Příloha č.1	Minimální požadavek na funkcionalitu	Upřesnit požadavek	Účastník doplní ANO/NE nebo nabízené parametry
Obecné, HW a výkonové požadavky		Praha, budova SFDI	
• Požadujeme platformu postavenou na HW akcelerované architektuře (tj. zařízení vybavené kombinací CPU + specializované obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekrypce, porovnávání se signaturovou databází, …) • Celá dodávka musí obsahovat všechny HW komponenty a licence na dobu 3 let. Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány. • Požadujeme dodání zařízení ve formátu HW appliance o velikosti 1RU • Požadujeme veškeré příslušenství (montážní prvky) pro montáž do RACKu • Možnost rozšíření platformy i další prvek typu NGFW jehož cílem bude zajišťování sdílení telemetrických informací, vizualizace stavu sítě, zařízení a klientů, přičemž cele řešení musí být podporováno výrobcem. • Možnost o rozšíření platformy pro sběr logů a grafického reportingu včetně oboustranné komunikace (tím se rozumí minimálně odeslání a zpětné načítání logů pro účel vizualizace), přičemž zde musí existovat garantovaná podpora funkcionality.	**Pro tuto lokalitu požadujeme dvě identická zařízení pracující společně v HA módu a jednotlivě splňující veškeré minimální uvedené požadavky.**	ANO
Počet síťových rozhraní, RJ45 10/100/1000		16	ANO
Počet GE SFP		8	ANO
Počet 10 GE SFP		4	ANO
• Konzolový port pro management • Dedikovaný port RJ45 pro management • Dedikovaný port RJ45 pro HA konfiguraci • USB 3.0 port pro zálohu konfigurace, případně pro připojení USB 4G modemu • Redundantní napájecí zdroj		-	ANO
• Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B- min 26000 Mbps, 26000 Mbps, 10000 Mbps • Latence firewallu (64 B UDP paket) - max 5 mikro sec • Počet naráz otevřených spojení – min 2,7 M • Počet nových spojení za sekundu - min. 260 000 • Počet firewall pravidel až 10 000 • Podpora virtualizace (min 10 virtuálních kontextů) • Podpora funkce bezdrátový kontrolér - 128 AP • Podpora funkce integrovaný switch controller – podpora až 64 switchů		-	ANO
Funkce		Praha, budova SFDI	
Networking a High Availibility • Podpora režimu vysoké dostupnosti, L2, Active Active, Active Passive, full mesh HA, VRRP, synchronizace stavové tabulky a IPsec SAs mezi nódy v clusteru • Režim fungování L2 – transparentní režim, L3 – NAT/Router • Podpora VLAN • Podopora multicast, vytváření politiky pro multicast routování • Podpora 802.3ad link aggregation • Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offloading • Podpora centrální NATovácí tabulky, stavová inspekce SCTP komunikace • Podpora dynamických routovacích protokolů BGP, OSPF, ISIS, RIP • Policy-based routing • Funkce SD WAN – možnost rozkládání provozu mezi více linek na základě aplikačních signatur, IP adres a portů u známých aplikací, kvality linky včetně automatické detekce nefunkčnosti linky		-	ANO
VPN • Funkce SSL VPN o Podpora klientského i bezklientského (portálového) režimu o Minimální počet současně navázaných SSL VPN tunelů: 450 o Minimální propustnost SSL VPN: 1900Mbps • Funkce IPSEC VPN o podpora site-to-site VPN o podpora klientských VPN o dostupnost VPN klienta pro koncové stanice (Windows, MacOS) o funkce klientských IPSec VPN nesmí být licencovaná na počet uživatel. V opačném případě požadujeme dodání neomezené licence. o Minimální počet IPSEC VPN tunelů typu lokalita-lokalita: 2300 o Minimální počet klientských IPSEC VPN tunelů: 15000 o propustnost IPSec VPN min. 12,5 Gbps (měřeno při AES256-SHA256) o podpora konfigurace redundatních IPSec VPN tunelů za pomoci statického směrování o podpora konfigurace redundatních IPSec VPN tunelů za pomoci dynamického směrování o podpora funkce dynamického navazování IPsec tunelů dle potřeby komunikace • Podpora VXLAN • Podpora L2TP, PPTP, GRE • podpora dynamických routovací protokolů OSPF, BGP ve VPN IPsec		-	ANO

UTM • Funkce detekce aplikací na L7 (Application Control) o Detekce známých aplikací na základě signatur o Signaturový database automaticky aktualizované výrobcem o alespoň 4000 podporovaných aplikací o pro populárná cloudové aplikace (minimálně Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) požadujeme pokročilé akce typu blokování upload/download souborů, blokování her v rámci aplikace, blokování login, atd. (relevantní k dané aplikaci) o možnost tvorby vlastních signatur o detekované aplikace je možné: povolit, monitorovat, blokovat o na základě typu aplikace musí být možné omezit šířku pásma pro danou aplikaci o funkce AppCtr se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. Alternativně požadujeme možnost využití v rámci tzv. NGFW pravidel popsaných výše. • Funkce detekce a potlačení narušení (IPS/IDS) o signatury automaticky aktualizované výrobcem o alespoň 11.000 rozpoznávaných hrozeb (signatur) definovaných výrobcem o možnost tvorby vlastních signatur o funkce IPS se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům o propustnost funkce IPS včetně logování min. 4800Mbps (měřeno na komunikaci typu mix aplikací) • Funkce antivirové kontroly o Ochrana před škodlivým kódem (malware, trojské koně, atp.), včetně ochrany před polymorfním kódem o Signatury automaticky aktualizované výrobcem o požadujeme AV kontrolu rozšířenou o inspekci tzv. sandbox technikou, poskytovanou formou služby dodávané výrobcem FW (licence musí být součástí dodávky) o možnost rozšíření o inspekci tzv. sandbox technikou formou lokálné HW appliance stejného výrobce o deklarovaná propustnost AV kontroly, v kombinaci s IPS, Application Control a zapnutým logováním min. 2900 Mbps o funkce AV kontroly se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. o Podpora služby výrobce, která umožnǐ detekovat malware, který byl objevený v době od poslednǐ aktualizace AV signaturové databáze pomocí globálnǐ a rychle se aktualizujícǐ databáze hashů o Funkce odstraněnǐ aktivního obsahu z dokumentů kancelářských aplikací – AV engine na firewallu/bezpečnostnǐ emailové bráně v reálném čase odstraní aktivní obsah z dokumentu, Dokument zůstává v původním formátu, jsou z něj odstraněny všechny aktivní prvky. Upravený dokument jde k původnímu příjemci, originální dokument se odešle do Sandboxu. • Funkce kategorizace webových stránek o založená na centrálně spravované databázi výrobce o minimálně 50 filtračních kategorií o možnost definice vlastních kategorií o možnost definice vlastních seznamů zakázaných URL o kategorizace musí zahrnovat I české a slovenské internetové stránky • Funkce DNS filtru o Možnost blokovat DNS dotazy na základě příslušnosti k URL kategorii (obdobné kategorie jako u předchozího bodu) o Možnost definovat vlastní tzv. blacklist domén o Možnost přesměrovat komunikace se zakázanými doménami na vlastní portal/URL o Možnost importu seznamu blokovaných domén do DNS filtru o Detekce a blokování komunikace do botnet sítí • Funkce ochrany před únikem citlivých informací (DLP) o možností analýzy běžných typů dokumentů a protokolů o možnost definice pravidel min. na základě regulárních výrazů, watermarkovacího nástroje a typu kontroly typu file checksum • Email filter – jednoduchá antispamová a antivirová inspekce elektronické pošty		ANO - ANO
• Možnost nastavovat firewall politiku na základě geografických údajů • Aplikace firewall policy na známé internetové služby, kde databáze těchto služeb je pravidelně aktualizována výrobcem • Možnost snadné integrace cloudové služby. Minimálně na: MS Azure, Amazon Web Services, Google Cloud • Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru • Viditelnost do provozu na aplikační úrovni • 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 application control, nikoliv pouhý TCP/UDP port) resp. kategorie URL filteringu (nikoliv jako AppCtrl resp URL filtering profil aplikovaný na dané pravidlo). • Ověřování uživatelů LDAP, Active Directory, Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu • Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření. • Traffic Shaping, QoS s podporou priroritizace provozu na základě DSCP markování a ToS, aplikace traffic shaping na konkrétní aplikaci nebo webovou kategorii • Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu • Podpora funkce reverzní proxy • Podpora silné autentizace uživatelů – integrovaná podpora generátor jednorázových hesel (OTP) – pro		ANO

• Podpora silné autentizace uživatelů – integrovaná podpora generátor jednorázových hesel (OTP) – pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů • Explicit proxy o podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl, DLP) o podpora transparentního ověřování uživatel proti MS AD protokolem Kerberos o funkce transparentní proxy, kdy dochází k automatickému přesměrování provozu na proxy server bez nutnosti konfigurovat klienta o Funkce transparentního ověřování uživatelů pomocí domény (MS Active Directory) včetně podpory autentizace uživatel na terminálovém serveru Integrovaný controller bezdrátových (Wifi) sítí • Wifi controller integrovaný do NGFW platformy • Každá bezdrátová síť (SSID) bude reprezentována virtuálním síťovým rozhraním • podpora bezpečnostních profilů (AV, AppControl, Webfilter, DLP) přímo na wifi controlleru • podpora SSL dekrypce uživatelského provozu přímo na wifi controlleru • Podpora wifi přístupových bodů stejného výrobce s výrobcem FW řešení • Možnost volby z různých modelů (např. 802.11abgn, 802.11ac, 802.11ac wave2, indoor, outdoor) • On-wire rogue AP detekce a mitigace • Podpora fast-roamingu (802.11 k,v,r) • podpora více PSK u jednoho SSID • podpora IPSEC tunelu pro šifrování data plane (uživatelských dat) • podpora WPA3 šifrování • podpora WiFi 6 standardu • podpora BSS coloring (WiFi 6) • podpora diagnostických WiFi nástrojů, například pro analýzu spektra	-	ANO
Virtualiazce • Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext musí být plnohodnotné řešení včetně odděleného GUI, management účtů, atp. • Součástí dodávky musí být licence na min. 10 virtuálních kontextů (včetně licence na kompletní podporu požadovaných bezpečnostních funkcí v těchto virtuálních kontextech) • Každý virtuální kontext je zároveň samostatným wifi controllerem • Podporou izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů)	-	ANO
Management • FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici • Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě • Podpora otevřeného API (možnost integrace vybraných funkcí do stávající management infrastruktury)	-	ANO

Instalace a nastavení		**Doplní účastník ANO/NE nebo nabízené parametry**
Součástí předmětu plnění bude instalace a nastavení všech dodaných zařízení, SW a podpis akceptačního protokolu. Požadavky na instalaci a nastavení jsou specifikovány na samostatném listu tohoto dokumentu (list Implementace)	-	ANO

Minimální požadavek na funkcionalitu	Upřesnit požadavek	Účastník doplní ANO/NE nebo nabízené parametry
Obecné, HW a výkonové požadavky	Datacentrum	
• Požadujeme platformu postavenou na HW akcelerované architektuře (tj. zařízení vybavené kombinací CPU + specializované obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekrypce, porovnávání se signaturovou databází, …) • Celá dodávka musí obsahovat všechny HW komponenty a licence na dobu 3 let. Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány. • Požadujeme dodání zařízení ve formátu HW appliance o velikosti 1RU • Požadujeme veškeré příslušenství (montážní prvky) pro montáž do RACKu • Možnost rozšíření platformy i další prvek typu NGFW jehož cílem bude zajišťování sdílení telemetrických informací, vizualizace stavu sítě, zařízení a klientů, přičemž cele řešení musí být podporováno výrobcem. • Možnost o rozšíření platformy pro sběr logů a grafického reportingu včetně oboustranné komunikace	**Pro tuto lokalitu požadujeme dvě identická zařízení pracující společně v HA módu a jednotlivě splňující veškeré minimální uvedené požadavky.**	ANO
Počet síťových rozhraní, RJ45 10/100/1000	16	ANO
Počet GE SFP	4	ANO
Počet 10 GE SFP	2	ANO
• Konzolový port pro management • Dedikovaný port RJ45 pro management • Dedikovaný port RJ45 pro HA konfiguraci • USB 3.0 port pro zálohu konfigurace, případně pro připojení USB 4G modemu • Redundantní napájecí zdroj	-	ANO
• Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B- min 18000 Mbps, 16000 Mbps, 9000 Mbps • Latence firewallu (64 B UDP paket) - max 7 mikro sec • Výkon firewall – 14000000 paketů / s • Počet naráz otevřených spojení – min 1.3 M • Počet nových spojení za sekundu - min. 52 000 • Počet firewall pravidel až 10 000 • Podpora virtualizace (min 10 virtuálních kontextů) • Podpora funkce bezdrátový kontrolér - 64 AP • Podpora funkce integrovaný switch controller – podpora až 24 switchů	-	ANO
Funkce	Datacentrum	
Networking a High Availibility • Podpora režimu vysoké dostupnosti, L2, Active Active, Active Passive, full mesh HA, VRRP, synchronizace stavové tabulky a IPsec SAs mezi nódy v clusteru • Režim fungování L2 – transparentní režim, L3 – NAT/Router • Podpora VLAN • Podopora multicast, vytváření politiky pro multicast routování • Podpora 802.3ad link aggregation • Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offloading • Podpora centrální NATovácí tabulky, stavová inspekce SCTP komunikace • Podpora dynamických routovacích protokolů BGP, OSPF, ISIS, RIP • Policy-based routing • Funkce SD WAN – možnost rozkládání provozu mezi více linek na základě aplikačních signatur, IP adres a portů u známých aplikací, kvality linky včetně automatické detekce nefunkčnosti linky	-	ANO
VPN • Funkce SSL VPN o Podpora klientského i bezklientského (portálového) režimu o Minimální počet současně navázaných SSL VPN tunelů: 450 o Minimální propustnost SSL VPN: 900Mbps • Funkce IPSEC VPN o podpora site-to-site VPN o podpora klientských VPN o dostupnost VPN klienta pro koncové stanice (Windows, MacOS) o funkce klientských IPSec VPN nesmí být licencovaná na počet uživatel. V opačném případě požadujeme dodání neomezené licence. o Minimální počet IPSEC VPN tunelů typu lokalita-lokalita: 2300 o Minimální počet klientských IPSEC VPN tunelů: 15000 o propustnost IPSec VPN min. 11Gbps (měřeno při AES256-SHA256) o podpora konfigurace redundatních IPSec VPN tunelů za pomoci statického směrování o podpora konfigurace redundatních IPSec VPN tunelů za pomoci dynamického směrování o podpora funkce dynamického navazování IPsec tunelů dle potřeby komunikace • Podpora VXLAN • Podpora L2TP, PPTP, GRE • podpora dynamických routovací protokolů OSPF, BGP ve VPN IPsec	-	ANO

UTM • Funkce detekce aplikací na L7 (Application Control) o Detekce známých aplikací na základě signatur o Signaturový database automaticky aktualizované výrobcem o alespoň 4000 podporovaných aplikací o pro populárná cloudové aplikace (minimálně Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) požadujeme pokročilé akce typu blokování upload/download souborů, blokování her v rámci aplikace, blokování login, atd. (relevantní k dané aplikaci) o možnost tvorby vlastních signatur o detekované aplikace je možné: povolit, monitorovat, blokovat o na základě typu aplikace musí být možné omezit šířku pásma pro danou aplikaci o funkce AppCtr se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. Alternativně požadujeme možnost využití v rámci tzv. NGFW pravidel popsaných výše. • Funkce detekce a potlačení narušení (IPS/IDS) o signatury automaticky aktualizované výrobcem o alespoň 11.000 rozpoznávaných hrozeb (signatur) definovaných výrobcem o možnost tvorby vlastních signatur o funkce IPS se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům o propustnost funkce IPS včetně logování min. 2500Mbps (měřeno na komunikaci typu mix aplikací) • Funkce antivirové kontroly o Ochrana před škodlivým kódem (malware, trojské koně, atp.), včetně ochrany před polymorfním kódem o Signatury automaticky aktualizované výrobcem o požadujeme AV kontrolu rozšířenou o inspekci tzv. sandbox technikou, poskytovanou formou služby dodávané výrobcem FW (licence musí být součástí dodávky) o možnost rozšíření o inspekci tzv. sandbox technikou formou lokálné HW appliance stejného výrobce o deklarovaná propustnost AV kontroly, v kombinaci s IPS, Application Control a zapnutým logováním min. 900 Mbps o funkce AV kontroly se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. o Podpora služby výrobce, která umožní detekovat malware, který byl objevený v době od poslední aktualizace AV signaturové databáze pomocí globální a rychle se aktualizující databáze hashů o Funkce odstranění aktivního obsahu z dokumentů kancelářských aplikací – AV engine na firewallu/bezpečnostní emailové bráně v reálném čase odstraní aktivní obsah z dokumentu, Dokument zůstává v původním formátu, jsou z něj odstraněny všechny aktivní prvky. Upravený dokument jde k původnímu příjemci, originální dokument se odešle do Sandboxu. • Funkce kategorizace webových stránek o založená na centrálně spravované databázi výrobce o minimálně 50 filtračních kategorií o možnost definice vlastních kategorií o možnost definice vlastních seznamů zakázaných URL o kategorizace musí zahrnovat I české a slovenské internetové stránky • Funkce DNS filtru o Možnost blokovat DNS dotazy na základě příslušnosti k URL kategorii (obdobné kategorie jako u předchozího bodu) o Možnost definovat vlastní tzv. blacklist domén o Možnost přesměrovat komunikace se zakázanými doménami na vlastní portal/URL o Možnost importu seznamu blokovaných domén do DNS filtru o Detekce a blokování komunikace do botnet sítí • Funkce ochrany před únikem citlivých informací (DLP) o možností analýzy běžných typů dokumentů a protokolů o možnost definice pravidel min. na základě regulárních výrazů, watermarkovacího nástroje a typu kontroly typu file checksum	-	ANO
Firewall • Možnost nastavovat firewall politiku na základě geografických údajů • Aplikace firewall policy na známé internetové služby, kde databáze těchto služeb je pravidelně aktualizována výrobcem • Možnost snadné integrace cloudové služby. Minimálně na: MS Azure, Amazon Web Services, Google Cloud • Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru • Viditelnost do provozu na aplikační úrovni • 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 application control, nikoliv pouhý TCP/UDP port) resp. kategorie URL filteringu (nikoliv jako AppCtrl resp URL filtering profil aplikovaný na dané pravidlo). • Ověřování uživatelů LDAP, Active Directory, Single Sign On, Radius, TACACS+, Ověřování na základě		

certifikátu • Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření. • Traffic Shaping, QoS s podporou priroritizace provozu na základě DSCP markování a ToS, aplikace traffic shaping na konkrétní aplikaci nebo webovou kategorii • Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu • Podpora funkce reverzní proxy • Podpora silné autentizace uživatelů – integrovaná podpora generátor jednorázových hesel (OTP) – pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů • Explicit proxy o podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl, DLP) o podpora transparentního ověřování uživatel proti MS AD protokolem Kerberos o funkce transparentní proxy, kdy dochází k automatickému přesměrování provozu na proxy server bez nutnosti konfigurovat klienta o Funkce transparentního ověřování uživatelů pomocí domény (MS Active Directory) včetně podpory autentizace uživatel na terminálovém serveru Integrovaný controller bezdrátových (Wifi) sítí • Wifi controller integrovaný do NGFW platformy • Každá bezdrátová síť (SSID) bude reprezentována virtuálním síťovým rozhraním • podpora bezpečnostních profilů (AV, AppControl, Webfilter, DLP) přímo na wifi controlleru • podpora SSL dekrypce uživatelského provozu přímo na wifi controlleru • Podpora wifi přístupových bodů stejného výrobce s výrobcem FW řešení • Možnost volby z různých modelů (802.11abgn, 802.11ac, 802.11ac wave2, indoor, outdoor) • On-wire rogue AP detekce a mitigace • Podpora fast-roamingu (802.11 k,v,r) • podpora více PSK u jednoho SSID	-	ANO
Virtualiazce • Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext musí být plnohodnotné řešení včetně odděleného GUI, management účtů, atp. • Součástí dodávky musí být licence na min. 10 virtuálních kontextů (včetně licence na kompletní podporu požadovaných bezpečnostních funkcí v těchto virtuálních kontextech) • Každý virtuální kontext je zároveň samostatným wifi controllerem • Podporou izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů)	-	ANO
Management • FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici • Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě • Podpora otevřeného API (možnost integrace vybraných funkcí do stávající management infrastruktury)	-	ANO

Instalace a nastavení		**Doplní účastník ANO/NE nebo nabízené parametry**
Součástí předmětu plnění bude instalace a nastavení všech dodaných zařízení, SW a podpis akceptačního protokolu. Požadavky na instalaci a nastavení jsou specifikovány na samostatném listu tohoto dokumentu (list Implementace)	-	ANO

Minimální požadavek na funkcionalitu	Upřesnit požadavek	Účastník doplní ANO/NE nebo nabízené parametry
Obecné, HW a výkonové požadavky	Pobočky Brno, Ostrava, České Budějovice	
• Požadujeme platformu postavenou na HW akcelerované architektuře (tj. zařízení vybavené kombinací CPU + specializované obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekrypce, akcelerace IPsec VPN, porovnávání se signaturovou databází, …) • Celá dodávka musí obsahovat všechny HW komponenty a licence na dobu 3 let. Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány. • Požadujeme dodání zařízení ve formátu HW appliance • Možnost rozšíření platformy i další prvek typu NGFW jehož cílem bude zajišťování sdílení telemetrických informací, vizualizace stavu sítě, zařízení a klientů, přičemž cele řešení musí být podporováno výrobcem. • Možnost o rozšíření platformy pro sběr logů a grafického reportingu včetně oboustranné komunikace (tím se rozumí minimálně odeslání a zpětné načítání logů pro účel vizualizace), přičemž zde musí existovat garantovaná podpora funkcionality • Součástí dodávky musí být komponenta, jenž umožňuje snadnou instalaci do klasického racku 1-U	**Požadujeme 4 zařízení. Po jednom pro každou lokalitu a další jeden kus s nimi identického zařízení pro testování a záložní provoz.**	ANO
Počet síťových rozhraní, RJ45 10/100/1000	8	ANO
Počet GE SFP	2	ANO
• Dedikovaný konzolový port – min 1x • USB port umožňující připojení USB flash paměti pro zálohování konfigurace, zároveň umožňující připojení USB modemu pro záložní připojení internetu – min 1x • Podpora redundantního napájení	-	ANO
• Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B- min 9000 Mbps, 9000 Mbps, 6000 Mbps • Latence firewallu (64 B UDP paket) - max 5 mikro sec • Počet naráz otevřených spojení – min 1 250 000 • Počet nových spojení za sekundu - min. 40 000 • Počet firewall pravidel až 5 000 • Podpora virtualizace (min 10 virtuálních kontextů) • Podpora funkce bezdrátový kontrolér – min 90 AP • Podpora funkce integrovaný switch controller – podpora min. 12 switchů	-	ANO
Funkce	Pobočky Brno, Ostrava, České Budějovice	
Networking a High Availibility • Podpora režimu vysoké dostupnosti, L2, Active Active, Active Passive, full mesh HA, VRRP, synchronizace stavové tabulky a IPsec SAs mezi nódy v clusteru • HA musí podporovat až 4 nódy v HA režimu • Režim fungování L2 – transparentní režim, L3 – NAT/Router • Podpora VLAN • Podopora multicast, vytváření politiky pro multicast routování • Podpora 802.3ad link aggregation • Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offloading • Podpora centrální NATovácí tabulky, stavová inspekce SCTP komunikace • Podpora dynamických routovacích protokolů BGP, OSPF, ISIS, RIP • Policy-based routing • Podpora uplatňování základních pravidel pro kontrolu na přístupové vrstvě (NAC pravidla, politiky) • Zařízení musí podporovat možnost rozkládání provozu mezi více linek na základě aplikačních signatur, IP adres a portů u známých aplikací, kvality linky včetně automatické detekce nefunkčnosti linky (SD-WAN). • Funkce SD-WAN nesmí být licenčně omezeno. V rámci nabízeného řešení musí být dodáno v podobě, jenž umožňuje neomezené využívání i v případě, že dojde k nárůstu počtů zařízeních komunikující skrze SW-WAN do internetu, tak i v případě, že dojde k navýšení počtu konektivit a jejich rychlosti. • Integrované SD-WAN řešení musí podporovat podle dokumentace výrobce min. 200 členů virtuálního rozhraní, které sdružuje konektivitu a jsou na něj uplatněna pravidla provozu a routingu.	-	ANO
Funkce SSL VPN • Nabízené řešení musí podpovat možnost připojení klientů do VPN pomocí proprietární SSL VPN. Aplikace pro do VPN musí být podporována nejběžnějšími operačními systémy, jako například: Windows, macOS, Linux, Android nebo iOS. • Podpora bez klientského připojení do VPN na úrovni webového portálu, pomocí standardního internetového prohlížeče. • Možnost zabezpečení připojení do VPN vynucením dvou faktorového ověření. Například pomocí emailu, SMS, hardwarovou klíčenkou, nebo proprietární aplikace dostupná pro Android i iOS. • Zařízení musí umožňovat rozšíření pro využití dostupného dvou faktorového ověření • Zařízení musí být dodáno s min. 2 licencemi pro případné vyzkoušení dvou faktorového ověření • Vynucení ověření klientského certifikátu pro zvýšení zabezpečení. • Minimální počet současně navázaných SSL VPN tunelů: 180 • Minimální propustnost SSL VPN: 850 Mbps Funkce IPsec VPN • podpora site-to-site VPN • podpora klientských VPN • dostupnost VPN klienta pro koncové stanice (Windows, MacOS) z veřejně dostupných webových stránek • funkce klientských IPSec VPN nesmí být licencovaná na počet uživatel. V opačném případě požadujeme dodání neomezené licence. • Minimální počet IPSEC VPN tunelů typu lokalita-lokalita: 180 • Minimální počet klientských IPSEC VPN tunelů: 2200 • propustnost IPSec VPN min. 6 Gbps (měřeno při AES256-SHA256) • podpora konfigurace redundatních IPSec VPN tunelů za pomoci statického směrování • podpora konfigurace redundatních IPSec VPN tunelů za pomoci dynamického směrování • podpora funkce dynamického navazování IPsec tunelů dle potřeby komunikace • Podpora VXLAN • Podpora L2TP, PPTP, GRE	-	ANO

Funkce detekce aplikací na L7 (Application Control) o detekce známých aplikací na základě signatur o signaturový database automaticky aktualizované výrobcem o alespoň 4 000 podporovaných aplikací o pro populární cloudové aplikace (minimálně Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) požadujeme pokročilé akce typu blokování upload/download souborů, blokování her v rámci aplikace, blokování login atd. (relevantní k dané aplikaci) o možnost tvorby vlastních signatur o detekované aplikace je možné: povolit, monitorovat, blokovat o na základě typu aplikace musí být možné omezit šířku pásma pro danou aplikaci o funkce detekce aplikací se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. Alternativně požadujeme možnost využití v rámci tzv. NGFW pravidel popsaných výše. Funkce detekce a potlačení narušení (IPS/IDS) o minimální propustnost IPS inspekce 1,2 Gbps o signatury automaticky aktualizované výrobcem o alespoň 11 000 rozpoznávaných hrozeb (signatur) definovaných výrobcem o možnost tvorby vlastních signatur o funkce IPS se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům o funkce tzv. fail-open - při přetížení IPS je možné definovat, zda dojde k blokaci nebo propuštění provozu Funkce antivirové kontroly o ochrana před škodlivým kódem (malware, trojské koně apod.), včetně ochrany před polymorfním kódem o signatury automaticky aktualizované výrobcem o požadujeme AV kontrolu rozšířenou o inspekci tzv. sandbox technikou, poskytovanou formou služby dodávané výrobcem FW (licence musí být součástí dodávky) o možnost rozšíření o inspekci tzv. sandbox technikou formou lokálné HW appliance stejného výrobce o deklarovaná propustnost AV kontroly, v kombinaci s IPS, Application Control a zapnutým logováním min. 800 Mbps o funkce AV kontroly se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. o Podpora služby výrobce, která umožní detekovat malware, který byl objevený v době od poslední aktualizace AV signaturové databáze pomocí globální a rychle se aktualizující databáze hashů o Funkce odstranění škodlivého aktivního obsahu z dokumentů kancelářských aplikací. Funkce kategorizace webových stránek o založená na centrálně spravované databázi výrobce o minimálně 50 filtračních kategorií o možnost definice vlastních kategorií o možnost definice vlastních seznamů zakázaných URL o kategorizace musí zahrnovat I české a slovenské internetové stránky Funkce blokování video obsahu portálu YouTube o založená na centrálně spravované databázi výrobce o minimálně 9 filtračních kategorií o možnost definice vlastních kanálů na základně channel ID Funkce DNS filtru o Možnost blokovat DNS dotazy na základě příslušnosti k URL kategorii (obdobné kategorie jako u předchozího bodu) o Možnost definovat vlastní tzv. deny-list domén o Možnost přesměrovat komunikace se zakázanými doménami na vlastní portal/URL o Možnost importu seznamu blokovaných domén do DNS filtru o Detekce a blokování komunikace do botnet sítí Funkce ochrany před únikem citlivých informací (DLP) o možností analýzy běžných typů dokumentů a protokolů o možnost definice pravidel min. na základě regulárních výrazů, watermarkovacího nástroje a typu kontroly typu file checksum Funkce blokace stahování konkrétních typů souborů o možnosti zablokovat stahování souborů s konkrétními typy, jako napři. MSI, EXE… o funkce blokace stahování konkrétních typů souborů se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. Emailový antispamový modul o jednoduchá antispamová a antivirová inspekce elektronické pošty Podpora SSL dekrypce o podpora SSL dekrypce a inspekce pro ochranu jak koncových zařízeních, nebo serverů o funkce SSL dekrypce se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. o zařízení musí u SSL inspekce dosáhnout min. propustnost 700 Mbps Podpora pravidel pro obranu proti útokům typu DoS o zařízení musí umožnit uplatnit pravidla proti DoS útokům na základě politik, které se aplikují na konkrétní interface zařízení. o podpora detekce anomálií na 3. a 4. vrstvě o podpora např. TCP SYN FLOOD, ICMP FLOOD, SCTP SRC SESSION o funkce musí umožňovat provoz nejen blokovat, ale i sledovat pro možnost orientace na síti Explicitní proxy o podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl, DLP)	-	ANO
Firewall • Možnost nastavovat firewall politiku na základě geografických údajů • Aplikace firewall policy na známé internetové služby, kde databáze těchto služeb je pravidelně aktualizována výrobcem • Možnost snadné integrace cloudové služby. Minimálně na: MS Azure, Amazon Web Services, Google Cloud • Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru • Viditelnost do provozu na aplikační úrovni • Možnost dynamického stahování externích seznamů IP adres a jejich následné použití ve firewall policy • 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 application control, nikoliv pouhý TCP/UDP port) resp. kategorie URL filteringu (nikoliv jako AppCtrl resp URL filtering profil aplikovaný na dané pravidlo). • Ověřování uživatelů LDAP, Active Directory, Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu • Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření. • Traffic Shaping, QoS s podporou priroritizace provozu na základě DSCP markování a ToS, aplikace traffic shaping na konkrétní		

aplikaci nebo webovou kategorii • Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu • Podpora funkce reverzní proxy • Podpora silné autentizace uživatelů – integrovaná podpora generátor jednorázových hesel (OTP) – pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů • Administrátorské účty mohou být volitelně zabezpečený pomocí dvou faktorového ověření Integrovaný kontroler bezdrátových sítí (Wi-Fi) • Wifi kontroler integrovaný do NGFW platformy • Bezdrátová síť (SSID) může být reprezentována virtuálním síťovým rozhraním – provoz tunelován z AP do kontroleru • podpora bezpečnostních profilů (AV, AppControl, Webfilter, DLP) přímo na wifi kontroleru • podpora SSL dekrypce uživatelského provozu přímo na wifi kontroleru • Podpora wifi přístupových bodů stejného výrobce s výrobcem FW řešení • Možnost volby z různých modelů (802.11abgn, 802.11ac, 802.11ac wave2, indoor, outdoor, WiFi 6) • Podpora BSS Coloring • On-wire rogue AP detekce a mitigace • Podpora fast-roamingu (802.11 k,v,r) • podpora více PSK u jednoho SSID • podpora IPSEC tunelu pro šifrování data plane (uživatelských dat) • Podpora WPA3 protokolu Integrovaný switch kontroler • Zařízení musí podporovat switch kontroler jenž umožní spravovat switche výrobce z jednoduchého GUI • Možnost správy VLAN • Spolu s NAC politikami musí nabídnout možnost automatické přiřazení VLAN pro konkrétní zařízení či skupinu zařízeních • Z integrovaného switch kontroleru musí být obsluha schopna pomocí GUI jednoduše definovat VLAN na konkrétní port • V případě správy switche s funkcí PoE musí být v GUI možnost resetování PoE pro vzdálený restart zařízení	-	ANO
Virtualiazce • Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext musí být plnohodnotné řešení včetně odděleného GUI, management účtů atp. • Součástí dodávky musí být licence na min. 10 virtuálních kontextů (včetně licence na kompletní podporu požadovaných bezpečnostních funkcí v těchto virtuálních kontextech) • Každý virtuální kontext je zároveň samostatným wifi kontrolerem • Podporou izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů)	-	ANO
Management • FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici • Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě • Podpora otevřeného API (možnost integrace vybraných funkcí do stávající management infrastruktury)	-	ANO

Instalace a nastavení		**Doplní účastník ANO/NE nebo nabízené parametry**
Součástí předmětu plnění bude instalace a nastavení všech dodaných zařízení, SW a podpis akceptačního protokolu. Požadavky na instalaci a nastavení jsou specifikovány na samostatném listu tohoto dokumentu (list Implementace)	-	ANO

Minimální požadavek na funkcionalitu	Upřesnit požadavek	Účastník doplní ANO/NE nebo nabízené parametry
Obecné požadavky		
Je poptáván systém pro ukládání a korelaci logů (dále jen "Systémem ukládání logů") v síti Zadavatele. Systém musí být plně kompatibilní s dodávanými zařízeními, musí podporovat analýzu logů nad provozem. Dále musí být schopné poskytovat reporty nad logy a informovat správce systému o hrozbách, které byly v síti odhaleny.	-	ANO
Hlavní parametry appliance: • Musí se jednat o virtuální appliance s podporou minimálně VMware, KVM a Hyper-V • Kapacita úložiště logů minimálně 3TB a minimální limit pro množství přijatých logů za jeden den 6GB • Podpora minimálně 4 virtuálních interfaců • Možnost škálovatelného navýšení kapacity úložiště na základě licence • Možnost provozovat appliance pouze jako dočasné úložiště logů z důvodu šetření datového pásma o Mít možnost specifikovat typ logů, které budou na hlavní analyzační nástroj odeslány okamžitě Multitenantnost • Možnost rozdělení zařízení na oddělené administrativní sekce (každý virtuální kontext firewallu může být v jiném administrativním kontextu centrálního logovacího zařízení) • Každý administrativní celek musí mít možnost mít vlastního administrátora, který nebude mít přístup do jiných administrativních celků	Umístění v lokalitě datového centra	ANO
Funkce		
Logovací funkce • Musí se jednat o centrální logovací prvek pro všechny UTM firewally • Musí umět ukládat jakkoliv Syslog zprávy • Funkce zpětné kontroly logů o přístupu na web (až 7 dní) z důvodu „zero-day“ malicious websites • Vizualizace provozu nad všemi firewally • Možnost dostat se z vizuálního zobrazení proklikem na konkrétní logy • Realtime a historický náhled do logů • Korelace logů • Samostatná sekce týkající se hrozeb v síti • Podpora prohlížení statistických údajů nad logy Reporting • Podpora reportů nad logy ve formátu HTML/CSV/XML/PDF • Generování reportů v pravidelných intervalech • Předefinované vzory pro reporty na nejčastější použití • Možnost vytváření vlastních reportů na základě konkrétních SELECT dotazů do databáze • Možnost úpravy reportů do vlastního designu – vlastní loga, texty, úprava hlavičky Další funkce • Event Management - upozorňování na důležité informace z logů – emailem a snmp trapy, syslog zprávou • Předvytvořený dashboard pro využití dohledovým centrem • Možnost customizace rozhraní pro NOC/SOC dle konkrétních požadavků na dohlížené informace Možnosti správy a komunikace • Podpora SNMPv2, SNMPv3 • Podpora REST API • Správa přes webové rozhraní HTTPS • Administrátorské účty musí být možné konfigurovat lokálně nebo na vzdáleném serveru (LDAP, RADIUS, Tacacs+) • Podpora statického routování • Možnost zašifrování spojení mezi zařízením které odesílá logy a Systémem ukládání logů.	-	ANO

Minimální požadavek na funkcionalitu	Upřesnit požadavek	Účastník doplní ANO/NE nebo nabízené parametry
Obecné požadavky		
Endpoint Management System Požadujeme dodání celého řešení včetně technické podpory, to po dobu minimálně 3 let. Celé řešení musí podporovat centrální správu koncových bodů z jedné platformy. V rámci Veřejné zakázky poptáváme licenci pro 25 koncových bodů. Nástroj pro centrální správu koncových bodů musí být dostupný pod operační systém Windows Server. Celé řešení musí být modulární, mít charakter instalačních balíčků a musí umožňovat instalaci všech modulů a jejich případnou pozdější aktivaci/deaktivaci. Ochrana koncových bodů musí být dostupná pro následující operační systémy: Windows, macOS, Linux, Android, iOS, Chromebook. Níže popsané funkce musí být v plném rozsahu dostupné minimálně pro operační systém Windows. U jiných operačních systémů není potřeba podpora všech funkcí.	**Umístění centrální správy koncových bodů v lokalitě datového centra**	ANO
Funkce		
• Integrace do poptávaného firewallového řešení • Centrální správa skrze dedikovanou aplikaci, která musí být součástí dodávky včetně všech potřebných licencí. • Endpoint ochrana musí podporovat funkci vzdáleného logování do nástroje, jenž je součástí celé dodávky. • Podpora prohledání operačních systémů za cílem nalezení neaktuálního softwaru. Endpoint ochrana zároveň musí podporovat jejich automatickou aktualizaci. • Podpora integrace VPN klienta, kompatibilního s firewallem jenž je součástí celé dodávky. • Podporovat musí jak klasickou IPsec VPN, tak i VPN specifickou pro dodávaný firewall. • Možnost filtrovat webové stránky na základě jejich kategorie – pro zjednodušení celé správy musí podporovat minimálně jednorázový import filtračních pravidel z používaného, nebo dodaného firewallu. • Podpora kontroly USB zařízeních. Endpoint ochrana musí být schopna zakázat nebo naopak povolit konkrétní USB zařízení na základě HW ID. • Součástí endpoint ochrany musí být i antivirový modul, jenž se aktualizuje pomocí klasických definic signatur. • Podpora sandboxování neznámých souborů přímo v operačním systému koncového bodu – podporovat musí jak lokální fyzický sandbox, nebo musí umožňovat napojení na službu, jenž tyto funkce pokryje, součástí dodávky musí být náležité licence. • Podpora automatického vložení koncového bodu do karantény. • Endpoint ochrana musí být vybavena aplikačním firewallem, jenž podporuje blokaci aplikací podle jejich signatur. • Centrální správa celého řešení musí obsahovat modul, jenž umožňuje nahlédnutí do softwarové výbavy všech spravovaných zařízeních. • Řešení musí obsahovat dedikovaný modul pro ochranu proti Ransomware.	-	ANO

Požadavky na implementační práce	Upřesnit požadavek	Účastník doplní ANO/NE nebo nabízené parametry
Obecné požadavky		
Realizace v sídle Zadavatele, v datovém centru a na pobočkách		ANO
Funkce		
Úvodní plánovací a přípravné práce Diskuze se zákazníkem, informace k záměru Analytické a přípravné práce včetně zmapování současného řešení Kerio, vyhodnocení politik a nastavení z hlediska dnešních bezpečnostních standardů a best practice. Hlavní lokalita Praha Plánování součinnosti a tech. připravenosti Příprava základní konfigurace firewallu vč. HA a úvodní policy Autentizace uživatele (LDAP/FSAE/Kerberos/Radius…), doplnění pravidel Fyzická instalace v lokalitě a testování firewallu onsite Doplnění SSL Decrypce, GPO/distribuce certifikát, ladění VPN-S2S(SPOKE)/SDWAN sestavení a ladění vč. routingu a policy/rolí Dokončovací práce, ladění politiky a přístupu Datové centrum Plánování součinnosti a tech. připravenosti Příprava základní konfigurace firewallu vč. HA a úvodní policy Příprava publikačních pravidel + WAF/SSL Offloading Konfigurace firewallů v DC na separátní IP adresaci, testování, fyzickou instalaci provede Zadavatel VPN-C2S/S2S(HUB)/SDWAN sestavení a ladění vč. routingu a policy/rolí Dokončovací práce, ladění politiky a přístupu Ostatní tři lokality Příprava základní konfigurace firewallu Autentizace uživatele (LDAP/FSAE/Kerberos/Radius…), doplnění pravidel Konfigurace a testování firewallů onsite, fyzickou instalaci provede Zadavatel VPN-S2S/SDWAN sestavení a ladění vč. routingu a policy/rolí Dokončovací práce, ladění politiky a přístupu Centrálně řízený EMS Plánování součinnosti a tech. připravenosti Instalace a konfigurace EMS (na připravený Win. server) Provázání s AD, sestavení EPP policy-struktury Příprava a aplikace EPP policy vč. compliance a vazby na NGFW a log management Publikace EMS a příprava instalačních balíků EPP klienta Testování v provozu (vybrané stroje), konf. požadovaných výjimek Roullout klienta a dohled nad tím Post-deployement support Log managemnent - Systémem ukládání logů Základní deployement a konfigurace Notifikace a reporting IoC a konfigurace automations na straně NGFW Další práce: Školení na úroveň administrátor pro dodávané firewally a SW. Školení bude pro minimálně 2 osoby v rozsahu min. 2 dny. První den školení bude obsahovat obecné informace o dodaném firewallu a druhý den školení bude obsahovat konkrétní informace o naší instalaci a použití produktu typu Analyzer pro zpracování statistik. Vytvoření impl. dokumentace Konzultace v celkovém rozsahu 3 dny (tedy 24 hodin), čerpání v blocích min 4 hodiny, možnost čerpání do 6 měsíců od instalace	-	ANO