**Příloha č. 6 zadávací dokumentace k veřejné zakázce**

**OBNOVA A ROZŠÍŘENÍ OCHRANY INTERNÍCH ZÓN A PERIMETRU POMOCÍ NOVÝCH FIREWALL**

**TECHNICKÁ SPECIFIKACE**

1. POPIS POŽADAVKŮ
	1. Stávající stav

Zadavatel provozuje dva perimetrové Firewally (FW) v HA klastru ACTIV - PASIV, které jsou umístěny ve fyzicky oddělených datových centrech. Připojení do interní sítě pomocí 2 x 10Gb SFP+ a do externí sítě pomocí 1 Gb Eth. Zadavatel provozuje dvě detašovaná pracoviště připojena pomocí 1Gb Eth.

Uživatelská VPN z externí sítě do vnitřní využívá VPN Klienty daného řešení.

VPN Site to Site pro přístupy externích dodavatelů IT služeb a detašovaných pracovišť.

* 1. Požadovaný stav

Předmětem veřejné zakázky je dodání vysoce dostupného řešení firewall typu NGFW dle níže uvedené specifikace. Vlastní zařízení budou umístěna v geograficky oddělených, datově propojených lokalitách, a budou propojena do funkčního, vysoce dostupného clusteru. Požadujeme vysokou variabilitu síťových rozhraní – minimálně kombinace 1GE metalických, 1GE optických a 10GE optických portů. Dodávka perimetrových, segmentačních FW a FW pro detašovaná pracoviště.

Z důvodu požadavku na mikro segmentaci sítě požadujeme řešení, které umožní rozdělit systém na perimetrové FW (hraniční směrovače) a segmentační FW (směrovač interních serverových zón).

Uživatelská VPN z externí sítě do vnitřní bude využívat VPN Klienty daného řešení.

Zavedení 2FA VPN klienta pro správce IT.

Přístupy externích dodavatelů IT služeb a detašovaných pracovišť bude řešen VPN Site to Site.

1. POŽADOVANÉ VLASTNOSTI A FUNKCE SEGMENTAČNÍCH FIREWALLŮ
	1. Hraniční směrovače (firewall) – perimetrové

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kategorie vlastností** | **Požadovaný parametr nebo funkce** | **Požadovaná hodnota** | **Splnění požadovaných parametrů (ANO/NE)** | **Komentář** |
| **Typ a počet zařízení** | Hraniční směrovač (firewall), celkový počet: 2 kusů |  |   | *Název dodávaného zařízení / označení (PN)* |
|  | min. počet nových spojení za sekund | 100 000 |   |   |
| min. počet současně navázaných TCP spojení: | 945 000 |   |   |
| min. propustnost funkce IPSEC VPN (při použití AES256, SHA256)  | 4,1 Gbps |   |   |
| min. propustnost funkce NGFW (stavový firewall + IPS, rozpoznávání aplikací na L7)  | 4,5 Gbps |   |   |
| min. počet metalických sítových rozhraní GE RJ45  | 8 |   |   |
| min. počet optických sítových rozhraní 1 GE SFP  | 4 |   |   |
| min. počet optických sítových rozhraní 10 GE SFP+  | 4 |   |   |
| min. počet metalických sítových rozhraní 5GE RJ45  | 4 |   |   |
| konzolový port (sériová linka)  | 1 |   |   |
| USB port (bootstrap konfigurace, připojení externího LTE modemu)  | 1 |   |   |
| Duální napájení (dva integrované zdroje 230 V) | ANO |   |   |
| **Požadavky na obecné funkce** | Hardware řešení formátu rackmount, o maximální velikosti 1U | ANO |   |   |
| Konsolidované bezpečnostní řešení obecně značené jako firewall nové generace (next generation firewall, NGFW) | ANO |   |   |
| Podpora vysoké dostupnosti v režimu active-active i active-passive. Pokud tato funkce vyžaduje licenci, tak tato licence musí být součástí dodávky. | ANO |  |  |
| Zařízení musí být dodáno v režimu vysoké dostupnosti. Bez výpadkový cluster bude sestaven celkem ze 2 zařízení – součástí dodávky musí být obě zařízení včetně všech potřebných licencí. | ANO |  |  |
| Grafické konfigurační rozhraní (např. webový prohlížeč) a příkazový řádek bez omezení na počet administrátorů | ANO |   |   |
| Podpora virtuálních  | ANO |   |   |
| Podpora stavového firewallingu pro IPv4 i IPv6, podpora nat 64/46, plnohodnotná podpora IPv6 | ANO |   |   |
| Nasazení NGFW musí podporovat zapojení v režimech L2 (s virtuálním L3 rozhraním), L3, transparent a TAP | ANO |   |   |
| Podpora režimu vysoké dostupnost, plnohodnotná správy z lokálního management rozhraní́ celého HA clusteru (správa celého clusteru probíhá z jednoho místa, konfigurace se automaticky sdílí), podpora možnosti centrální správy | ANO |   |   |
| Podpora tunelování provozu pomocí technologie GRE | ANO |   |   |
| **Požadavky na sítové funkce** | Podpora VLAN dle IEE 802.1Q | ANO |  |  |
| Podpora agregovaných interface (LACP) IEE802.3ad | ANO |  |  |
| Podpora redundantních rozhraní | ANO |  |  |
| Podpora loopback rozhraní | ANO |  |  |
| Možnost vytvořit switch nad několika fyzickými porty | ANO |  |  |
| Možnost práce se zónami (logická skupina sítových rozhraní zastoupená objektem v konfiguraci) | ANO |  |  |
| Podpora vytvoření tzv. wire pair pro L2 transparentní inspekci | ANO |  |  |
| Podpora dynamických směrovacích protokolů min v rozsahu: RIP, OSPF, BGP, podpora BFD | ANO |  |  |
| Podpora LLDP |  |  |  |
| Ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign On | ANO |  |  |
| Podpora lokální databáze a vzdálené databáze (radius, ldap, tacacs+, saml, kerberos) pro ověřování uživatelů | ANO |  |  |
| Ověřování uživatelů pomocí SSO funkcionality pomocí Radius Single Sign On a AD pollingu | ANO |  |  |
| Funkce QoS a traffic shaping min. ve variantě policing a queuing, aplikace politiky globálně nebo pomocí pravidel, podpora DSCP v pravidlech | ANO |  |  |
| Podpora funkcí VPN brány ‐ IPSec VPN (dle platných standardů pro možnost propojení se zařízeními třetích stran), SSL VPN (portálový režim bez klienta, tunelový režim s klientem), podpora funkce bezpečného vzdáleného přístupu do vnitřní sítě založeném na principu zero trust | ANO |  |  |
| Podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3  | ANO |  |  |
| **Požadavky na bezpečnostní funkce** | Antivirový engine musí být vybaven lokální databází vzorků škodlivého kódu a AI/ML enginem pro identifikaci podezřelých či neznámých vzorků | ANO |  |  |
| Funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (tzv. mobile malware), detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak) | ANO |  |  |
| Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 5000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace | ANO |  |  |
| Funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), výrobcem aktualizovaná a udržovaná databáze, vynikající pokrytí českého internetu; požadované akce – povolení stránky, logování stránky, brouzdání s proklikem, nutnost autentizace uživatele pro určitou kategorii | ANO |  |  |
| Funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů | ANO |  |  |
| Možnost blokovat sítový provoz na základě URL, kategorie webové stránky, IP adresy (rozsahu), GeoIP databáze, data a času | ANO |  |  |
| Podpora dvoufaktorové autentizace pomocí HW nebo mobilních OTP tokenů pro uživatele i administrátory | ANO |  |  |
| Analýza a zabezpečení DNS dotazů (ochrana před DNS poisoningem), filtrování DNS dotazů na základě kategorizace | ANO |  |  |
| Integrovaná funkce filtrování přenášených souborů pro protokoly CIFS, FTP, HTTP, IMAP, MAPI, POP3, SMTP a SSH; možnost konfigurace různého chování pro příchozí a odchozí směr, možnost práce s heslem chráněnými soubory, možnost logovat a blokovat provoz | ANO |  |  |
| Integrovaná funkcionalita pro ochranu publikovaných webových služeb proti sítovým útokům, možnost konfigurace ochrany proti útokům typu SQL injection, generické techniky, trojské koně, únik informací, známé zranitelnosti).  | ANO |  |  |
| Ochrana VoIP komunikace min. pro protokoly SIP a SCCP SIP ALG, inspekce SIP komunikace | ANO |  |  |
| **Licence** | Licence na 60 měsíců | ANO |   |   |
| **Záruky** | Minimální záruka režim 24x7 na 60 měsíců se zaručeným odesláním nového zařízení do konce následujícího pracovního dne od nahlášení závady | ANO |   |   |
| **Podpora** | Podpora, aktualizace SW a přístup k novým funckionalitám na dobu minimálně 60 měsíců | ANO |   |   |
| **SFP+ transceiver** | OEM SFP+ transceiver 10 Gbps, SM, LC duplex, 8 ks | ANO |  |  |
| **Optický kabel** | Optický patchcord, 9/125,LC-LC, SM, duplex, 2m 4ks | ANO |   |   |
| **Optický kabel** | Optický patchcord, 9/125,LC-LC, SM, duplex, 1m 4ks | ANO |   |   |

* 1. Směrovač (firewall) interních serverových zón – segmentační

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kategorie vlastností** | **Požadovaný parametr nebo funkce** | **Požadovaná hodnota** | **Splnění požadovaných parametrů (ANO/NE)** | **Komentář** |
| **Typ a počet zařízení** | Hraniční směrovač (firewall), celkový počet: 2 kusů | ANO |  ANO | *Název dodávaného zařízení / označení (PN)* |
| **Obecné** | Podpora vysoké dostupnosti v režimu active-active i active-passive. Pokud tato funkce vyžaduje licenci, tak tato licence musí být součástí dodávky. | ANO |  |  |
| Zařízení musí být dodáno v režimu vysoké dostupnosti. Bez výpadkový cluster bude sestaven celkem ze 2 zařízení – součástí dodávky musí být obě zařízení včetně všech potřebných licencí. | ANO |  |  |
| min. počet nových spojení za sekundu  | 100 000 |   |   |
| min. počet současně navázaných TCP spojení  | 945 000 |   |   |
| min. propustnost funkce IPSEC VPN (při použití AES256, SHA256)  | 4,1 Gbps |   |   |
| min. propustnost funkce NGFW (stavový firewall + IPS, rozpoznávání aplikací na L7)  | 4,5 Gbps |   |   |
| min. počet metalických sítových rozhraní GE RJ45  | 8 |   |   |
| min. počet optických sítových rozhraní 1 GE SFP  | 4 |   |   |
| min. počet optických sítových rozhraní 10 GE SFP+  | 4 |   |   |
| konzolový port (sériová linka)  | 1 |   |   |
| USB port (bootstrap konfigurace)  | 1 |   |   |
| duální napájení (dva zdroje 230 V vyměnitelné za provozu bez výpadku systému a musí být součástí dodávky) | ANO |   |   |
| min. počet virtuálních kontextů  | 6 |   |   |
| **Požadavky na obecné funkce** | hardware řešení formátu rackmount, o maximální velikosti 1U | ANO |   |   |
| Konsolidované bezpečnostní řešení obecně značené jako firewall nové generace (next generation firewall, NGFW) | ANO |   |   |
| Podpora vysoké dostupnosti v režimu active-active i active-passive. Pokud tato funkce vyžaduje licenci, tak tato licence musí být součástí dodávky. | ANO |  |  |
| Zařízení musí být dodáno v režimu vysoké dostupnosti. Bez výpadkový cluster bude sestaven celkem ze 2 zařízení – součástí dodávky musí být obě zařízení včetně všech potřebných licencí. | ANO |  |  |
| Grafické konfigurační rozhraní (např. webový prohlížeč) a příkazový řádek bez omezení na počet administrátorů | ANO |   |   |
| Podpora virtuálních kontextů  | ANO |   |   |
| Podpora stavového firewallingu pro IPv4 i IPv6, podpora nat 64/46, plnohodnotná podpora IPv6 | ANO |   |   |
| Nasazení NGFW musí podporovat zapojení v režimech L2 (s virtuálním L3 rozhraním), L3, transparent a TAP Nasazení NGFW ve všech z následujících režimů (kombinace možné pomocí použití různých režimů pro různé virtuální kontexty): L2 bridge režim (inline), virtual wire (L2), L3 router/NAT režim (inline), explicitní proxy (inline/out of path), transparentní proxy (inline), reverzní proxy s loadbalancingem a healthcheck funkcí pro fyzické servery | ANO |   |   |
| Podpora režimu vysoké dostupnost, plnohodnotná správy z lokálního management rozhraní́ celého HA clusteru (správa celého clusteru probíhá z jednoho místa, konfigurace se automaticky sdílí), podpora možnosti centrální správy | ANO |   |   |
| Podpora tunelování provozu pomocí technologie GRE | ANO |   |   |
| **Požadavky na sítové funkce** | Podpora VLAN dle IEE 802.1Q | ANO |  |  |
| Podpora agregovaných interface (LACP) IEE802.3ad | ANO |  |  |
| Podpora redundantních rozhraní | ANO |  |  |
| Podpora loopback rozhraní | ANO |  |  |
| Možnost vytvořit switch nad několika fyzickými porty | ANO |  |  |
| Možnost práce se zónami (logická skupina sítových rozhraní zastoupená objektem v konfiguraci) | ANO |  |  |
| Podpora vytvoření tzv. wire pair pro L2 transparentní inspekci | ANO |  |  |
| Podpora dynamických směrovacích protokolů min v rozsahu: RIP, OSPF, BGP, IS-IS; podpora BFD | ANO |  |  |
| Podpora LLDP | ANO |  |  |
| Ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign On | ANO |  |  |
| Podpora lokální databáze a vzdálené databáze (radius, ldap, tacacs+, saml, kerberos) pro ověřování uživatelů | ANO |  |  |
| Ověřování uživatelů pomocí SSO funkcionality pomocí Radius Single Sign On a AD pollingu | ANO |  |  |
| Funkce QoS a traffic shaping min. ve variantě policing a queuing, aplikace politiky globálně nebo pomocí pravidel, podpora DSCP v pravidlech | ANO |  |  |
| Podpora funkcí VPN brány ‐ IPSec VPN (dle platných standardů pro možnost propojení se zařízeními třetích stran), SSL VPN (portálový režim bez klienta, tunelový režim s klientem), podpora funkce bezpečného vzdáleného přístupu do vnitřní sítě založeném na principu zero trust | ANO |  |  |
| Podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3  | ANO |  |  |
| **Požadavky na bezpečnostní funkce** | Antivirový engine musí být vybaven lokální databází vzorků škodlivého kódu a AI/ML enginem pro identifikaci podezřelých či neznámých vzorků | ANO |  |  |
| Funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (tzv. mobile malware), detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak) | ANO |  |  |
| Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 5000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace | ANO |  |  |
| Funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), výrobcem aktualizovaná a udržovaná databáze, vynikající pokrytí českého internetu; požadované akce – povolení stránky, logování stránky, brouzdání s proklikem, nutnost autentizace uživatele pro určitou kategorii, možnost definice časových kvót pro uživatele a kategorie webu | ANO |  |  |
| Funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů | ANO |  |  |
| Možnost blokovat sítový provoz na základě URL, kategorie webové stránky, IP adresy (rozsahu), GeoIP databáze, data a času | ANO |  |  |
| Analýza a zabezpečení DNS dotazů (ochrana před DNS poisoningem), filtrování DNS dotazů na základě kategorizace | ANO |  |  |
| Integrovaná funkce filtrování přenášených souborů pro protokoly CIFS, FTP, HTTP, IMAP, MAPI, POP3, SMTP a SSH; možnost konfigurace různého chování pro příchozí a odchozí směr, možnost práce s heslem chráněnými soubory, možnost logovat a blokovat provoz | ANO |  |  |
| Integrovaná funkcionalita pro ochranu publikovaných webových služeb proti sítovým útokům, možnost konfigurace ochrany proti útokům typu SQL injection, generické techniky, trojské koně, únik informací, známé zranitelnosti).  | ANO |  |  |
| Ochrana VoIP komunikace min. pro protokoly SIP a SCCP SIP ALG, inspekce SIP komunikace | ANO |  |  |
| **Licence** | Licence na 60 měsíců | ANO |   |   |
| **Záruky** | Minimální záruka režim 24x7 na 60 měsíců se zaručeným odesláním nového zařízení do konce následujícího pracovního dne od nahlášení závady | ANO |   |   |
| **Podpora** | Podpora, aktualizace SW a přístup k novým funckionalitám na dobu minimálně 60 měsíců | ANO |   |   |
| **SFP+ transceiver** | OEM SFP+ transceiver 10 Gbps, SM, LC duplex, 8 ks | ANO |  |  |
| **Optický kabel** | Optický patchcord, 9/125,LC-LC, SM, duplex, 2m 4ks | ANO |   |   |
| **Optický kabel** | Optický patchcord, 9/125,LC-LC, SM, duplex, 1m 4ks | ANO |   |   |

* 1. Hraniční směrovače (firewall) – perimetrové (detašovaná pracoviště)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kategorie vlastností** | **Požadovaný parametr nebo funkce** | **Požadovaná hodnota** | **Splnění požadovaných parametrů (ANO/NE)** | **Komentář** |
| **Typ a počet zařízení** | Hraniční směrovač (firewall), celkový počet: 2 kusů | ANO |  ANO | *Název dodávaného zařízení / označení (PN)* |
|  | min. počet nových spojení za sekundu  | 11 000 |   |   |
| min. počet současně navázaných TCP spojení  | 64 000 |   |   |
| min. propustnost funkce IPSEC VPN (při použití AES256, SHA256)  | 650 Mbps |   |   |
| min. propustnost funkce NGFW (stavový firewall + IPS, rozpoznávání aplikací na L7)  | 780 Mbps |   |   |
| min. počet metalických sítových rozhraní GE RJ45  | 5 |   |   |
| min. počet optických sítových rozhraní GE SFP  | 1 |   |   |
| konzolový port (sériová linka)  | 1 |   |   |
| USB port (bootstrap konfigurace, připojení externího LTE modemu)  | 1 |   |   |
| **Požadavky na obecné funkce** | Hardware řešení formátu desktop s možností montáže do racku | ANO |   |   |
| Konsolidované bezpečnostní řešení obecně značené jako firewall nové generace (next generation firewall, NGFW) | ANO |   |   |
| Grafické konfigurační rozhraní (např. webový prohlížeč) a příkazový řádek bez omezení na počet administrátorů | ANO |  |  |
| Podpora stavového firewallingu pro IPv4 i IPv6, podpora nat 64/46, plnohodnotná podpora IPv6 | ANO |   |   |
| Nasazení NGFW musí podporovat zapojení v režimech L2 (s virtuálním L3 rozhraním), L3, transparent a TAP  | ANO |   |   |
| Podpora režimu vysoké dostupnosti, plnohodnotné správy z lokálního management rozhraní́ celého HA clusteru (správa celého clusteru probíhá z jednoho místa, konfigurace se automaticky sdílí), podpora možnosti centrální správy | ANO |   |   |
| Podpora tunelování provozu pomocí technologie GRE | ANO |   |   |
| **Požadavky na sítové funkce** | Podpora VLAN dle IEE 802.1Q | ANO |  |  |
| Podpora agregovaných interface (LACP) IEE802.3ad | ANO |  |  |
| Podpora redundantních rozhraní | ANO |  |  |
| Podpora loopback rozhraní | ANO |  |  |
| Možnost vytvořit switch nad několika fyzickými porty | ANO |  |  |
| Možnost práce se zónami (logická skupina sítových rozhraní zastoupená objektem v konfiguraci) | ANO |  |  |
| Podpora vytvoření tzv. wire pair pro L2 transparentní inspekci | ANO |  |  |
| Podpora dynamických směrovacích protokolů min v rozsahu: RIP, OSPF, BGP, IS-IS; podpora BFD | ANO |  |  |
| Podpora LLDP | ANO |  |  |
| Ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign On | ANO |  |  |
| Podpora lokální databáze a vzdálené databáze (radius, ldap, tacacs+, saml, kerberos) pro ověřování uživatelů | ANO |  |  |
| Ověřování uživatelů pomocí SSO funkcionality pomocí Radius Single Sign On a AD pollingu | ANO |  |  |
| Funkce QoS a traffic shaping min. ve variantě policing a queuing, aplikace politiky globálně nebo pomocí pravidel, podpora DSCP v pravidlech | ANO |  |  |
| Podpora funkcí VPN brány ‐ IPSec VPN (dle platných standardů pro možnost propojení se zařízeními třetích stran) | ANO |  |  |
| Podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3  | ANO |  |  |
| **Požadavky na bezpečnostní funkce** | Antivirový engine musí být vybaven lokální databází vzorků škodlivého kódu a AI/ML enginem pro identifikaci podezřelých či neznámých vzorků | ANO |  |  |
| Funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (tzv. mobile malware), detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak) | ANO |  |  |
| Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 5000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace | ANO |  |  |
| Funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), výrobcem aktualizovaná a udržovaná databáze, vynikající pokrytí českého internetu; požadované akce – povolení stránky, logování stránky, brouzdání s proklikem, nutnost autentizace uživatele pro určitou kategorii | ANO |  |  |
| Funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů | ANO |  |  |
| Možnost blokovat sítový provoz na základě URL, kategorie webové stránky, IP adresy (rozsahu), GeoIP databáze, data a času | ANO |  |  |
| Podpora dvoufaktorové autentizace pomocí HW nebo mobilních OTP tokenů pro uživatele i administrátory | ANO |  |  |
| Analýza a zabezpečení DNS dotazů (ochrana před DNS poisoningem), filtrování DNS dotazů na základě kategorizace | ANO |  |  |
| Integrovaná funkce filtrování přenášených souborů pro protokoly CIFS, FTP, HTTP, IMAP, MAPI, POP3, SMTP a SSH; možnost konfigurace různého chování pro příchozí a odchozí směr, možnost práce s heslem chráněnými soubory, možnost logovat a blokovat provoz | ANO |  |  |
| Integrovaná funkcionalita pro ochranu publikovaných webových služeb proti sítovým útokům, možnost konfigurace ochrany proti útokům typu SQL injection, generické techniky, trojské koně, únik informací, známé zranitelnosti).  | ANO |  |  |
| Ochrana VoIP komunikace min. pro protokoly SIP a SCCP s podporou NAT46 a NAT64 SIP ALG, inspekce SIP komunikace, SIP pinholes, SIP over TLS, kontrola MSRP provozu | ANO |  |  |
| **Licence** | Licence na 60 měsíců | ANO |   |   |
| **Záruky** | Minimální záruka režim 24x7 na 60 měsíců se zaručeným odesláním nového zařízení do konce následujícího pracovního dne od nahlášení závady | ANO |   |   |
| **Podpora** | Podpora, aktualizace SW a přístup k novým funckionalitám na dobu minimálně 60 měsíců | ANO |   |   |

* 1. Software OTP token

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kategorie vlastností** | **Požadovaný parametr nebo funkce** | **Požadovaná hodnota** | **Splnění požadovaných parametrů (ANO/NE)** | **Komentář** |
| **Typ a počet zařízení** | Software aplikace pro generování jednorázových hesel, instalace a provoz v mobilním zařízeni, celkový počet: 10 kusů | ANO |   | *Název dodávaného zařízení / označení (PN)* |
|  | Podporované mobilní platformy iOS, Android, Windows 10 a 11 |  |  |  |
|  | Podpora push notifikací (tj. uživatel nemusí přepisovat jednorázové heslo, ale pouze v rámci push notifikace v aplikaci povolí přístup) |  |  |  |
|  | Možnost deaktivace tokenu ze strany administrátora bez přístupu ke koncovému zařízení, možnost převedení na jiného uživatele bez ztráty licence |  |  |  |
|  | Zabezpečeni pomocí PIN/otisku prstu |  |  |  |
|  | Ochrana před útoky typu brute force (tj. automatické deaktivace při překročení max. počtu neúspěšných pokusů) |  |  |  |
|  | Použití pro ověřování VPN uživatelů |  |  |  |

* 1. VPN klient

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kategorie vlastností** | **Požadovaný parametr nebo funkce** | **Požadovaná hodnota** | **Splnění požadovaných parametrů (ANO/NE)** | **Komentář** |
| **Typ a počet zařízení** | Platforma pro správu VPN klientů | ANO |   | *Název dodávaného zařízení / označení (PN)* |
|  | Řešení stejného výrobce jako firewall | ANO |  |  |
|  | Podpora klientských OS v rozsahu Windows, Mac, Linux, Android, IOS  | ANO |  |  |
|  | Podpora integrace s prostředím Active Directory | ANO |  |  |
|  | Funkce automatického připojení do VPN před přihlášení uživatele do Windows | ANO |  |  |
|  | SSL VPN funckionalita dostupná minimálně pro Windows, MAC, Android, IOS a Linux klienty  | ANO |  |  |
|  | IPsec VPN funkcionalita dostupná minimálně pro Windows, MAC a Android klienty | ANO |  |  |
|  | Předávání telemetrických informací z koncové stanice na firewall. Použití těchto informací pro aplikaci bezpečnostních politik na NGFW firewallu. | ANO |  |  |

* 1. Logovací server

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kategorie vlastností** | **Požadovaný parametr nebo funkce** | **Požadovaná hodnota** | **Splnění požadovaných parametrů (ANO/NE)** | **Komentář** |
| **Typ a počet zařízení** | Logovací server Virtuální appliance s podporou minimálně VMware, KVM a Hyper-V | ANO |   | *Název dodávaného zařízení / označení (PN)* |
|  | Minimální limit pro množství přijatých logů za jeden den 10 GB | ANO |  |  |
|  | Řešení stejného výrobce jako firewall | ANO |  |  |
|  | Podpora Syslog formátu | ANO |  |  |
|  | Funkce zpětné kontroly logů  | ANO |  |  |
|  | Podpora reportů nad logy ve formátu CSV/XML/PDF | ANO |  |  |
|  | Možnost vytváření vlastních reportů na základě konkrétních SELECT dotazů do databáze | ANO |  |  |
|  | Podpora SNMPv2, SNMPv3 | ANO |  |  |
|  | Podpora REST API | ANO |  |  |
|  | Správa přes webové rozhraní HTTPS | ANO |  |  |
|  | Administrátorské účty musí být možné konfigurovat lokálně nebo na vzdáleném serveru (LDAP, RADIUS, Tacacs\*) | ANO |  |  |
|  | Možnost zašifrováni spojení mezi zařízeními, které odesílá logy a analyzačním nástrojem, který je předmětem této zadávací dokumentace | ANO |  |  |

1. DALŠÍ SLUŽBY
	1. Projektové řízení

Zadavatel požaduje zajištění projektového vedení realizace předmětu plnění. Dodavatel zajistí projektové vedení po celou dobu realizace zakázky. Dodavatel zajistí:

* 1. Projektové vedení plnění předmětu plnění po celou dobu realizace dodávky prostřednictvím projektového manažera, který bude v průběhu plnění aktivně a konstruktivně komunikovat se jmenovaným zástupcem zadavatele;
	2. proaktivní vyžádání si součinnosti a koordinace prací, služeb a/nebo dodávek třetích stran (zejm. stávajících dodavatelů zadavatele) zapojených do plnění za účelem dosažení úspěšné realizace předmětu plnění veřejné zakázky jako celku a jeho úspěšné realizace v daném časovém rámci vč. jednotlivého oprávněného konkrétního úkolu s určeným termínem z kontrolního dne v rámci koordinace prací, služeb a/nebo dodávek;
	3. organizaci kontrolních dnů – kontrolní dny se budou konat za účasti zástupců dodavatele a zadavatele min. 1 x 14 dní; dodavatel zajistí řízení všech kontrolních dnů a dílčích jednání se členy realizačního týmu na straně zadavatele;
	4. zpracování harmonogramu prací v podobě navazujících činností, např. formou Ganttova diagramu nebo MS Project, či obdobného nástroje postihujícího návaznosti ke všem částem plnění;
	5. řízení vzniku veškeré provozně-technické dokumentace, školících materiálů pro školení administrátorů, organizace školení samotného a další projektové dokumentace;
	6. veškeré řídící činnosti projektu s vlastníky projektu na straně zadavatele nebo jím určených třetích stran na straně dodavatele.
	7. Školení

Zadavatel v rámci dodávky požaduje proškolení 3 správců v rozsahu nezbytném pro zajištění standardního provozu a správy dodaných segmentačních firewallů, min. však v délce 16 hodin.

* 1. Rozsah implementace

Náklady na provedení instalačních a implementačních prací musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují a nelze je vyčíslit zvlášť.

Zadavatel požaduje provedení prací minimálně v níže uvedeném rozsahu.

* Doprava veškerého hardware do místa instalace, sídla zadavatele.
* Instalace a nastavení HW a software bude provedeno dodavatelem v produkčním prostředí v prostorách zadavatele.
* Asistence při přípravě a konfiguraci firewallů
* Migrace a optimalizace stávajících pravidel pro interní provoz
* Přítomnost kvalifikovaného pracovníka dodavatele v místě instalace při nasazení segmentačních firewallů do ostrého provozu.
	1. Testovací provoz (akceptační testy)

Zhotovitel v rámci realizace předmětu smlouvy vypracuje návrh testovacích postupů pro ověření funkčnosti díla a vypracuje jednotlivé akceptační protokoly. Návrh testovacích postupů bude předložen objednateli a po jeho schválení bude objednatelem akceptován.

Testovací postupy se musí týkat minimálně těchto oblastí:

* vysoká dostupnost (HA),
* síťová pravidla, NAT,
* bezpečnostní funkce (IPS, analýza aplikací, ochrana před škodlivým kódem),
* dohled a napojení na SIEM (SNMP, syslog),
* výkonnostní parametry.

**Funkční testy**

Funkční testy ověří, že implementované řešení poskytuje bezchybně všechny požadované funkcionality uvedené v Technické specifikaci.

Testovací provoz bude probíhat v sídle objednatele minimálně v délce 30 dní.

* 1. Požadavky na dokumentaci

**Dodavatel zpracuje komplexní a detailní řešení nasazení díla**, a to ve vazbě na požadavky uvedené v této technické dokumentaci. Cílem je zpracování dokumentu v takové míře detailu jednotlivých postupů a prací zasazení do prostředí a jeho nastavení, která umožní dosažení zavedení řešení do rutinního provozu řízenou formou. Dokument proto bude jednoznačně a jasně konkretizovat jednotlivé kroky prací a to min. v rozsahu, které kroky a jakým způsobem budou řešeny, kým budou řešeny, za jaké součinnosti objednatele a v jakém čase. Taková konkretizace bude dále dodržovat časovou, věcnou a logickou souslednost a bude z ní tedy možné v každém okamžiku realizace jednotlivých částí díla určit, co je právě realizováno a v jakém stavu a co bude následovat.

Objednatel bude moci na základě takových podkladů alokovat své potřebné kapacity na součinnost a průběžnou kontrolu plnění díla. Bez odsouhlasené prováděcí dokumentace ze strany objednatele, tedy shody objednatele a zhotovitele na způsobu a formě nasazení jednotlivých částí díla nebude moci být započata implementace.

**Dodavatel zpracuje provozně-technickou dokumentaci v rozsahu** dokumentace skutečného provedení a provozní dokumentace.

Dokumentace skutečného provedení musí obsahovat minimálně tyto části:

* detailní popis cílového stavu včetně popisu funkcionalit jednotlivých HW a SW částí systému;
* výkresovou dokumentaci;
* seznam dodaného hardware, jeho produktových čísel a dalších podrobností (např. sériových čísel, MAC adres, IP adres a umístění apod.);
* seznam všech zařízení, rozhraní a jejich MAC adres a k nim odpovídajících IP adres použitých v nové infrastruktuře;
* detailní popis zajištění bezpečnosti informací;
* detailní popis designu řešení a jeho konfigurace;
* vazby na stávající infastrukturu a/nebo systémy a jejich konfigurace.

**Provozní dokumentace bude obsahovat instrukce a postupy pro administrátory a bezpečnostní správce zařízení.**

**Dodavatel dále zpracuje projektovou dokumentaci v rozsahu odpovídajícím předmětu plnění, zejména pak zápisy z kontrolních dnů a projektových porad a další odpovídající podklady nebo dokumenty související s plněním a dodáním předmětu plnění.**

* 1. Záruka, podpora a servis

Záruka min. 60 měsíců na HW zařízení a na veškerý SW, který je neoddělitelnou součástí HW zařízení, včetně práva na nové verze.

2 x ročně profylaktická / konzultační kontrola v délce 4 hodin na dodané řešení po dobu min. 60 měsíců (konzultace nastavení, aktualizace).

Standardní záruční podpora min. v délce 60 měsíců za jakost od instalace a zprovoznění díla jako celku, tj. aktualizace programového a technického vybavení (Update Service, maintenance) – např. předání nových verzí SW modulů programového vybavení s vylepšenými funkcemi tak, jak je výrobce dává k dispozici, řešení vad apod.

| **ZÁKLADNÍ SERVISNÍ PODPORA provozu HW** |
| --- |
| **Kategorie incidentu** | **Příjem hlášení** | **Servisní garance** |
| **Zahájení řešení** | **Servisní výjezd** |
| Haváriepřerušení provozu | HelpDesk – 24x7 | Neprodleně, nejpozději do 120 minut.v rámci pracovní doby tj. od 8:00 do 16:00. | Nejpozději **druhý následující pracovní den** nebo při příjmu hlášení v pracovní den do 10:00 nejpozději následující pracovní den |
| Významná závada významné omezení provozu | Nejpozději druhý následující pracovní den | Nejpozději pátý následující pracovní den |
| **Závada, chyba** – menší omezení provozu | Nesjednán | Nesjednán |

| **ZÁKLADNÍ SERVISNÍ PODPORA provozu SW** |
| --- |
| **Kategorie vad SW** | **Příjem hlášení** | **Servisní garance** |
| **Zahájení řešení** | **Servisní výjezd** |
| Havárie – A | HelpDesk – 24x7 | Do 24 hodin po oznámení chybyv rámci pracovní doby tj. od 8:00 do 16:00. | Nesjednán |
| Významná závada – B | Do 48 hodin po oznámení chybyv rámci pracovní doby tj. od 8:00 do 16:00. | Nesjednán |
| Závada, chyba – C | Do 120 hodin po oznámení chybyv rámci pracovní doby tj. od 8:00 do 16:00. | Nesjednán |

Pro kategorizaci vad SW či jakéhokoliv jiného software platí následující pravidla:

(A) Chyba, která:

1. znemožňuje užívání SW systému jako celku;
2. nebo znemožňuje užívání části SW systému, přičemž nemožnost užívání takové části SW systému může mít významný vliv na řádné zabezpečení běžné činnosti Objednatele a nelze jí schůdně překonat či obejít; nebo jí lze překonat či obejít pouze za cenu pro Objednatele vážných obtíží.

(B) Chyba, která nebrání v užívání SW systému ani jeho dílčích částí, neboť jí lze schůdně překonat či obejít, aniž by tím vznikaly pro Objednatele vážné obtíže.

(C) Chyba, která nebrání v užívání SW systému ani jeho dílčích částí a lze jí bez problémů překonat či obejít.

Zhotovitel zahájí odstraňování chyb SW oznámených v souladu s výše uvedenými pravidly:

1. pro chyby kategorie (A) do 24 hodin po oznámení chyby, odstraňování chyb bude prováděno v pracovní dny (tj. pondělí až pátek) v době od 08:00 do 16:00);
2. Pro chyby kategorie (B) do 48 hodin po oznámení chyby, odstraňování chyb bude prováděno v pracovní dny (tj. pondělí až pátek) v době od 08:00 do 16:00);
3. Pro chyby kategorie (C) do 120 hodin po oznámení chyby, odstraňování chyb bude prováděno v pracovní dny (tj. pondělí až pátek) v době od 08:00 do 16:00).

Termín odstranění závad SW si zhotovitel dohodne po analýze problému s objednatelem pro každou chybu prostřednictví e-mailu.

* 1. Licence

Řešení musí zahrnovat v ceně dodávky všechny náklady na provoz řešení, tedy včetně licence na operační systémy pro nabízené řešení, databázi, middleware apod.

1. POIMPLEMENTAČNÍ PODPORA

Zadavatel požaduje poskytnutí poimplementační technické podpory dodaného řešení proškoleným zaměstnancům zadavatele (administrátorům). Podpora bude využita zejména pro potřeby následného provozu a správy dodaných technologií a dodaného řešení.

* Požadovaný rozsah technické podpory – 8 hodin po dobu 1 měsíce od finální akceptace dodaného řešení.
* Technická podpora může být poskytována i vzdáleně (např. MS Teams) nebo telefonicky.
* Technická podpora bude dostupná v pracovní době od 8:00 do 16:00.
* Podpora bude poskytována technickým specialistou, který byl součástí realizačního týmu, případně technickým specialistou odpovídající kvalifikace.

Požadavek na podporu bude možné zadat prostřednictvím helpdeskového systému dodavatele nebo e-mailem, příp. telefonicky.

1. HARMONOGRAM

Zadavatel vyžaduje dodržení následujícího harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro realizaci dodávky. Údaj D značí datum nabytí účinnosti Smlouvy o dílo. Čísla značí počet kalendářních dnů.

| **Aktivita** | **Začátek** | **Termín splnění** |
| --- | --- | --- |
| Nabytí účinnosti smlouvy | D | D |
| Zahájení projektu – úvodní projektová schůzka | D | D+7 |
| Předimplementační analýza – zpracování | D+7 | D+17 |
| Předimplementační analýza – připomínkové řízení, schválení | D+17 | D+24 |
| Prováděcí dokumentace – zpracování | D+24 | D+34 |
| Prováděcí dokumentace – připomínkové řízení, schválení | D+34 | D+40 |
| Realizace předmětu plnění | D+40 | D+125 |
| Školení administrátorů | D+40 | D+135 |
| Testovací provoz | D+135 | D+165 |
| Akceptační testy | D+165 | D+180 |
| Zahájení ostrého provozu | D+181 |  - |

Dodavatel může dle svého uvážení výše uvedené maximální lhůty trvání zkrátit při dodržení všech částí předmětu plnění a bez snížení kvality dodávaných služeb.

Maximální lhůty trvání nesmí dodavatel při tvorbě detailního harmonogramu prodloužit.

**Detailní harmonogram plnění uvede dodavatel ve své nabídce.**

**Dodavatel uvede ve své nabídce (jako součást harmonogramu) požadovanou součinnost zadavatele pro splnění harmonogramu plnění.**