SPŠ EL+IT
STŘEDNÍ PRŮMYSLOVÁ ŠKOLA elektrotechniky a informačních technologií, DOBRUŠKA
info@spseldobruska.cz
+420 773 684 544
+420 494 623 891
www.spseldobruska.cz
Čs. odboje 670, 51801 Dobruška

Příloha č. 4 - Krycí list k podání nabídky na dodávku Next Generation Firewallu

Zadavatel: Střední průmyslová škola elektrotechniky a informačních technologií, Dobruška, Čs.odboje 670

Název akce: Dodávka Next Generation Firewallu

Identifikační údaje uchazeče:	TAKTIK, a.s. IČ: 28522869, Eberlova 1472/9, PSČ 15500

Název	Požadované parametry dodávky	Splňuje parametry ANO / NE	Množství	Záruka v měsících	jednotková cena bez DPH	jednotková cena s DPH*	celková cena bez DPH	celková cena s DPH	Poznámka
Firewall *	Předmětem dodávky je NG Firewall ve formě fyzického zařízení - appliance.	ANO	**1**	60	139 500	168795	139 500	168795	Firewall Palo Alto Networks PA-440 včetně redundantního napájení a včetně předplatného Precision AI Network Security Subscription Bundle (Advanced Threat Prevention, Advanced URL Filtering, Advanced Wildfire, Advanced DNS Security a SD-WAN). Vše v délce trvání předplatných a podpory výrobce v délce trvání 60 měsíců.
	Nabízené řešení musí v nejnovější reportu "Gartner magic quadrant for network firewals" figurovat v kvadrantu "leaders".	ANO							
	Součástí dodávky je příslušenství pro montáž do standardní rackové skříně.	ANO							
	Součástí dodávky musí být veškeré licence potřebné pro požadované funkcionality v délce trvání min. 5 let.	ANO							
	Součástí dodávky musí být zajištění podpory výrobce v délce trvání 5 let. Zadavatel musí mít možnost přímého kontaktování podpory výrobce telefonicky, emailem nebo přes portál podpory výrobce v režimu 24/7. Výměna vadných HW součástí musí být v režimu nejpozději NBD.	ANO							
	Řešení musí umožňovat jednoduché rozšíření na HA konfiguraci dodáním pouze dalšího identického firewallu.	ANO							
	NG Firewall musí disponovat redundantními komponenty minimálně v oblasti chlazení a napájení - ventilátory a zdroje musí být minimálně v páru a vyměnitelné za běhu zařízení.	ANO							
	Minimální požadovaná propustnost zařízení při plné inspekci provozu (aplikační kontrola, IPS, AV, TP, kontrola veškerých paketů, logování veškerého síťového provozu) musí dosahovat nejméně hodnoty 1200Mbps.	ANO							
	Počet možných současných připojení musí být minimálně 200 000.	ANO							
	Počet nový připojení za sekundu musí být minimálně 30 000.	ANO							
	Konektivita pro vlastní produkční síť minimálně v rozsahu: 8x 1G RJ45.	ANO							
	Dedikovaný port 1G RJ45 pro správu NG Firewallu.	ANO							
	NG Firewall disponuje úložištěm pro ukládání logů o kapacitě minimálně 100GB.	ANO							
	Rozhraní pro správu firewallu musí být fyzicky odděleno od rozhraní pro filtrování produkčního síťového provozu tak, aby v případě zahlcení provozem (například DDoS útokem) bylo stále možné firewall spravovat.	ANO							
	NG Firewall musí podporovat zapojení v režimech L2 (s virtuálním L3 rozhraním), L3, transparent a TAP.	ANO							
	NG Firewall plně podporuje IPv4 a IPV6.	ANO							
	NG Firewall 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							
	NG Firewall musí podporovat směrování typu Static route, OSPFv2, OSPFv3, BGP a PBR (Policy Based Routing).	ANO							
	PBR musí být možno nakonfigurovat na základě všech dostupných metrik typu interface, IP adresa, protokol a port, uživatel.	ANO							
	NG Firewall musí podporovat aplikační detekci a kontrolu jako svou nativní funkcionalitu.	ANO							
	NG Firewall podporuje konfiguraci Bidirectional Forwarding Detection (BFD) pro protokoly BGP a OSPF.	ANO							
	NG Firewall podporuje možnost oddělení provozu do routing-instancí a to i pod úrovní virtuálního systému.	ANO							
	NG Firewall podporuje konfigurace GRE tunelů.	ANO							
	NG Firewall 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							
	Z důvodu zapojení systému do kritické infrastruktury musí být NG Firewall schopen čerpat čas z autentizovaného NTP serveru.	ANO							
	NG Firewall podporuje Multicast PIM-SM, PIM-SSM, IGMP v1, v2, and v3.	ANO							
	NG Firewall 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							
	NG Firewall podporuje tvorbu bezpečnostních politik se specifikací source IP, destination IP , application, user/user group.	ANO							
	Při instalaci firewall politik nedojde k výpadku navázaných spojení.	ANO							
	NG Firewall podporuje konfiguraci ochrany firewallu na síťových rozhraních – podpora IP spoofing a UDP, ICMP a SYN floods.	ANO							
	NG Firewall podporuje překlady adres ve formě: Statický NAT, Destination NAT, Source NAT (za jednu nebo více IP adres), obousměrné překlady IPv4 a IPv6. Persistence překladu v rámci NAT poolu na úrovni IP.	ANO							
	NG Firewall podporuje konfigurace route-based site-to-site IPsec VPN.	ANO							
	NG Firewall 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							
	NG Firewall podporuje prioritizaci provozu na základě DSCP.	ANO							
	NG Firewall podporuje prioritizaci provozu na základě identifikované aplikace.	ANO							
	NG Firewall nebo jiné dekrypční zařízení musí podporovat dešifrování odchozího SSL/TLS provozu, za pomocí podvržení serverového certifikátu klientům reverse proxy.	ANO							
	NG Firewall nebo jiné dekrypční zařízení musí podporovat dešifrování příchozího SSL/TLS provozu, za pomocí naimportovaného privátního klíče interního serveru forward proxy.	ANO							
	NG Firewall nebo jiné dekrypční zařízení musí podporovat dešifrování Secure Shell (SSH proxy) a kontrolovat tunelované aplikace.	ANO							
	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							
	NG Firewall nebo jiné dekrypční zařízení poskytuje možnost dešifrovat pouze provoz spadající do rizikových skupin definovaných výrobcem NG Firewall nebo jiného dekrypčního zařízení.	ANO							
	NG Firewall nebo jiné dekrypční zařízení musí podporovat dešifrování za pomocí ECC (Elliptical Curve Cryptography), včetně DHE a ECDHE pro příchozí i odchozí provoz.	ANO							
	NG Firewall nebo jiné dekrypční zařízení musí podporovat dešifrování protokolu TLS verze 1.2 i 1.3.	ANO							
	NG Firewall nebo jiné dekrypční zařízení musí podporovat přeposílání dešifrovaného provozu na jiné skenovací zařízení (např. DLP, analýza provozu a souborů apod.)	ANO							
	NG Firewall nebo jiné dekrypční zařízení musí být schopno dekryptovat TLS obecně, tedy i protokoly LDAPS, FTPS, apod., nikoliv pouze HTTPS.	ANO							
	Detekce aplikace musí být součástí základní funkcionality NG Firewall.	ANO							
	Zadání aplikace je standardním kritériem při tvorbě bezpečnostního pravidla, aplikace není přidávána jako profil.	ANO							
	Definovaná aplikace je jedním "match" kritériem při policy lookup společně se source a destination IP.	ANO							
	Plná podpora logování pravidel s definovanými aplikacemi a viditelný název aplikace/kategorie v zaslaném logu.	ANO							
	NG Firewall obsahuje mimo definovaných jednotlivých aplikací i aplikační kategorie.	ANO							
	NG Firewall detekuje aplikaci nezávisle na protokolu a portu, na kterém je provozována.	ANO							
	NG Firewall podporuje identifikaci aplikací na nestandardních portech.	ANO							
	Identifikace aplikace musí probíhat přímo v NG Firewall.	ANO							
	NG Firewall musí umět pracovat s neznámými aplikacemi - upozornit na ně a mít možnost je zakázat.	ANO							
	NG Firewall 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							
	NG Firewall podporuje logování i blokace přenesených souborů aplikacemi v upload/download směru.	ANO							
	NG Firewall musí podporovat vytváření bezpečnostních pravidel na základě uživatelských identit.	ANO							
	Uživatelská identita, nebo uživatelská skupina, do které uživatelé patří je jedním "match" kritériem při policy lookup společně s aplikací a případně source/destination IP.	ANO							
	Identitu je možno přidat do pravidla jako jednotlivý uživatel, nebo jako skupina uživatelů vytvořená staticky na NG Firewall, nebo získaná ze všech následujících externích adresářových služeb: On-Premise AD, Azure AD.	ANO							
	NG Firewall podporuje získávání vazby IP adresa a uživatelské jméno bez nutnosti instalace klienta na koncové zařízení nebo doménový kontroler.	ANO							
	NG Firewall musí podporovat získávání vazby IP adresa a uživatelské jméno bez nutnosti instalace dalších komponent mimo samotné HW appliance.	ANO							
	NG Firewall musí podporovat získávání vazby IP adresa a uživatelské jméno z VPN agenta.	ANO							
	NG Firewall 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							
	NG Firewall musí být schopen detekovat neznámé vzorky přímo na firewallu bez nutnosti napojení na externí zařízení nebo službu.	ANO							
	NG Firewall musí podporovat sandboxing v cloudu, který využívá umělou inteligenci k ochraně před sofistikovanými útoky.	ANO							
	Sandbox musí umět používat introspekci VM (Virtual Machine) a paměťovou analýzu a umí předcházet tomu, aby malware rozpoznal, že se nachází ve virtuálním prostředí.	ANO							
	Sandbox musí používat inteligentní analýzu běžící paměti a zachycuje snímky v době, kdy probíhá podezřelá aktivita.	ANO							
	Sandbox musí rozpoznat, které závislosti malware potřebuje k tomu, aby se spustil a umí je nasimulovat.	ANO							
	NG Firewall disponuje Intrusion detection and prevention a databáze IPS signatur je uložena přímo ve NG Firewall a pravidelně aktualizována výrobce po celou dobu životního cyklu zařízení.	ANO							
	Aplikace IPS profilu lze nastavit granulárně na úrovni bezpečnostní politiky.	ANO							
	NG Firewall umožňuje tvorbu uživatelsky definovaných IPS a spyware signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele.	ANO							
	NG Firewall disponuje systémem ochrany proti virům a škodlivého kódu, databáze AV signatur je uložena přímo ve NG Firewall a pravidelně aktualizována výrobce po celou dobu životního cyklu zařízení.	ANO							
	Aplikace AV profilu lze nastavit granulárně na úrovni bezpečnostní politiky.	ANO							
	Antivirus je schopen kontrolovat provoz v minimálně těchto aplikacích: SMTP, POP3, IMAP, HTTP, HTTPS, HTTP/2, FTP a SMB.	ANO							
	NG Firewall podporuje v bezpečnostních pravidlech použití externích dynamických seznamů.	ANO							
	NG Firewall musí obsahovat integrovaný systém ochrany proti přítomnosti virů a škodlivého kódu. Databáze AV signatur musí být uložena přímo v NG Firewall. Aplikace AV profilu musí být granulární, na úrovni bezpečnostního pravidla.	ANO							
	NG Firewall musí podporovat možnost zablokování útoku využívajícího známá C&C centra i v případě, že je provoz šifrován a není možné provádět SSL dekrypci.	ANO							
	NG Firewall 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							
	NG Firewall 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							
	NG Firewall musí obsahovat plnohodnotné textové (CLI) i grafické rozhraní (GUI) pro správu síťových a bezpečnostních funkcí bez nutnosti používání centrálního management serveru. Vzdálené připojení k CLI nebo ke GUI musí podporovat šifrování.	ANO							
	NG Firewall GUI obsahuje offline kontextovou nápovědu.	ANO							
	NG Firewall CLI rozhraní umožňuje zobrazení konfigurace ve formátu, který je možné mírně upravit a následně dávkově vložit pro replikaci částí konfigurace (např. hromadné vytvoření objektů, statických route apod.)	ANO							
	NG Firewall GUI musí podporovat čtení a vyhledávání v logových záznamech bez nutnosti používání centrálního management serveru.	ANO							
	NG Firewall podporuje pro autentizaci a autorizaci administrátorů protokoly LDAP, Radius, SAML a osobní certifikát.	ANO							
	NG Firewall podporuje Multi-factor Authentication pro dodatečnou autentizaci administrátorů do management rozhraní.	ANO							
	NG Firewall podporuje možnost vlastní definice administrátorských rolí a možnost omezování přístupů do jednotlivých částí konfigurace.	ANO							
	NG Firewall disponuje nástrojem pro odchycení provozu pro analýzu (Packet capture).	ANO							
	NG Firewall "nástroj pro odchycení provozu" musí být schopen odchytit provoz jak na datových, tak na OOB management interfacech.	ANO							
	NG Firewall "nástroj pro odchycení provozu" musí být schopen odchytit provoz jak na vstupním, tak na výstupním interface a porovnáním času zjistit latenci daného paketu.	ANO							
	NG Firewall musí obsahovat nativní nástroje pro debugging problémových situací v úrovni L2 – L7 ISO/OSI modelu.	ANO							
	HW appliance musí obsahovat plnohodnotné API rozhraní pro čtení a konfiguraci síťových nastavení, bezpečnostních a dalších pravidel, nastavení síťových rozhraní a směrování. API musí být důkladně popsáno ve veřejně přístupné dokumentaci.	ANO							
	NG Firewall musí být možné spravovat z administrátorských stanic s OS Windows, Linux a MacOS X (včetně HW s čipem Apple Silicon).	ANO							
	NG Firewall management musí podporovat práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem.	ANO							
	NG Firewall musí podporovat kontrolu tzv. čtyř očí tak, že jeden administrátor připraví změny a druhý je následně schválí a aplikuje.	ANO							
	NG Firewall musí obsahovat nástroj pro analýzu logů bez nutnosti využití dalšího systému mimo GUI.	ANO							
	NG Firewall 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							
	NG Firewall musí podporovat přeposílání logů na zařízení třetích stran, minimálně SysLog ve formátu CEF.	ANO							
	NG Firewall musí umožňovat výběr přeposílaných logů na úrovni bezpečnostního pravidla, tedy nastavit, která bezpečnostní pravidla se mají logovat a která naopak ne.	ANO							
	NG Firewall musí mít možnost detailně definovat, které typy logů jsou zasílány, do jakých cílových lokací (email, SNMP Trap, SysLog atd.).	ANO							

***Střední průmyslová škola elektrotechniky a informačních technologií, Dobruška, Čs.odboje 670, příspěvková organizace je neplátce DPH. Nabídka musí být rozdělana zvlášť na cenové položky za HW a SW (licence, support, apod.).**

Předkladatel uvede reference na minimálně 3 zakázky podobného rozsahu v minimální výši 500 000,- včetně DPH. Uvede zákazníka, rok realizace a kontaktní osobu u zákazníka, která může potvrdit.

Pozn.: Zadavatel si vyhrazuje právo objednat jednotlivé položky nabídky zvlášť na více faktur.

Celková cena bez DPH	**139 500 Kč**		**Celková cena s DPH**	**168 795 Kč**

17.09.2024
Datum

Jméno a podpis osoby oprávněné jednat jménem uchazeče