je minimálně 4,5 Gbps	ANO	5.8 Gbps
Minimální počet souběžných spojení musí dosahovat hodnoty alespoň 1 000 000	ANO	1.4M
Minimální počet nových spojení za sekundu musí dosahovat hodnoty alespoň 100 000	ANO	140000
FW NG umožňuje vytvořit minimálně 5 plnohodnotných virtuálních domén (kontextů)	ANO	6
Jednotlivé virtuální domény musí mít možnost sdílet jeden interface bez nutnosti vyčerpat na tuto funkci jeden z požadovaných 5 virtuálních kontextů. Pokud je třeba pro tuto funkci nezbytné použít separátní kontext, je vyžadováno navýšení počtu dodaných kontextů na 6.	ANO	6
FW NG musí být schopen ukládat logové údaje na interní SSD disk o velikosti minimálně 200 GB	ANO	240 GB SSD

Požadavky na Firewally NG typ C	Splnění ANO/NE	Komentář ke způsobu plnění požadavku (pokud je relevantní)
Výrobce a model nabízeného produktu:		[redacted]
P/N a další specifikace nabízeného produktu:		[redacted]
Minimální počet portů 1Gbit RJ45 - 6 portů (celkem)	ANO	8
Minimální počet portů 1Gbit SFP - 2 porty (mohou být kombinované RJ45/SFP z celkových 6 portů minimálně)	ANO	2
Požadovaná propustnost v režimu FW NG (zapnutá aplikační kontrola bez kontroly IPS, AV apod.) je minimálně 3 Gbps.	ANO	3.6 Gbps
Požadovaná propustnost v režimu Threat Protection (zapnutá aplikační kontrola a všechny požadované bezpečnostní funkce, včetně všech signaturových ochran) je minimálně 1,5 Gbps	ANO	2.3 Gbps
Minimální počet souběžných spojení musí dosahovat hodnoty alespoň 250 000	ANO	300000
Minimální počet nových spojení za sekundu musí dosahovat hodnoty alespoň 25 000	ANO	56000
FW NG umožňuje vytvořit minimálně 3 plnohodnotné virtuální domény (kontexty)	ANO	5
Jednotlivé virtuální domény musí mít možnost sdílet jeden interface bez nutnosti vyčerpat na tuto funkci jeden z požadovaných 3 virtuálních kontextů. Pokud je třeba pro tuto funkci nezbytné použít separátní kontext, je vyžadováno navýšení počtu dodaných kontextů na 4.	ANO	5
FW NG musí být schopen ukládat logové údaje na interní SSD disk o velikosti minimálně 100 GB	ANO	128 GB

Role - Technik pro Firewally NG úrovně L1	Splnění ANO/NE	Komentář ke způsobu plnění požadavku (pokud je relevantní)
Minimálně 3 roky praxe v oboru IT Network Operations/Security Operations na pozici Network Engineer / Security Engineer	ANO	3+
Praxe na pozici Network Engineer / Security Engineer u minimálně jedné významné zakázky s cenou min. 3.000.000,00 Kč bez DPH	ANO	viz soubor Příloha č. 2. Formulář k prokázání kvalifikace - VZFW2024-F222L1.pdf
Existence pracovního nebo obdobného poměru u dodavatele, příp. poddodavatele, nebo, je-li fyzickou osobou podnikající, smluvního vztahu s dodavatelem	ANO	Zaměstnanec
Certifikace výrobce pro administraci, implementaci a podporu Firewallů NG výrobce nabídnutého řešení	ANO	[redacted]
Počáteční úroveň technické podpory, která je odpovědná za řešení běžných provozních požadavků a problémů	ANO	L1

Role - Technik pro Firewally NG úrovně L2	Splnění ANO/NE	Komentář ke způsobu plnění požadavku (pokud je relevantní)
Minimálně 5 let praxe v oboru IT Network Operations / Security Operations na pozici Network Engineer / Security Engineer	ANO	5+
Praxe na pozici Network Engineer / Security Engineer u minimálně jedné významné zakázky s cenou min. 5.000.000,00 Kč bez DPH	ANO	viz soubor Příloha č. 2. Formulář k prokázání kvalifikace - VZFW2024-F222L2.pdf
Existence pracovního nebo obdobného poměru u dodavatele, příp. poddodavatele, nebo, je-li fyzickou osobou podnikající, smluvního vztahu s dodavatelem	ANO	Zaměstnanec
Certifikace výrobce pro administraci, implementaci a podporu Firewallů NG výrobce daného řešení	ANO	[redacted]
Pokročilá úroveň technické podpory, která je odpovědná za řešení pokročilejší správy a provádění topologických změn v konfiguraci celého řešení	ANO	L1, L2

Role - Technik pro Firewally NG úrovně L3	Splnění ANO/NE	Komentář ke způsobu plnění požadavku (pokud je relevantní)
Minimálně 7 let praxe v oboru IT Network Operations/Security Operations na pozici Security Architekt	ANO	7+
Praxe na pozici Security Architekt, u minimálně jedné významné zakázky s cenou min. 10.000.000,00 Kč bez DPH, jejímž předmětem byla Dodávka, implementace a podpora Firewallů NG	ANO	viz soubor Příloha č. 2. Formulář k prokázání kvalifikace - VZFW2024-F222L3.pdf
Existence pracovního nebo obdobného poměru u dodavatele, příp. poddodavatele, nebo, je-li fyzickou osobou podnikající, smluvního vztahu s dodavatelem	ANO	Zaměstnanec
Certifikace výrobce pro návrh architektury a implementaci Firewallů NG výrobce daného řešení	ANO	[redacted]
Nejvyšší úroveň technické podpory, která je odpovědná za návrh architektury, řešení a diagnostiku technických problémů, komunikaci s výrobcem řešení	ANO	L1, L2, L3

Role - Projektový manažer / Team Leader	Splnění ANO/NE	Komentář ke způsobu plnění požadavku (pokud je relevantní)
Minimálně 3 roky praxe v oboru IT Operations / Security Operations na pozici Projektový manager / Delivery manager	ANO	3+
Praxe na pozici Projektový manager / Delivery manager u minimálně jedné významné zakázky, jejímž předmětem bylo Dodávka, implementace a služby v oblasti IT/Security	ANO	viz soubor Příloha č. 2. Formulář k prokázání kvalifikace - VZFW2024-F222PM.pdf
Existence pracovního nebo obdobného poměru u dodavatele, příp. poddodavatele, nebo, je-li fyzickou osobou podnikající, smluvního vztahu s dodavatelem	ANO	[redacted] zaměstnanec poddodavatele

Jednotkový ceník

Položka	Jednotka	Cena v Kč bez DPH
Centrální management	kpl	[redacted]
Firewall NG typ A	kpl	[redacted]
Firewall NG typ B	kpl	[redacted]
Firewall NG typ C	kpl	[redacted]
Optický modul QSFP28 100GBase-IR4 plně kompatibilní s Firewally NG	ks	[redacted]
Optický modul SFP28 25GBase-LR plně kompatibilní s Firewally NG	ks	[redacted]
Optický modul SFP28 25GBase-SR plně kompatibilní s Firewally NG	ks	[redacted]
Optický modul SFP+ 10GBase-LR plně kompatibilní s Firewally NG	ks	[redacted]
Optický modul SFP+ 10GBase-SR plně kompatibilní s Firewally NG	ks	[redacted]
Optický modul SFP 1GBase-LR plně kompatibilní s Firewally NG	ks	[redacted]
Optický modul SFP 1GBase-SR plně kompatibilní s Firewally NG	ks	[redacted]
Role - Technik pro Firewally NG úrovně L1	MD	[redacted]
Role - Technik pro Firewally NG úrovně L2	MD	[redacted]
Role - Technik pro Firewally NG úrovně L3	MD	[redacted]
Role - Projektový manažer / Team Leader	MD	[redacted]
Dopravné/Cestovné po ČR	km	[redacted]

Předpokládaný model čerpání

Položka	Počet	Jednotka	Cena v Kč bez DPH	Cena celkem v Kč bez DPH
Centrální management	2	kpl	[redacted]	[redacted]
Firewall NG typ A	4	kpl	[redacted]	[redacted]
Firewall NG typ B	10	kpl	[redacted]	[redacted]
Firewall NG typ C	15	kpl	[redacted]	[redacted]
Optický modul QSFP28 100GBase-IR4 plně kompatibilní s Firewally NG	8	ks	[redacted]	[redacted]
Optický modul SFP28 25GBase-LR plně kompatibilní s Firewally NG	8	ks	[redacted]	[redacted]
Optický modul SFP28 25GBase-SR plně kompatibilní s Firewally NG	8	ks	[redacted]	[redacted]
Optický modul SFP+ 10GBase-LR plně kompatibilní s Firewally NG	20	ks	[redacted]	[redacted]
Optický modul SFP+ 10GBase-SR plně kompatibilní s Firewally NG	20	ks	[redacted]	[redacted]
Optický modul SFP 1GBase-LR plně kompatibilní s Firewally NG	30	ks	[redacted]	[redacted]
Optický modul SFP 1GBase-SR plně kompatibilní s Firewally NG	30	ks	[redacted]	[redacted]
Role - Technik pro Firewally NG úrovně L1	250	MD	[redacted]	[redacted]
Role - Technik pro Firewally NG úrovně L2	200	MD	[redacted]	[redacted]
Role - Technik pro Firewally NG úrovně L3	100	MD	[redacted]	[redacted]
Role - Projektový manažer / Team Leader	100	MD	[redacted]	[redacted]
Dopravné/Cestovné po ČR	1	km	[redacted]	[redacted]
CELKEM				**38 451 313,60 Kč**

[redacted]

[redacted]