Název dokumentu	**Změna zadávací dokumentace na základě jednání s účastníky č. 2**
Zadavatel	**RegioJet a.s.** (dále jen „**Zadavatel**“) IČO: 28333187 se sídlem náměstí Svobody 86/17, Brno-město, 602 00 Brno zapsaný v obchodním rejstříku vedeném u Krajského soudu v Brně, oddílu B, vložce 5816
Název zakázky	**Zajištění síťové a aplikační bezpečnosti**
Identifikace zadávacího řízení	nadlimitní veřejná zakázka na služby zadávaná v jednacím řízení s uveřejněním dle § 60 a násl. ZZVZ
Evidenční číslo zakázky ve Věstníku veřejných zakázek	Z2025-071588
Číslo oznámení v Úředním věstníku Evropské unie	856080-2025

(dále jen **„Veřejná zakázka“** nebo **„Zadávací řízení“**)

Zadavatel v souladu s ust. § 61 odst. 11 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších (dál jen „**ZZVZ**“) realizuje změnu zadávací dokumentace na základě proběhlých jednání s účastníky a o této změně informuje.

1. **Změna zadávacích podmínek**
   1.1. **Příloha č. 2 ZD – Technická specifikace (dále jen „Technická specifikace“)**

      1.1.1. **Kapitola: e) WAF se mění, co do rozsahu požadavků následovně:**
      Požadavek č. se mění tak, že nově zní:

Nasazení SW zařízení ve funkci load-balancer s podporou autentizace uživatelů, SSL akcelerátoru a webového aplikačního firewallu.

2. **Závěr**

Zadavatel vyzývá účastníky, aby provedené změny zohlednili ve svých nabídkách. Výzva k podání nabídek bude provedena samostatnou výzvou.

Příloha č. 1 Technická specifikace ve znění změny ze dne 10. 3. 2026

V Praze dne dle elektronického podpisu

Ing. Jakub Skopal

Digitálně podepsal Ing. Jakub Skopal
DN: c=CZ, 2.5.4.97=NTRCZ-28333187, o=RegioJet a.s., ou=IT, ou=1, cn=Ing. Jakub Skopal, sn=Skopal, givenName=Jakub, serialNumber=P917713
Datum: 2026.03.10 16:05:52 +01'00'

Ing. Jakub Skopal

ředitel IT infrastruktury

a) Ochrana koncových stanic – technické parametry

Klíčové požadované funkcionality:

- Modulární architektura s možností postupného rozšiřování.
- Integrace s dalšími nástroji bezpečnostního ekosystému (SIEM, NDR apod.).
- Samostatný AV engine nezávislý na OS.
- Nízké nároky na výkon koncového zařízení.
- Centralizovaná správa politik a nastavení.
- Detekce známých i neznámých hrozeb pomocí heuristiky a strojového učení.
- Ochrana proti ransomwaru, zero-day hrozbám a útokům bez souboru (fileless).
- Monitoring procesů, skriptů, registrů a síťových spojení.
- Možnost izolace napadené stanice z prostředí.
- Vzdálený zásah a sběr forenzních dat.
- Reporting, notifikace a integrace do širšího SOC ekosystému.
- Dodávka bude realizovaná pro 1000 koncových stanic (OS Win/macOS/Linux) a pro 800 mobilních zařízení (OS Android/iOS)
- Součástí předmětu plnění musí být standardní záruka výrobce v délce trvání 60 měsíců, poskytovaná bez dalších poplatků.

Požadavek	Parametr / funkcionalita	Odpověď respondenta	Odkaz pro důkaz/další informace
1	Řešení musí být postaveno na modulární architektuře, která umožní zapnutí jednotlivých komponent ochrany		
2	Řešení musí umožňovat integraci s dalšími bezpečnostními systémy prostřednictvím dokumentovaného API.		
3	Řešení musí podporovat FDE, tzn. Šifrování lokálních disků a vyměnitelných medií		
4	Řešení na koncových stanicích nesmí vyžadovat lokální administrátorská práva ke spuštění		
5	Koncoví uživatelé nesmí mít možnost ovládat a měnit nastavení klienta nebo zásad zabezpečení		
6	Řešení musí mít zabudované kontroly/ochrany, které zabrání koncovým uživatelům provádět změny (odinstalace agenta, zastavit/spustit agenta nebo související služby)		

7	Řešení musí být schopné detekovat a odstranit viry, spyware a další malware na základě kombinace signatur, blokátorů chování a heuristické analýzy		
8	Řešení musí být schopné detekovat a identifikovat přítomnost virů v paměti systému, bootovacích sektorech, tabulkách oddílů a na všech formách dat uložených na pevném disku systému a jiných vyměnitelných médiích		
9	Řešení musí být schopné detekovat a zablokovat pokus o infekci známým malwarem		
10	Řešení musí informovat uživatele o pokusu infekce malwarem		
11	Řešení musí být schopné detekovat, identifikovat, blokovat a odstranit škodlivé aplikace v reálném čase. Skenování virů s minimálním dopadem na výkon koncové stanice		
12	Uživatel má možnost provést AV kontrolu určitých jednotek, adresářů nebo souborů		
13	Řešení musí být schopné provést nápravná opatření k odstranění virového kódu z infikovaných souborů, zaváděcích sektorů nebo tabulek oddílů		
14	Řešení musí být schopné přesunout neopravený soubor infikovaný virem do karantény na místním pevném disku pro další kontrolu nebo akci		
15	Řešení musí být schopné provést karanténu souborů / procesů		
16	Řešení musí být schopné skenovat nejpopulárnější soubory a přílohy (dokumenty Microsoft Office, komprimované soubory a grafické soubory…)		
17	Řešení musí být schopné automaticky identifikovat vstupní bod malwaru		
18	Řešení musí být odolné proti "evasion" technikám moderního malwaru		
19	Řešení podporuje technologii Content disarm and reconstruction (CDR) – proaktivní extrakce		

	potencionálně škodlivého obsahu, min podpora grafických souborů, MS Office a pdf		
20	Řešení blokuje útoky bez ohledu na to, zda jsou to webové, e-mailové, nebo z vyměnitelného média		
21	Řešení detekuje a blokuje „Command & Control“ komunikaci a schopné rozpoznat post infekční komunikaci s řídícím centrem malware		
22	Řešení musí být schopné detekovat zero-day útoky, detekcí a odesláním podezřelých souborů do prostředí sandboxu (cloud prostředí nebo lokální emulace)		
23	Řešení podporuje emulaci spustitelných souborů, archivů, dokumentů, Java a flash souborů		
24	Možnost emulovat soubory větší než 20 MB všech souborových typů		
25	Řešení chrání proti ransomware		
26	Řešení musí být schopné obnovit soubory při pokusu o zašifrování včetně automatické remediace systému		
27	Řešení musí být schopné blokovat a zadržet soubor před rozšířením na všechny koncové body		
28	Řešení musí být schopné automaticky vygenerovat forenzní zprávu o provedení útoku		
29	Řešení využívá detekci chování a technologie strojového učení pro detekci nových variant malwaru		
30	Řešení musí být schopné ověřit integritu updatu virových signatur před jeho aplikací		
31	Řešení musí být schopné ukládat data do hostitelského zařízení bez přídavného nebo externího zařízení		
32	Forenzní údaje shromážděné řešením jsou uloženy lokálně na samotném koncovém bodě. Uložená data jsou chráněna před neoprávněným přístupem nebo narušením struktury		

33	Řešení shromažďuje probíhající informace o činnosti operačního systému. Shromážděné informace zahrnují procesní činnost, síťovou komunikaci, změny v registru, přístup k souborovým systémům		
34	Možnost pozdržet download ve webovém prohlížeči		
35	Podporované Internetové prohlížeče MS Edge, Google Chrome, Firefox		
36	Klientský software s integrovanou funkci IPSec VPN kompatibilní s VPN koncentrátorem		
37	Podpora "Split tunnelling" (tj. možnost přístupu k Internetu mimo VPN)		
38	Podpora připojení VPN v prostředí za NAT zařízeními a bránami firewall, které neumožňují IPSec provoz (možnost tuneloval VPN přes HTTPS)		
39	Podpora připojení v „hotspot“ prostředí (agent dočasně umožní přístup k captive portálu)		
40	Podpora ověřování VPN pomocí uživatelského jména/hesla, klientského certifikátu, LDAP/AD		
41	Podpora multi-faktorové autentizace VPN		
42	Podpora OS koncových stanic min Windows 7 SP1 (32-bit a 64-bit), Windows 10 (32-bit a 64-bit), Windows 11, Windows 2016, Windows 2019, MAC OS 11/12, Debian 10/11, Ubuntu 20/21/22		
43	Podpora integrace s AD		
44	Centrální správa bezpečnostních pravidel a nastavení koncových klientů		
45	Centrální ukládaní logů		
46	Komunikace mezi management serverem a koncovým klientem musí být autentizovaná a šifrovaná		
47	Koncovým klient musí být schopen získat aktualizace signatur virů z centrálního management serveru i z internetu		

48	Výrobce řešení poskytuje aktualizované signatury. Nové signatury by měly být zpřístupněny alespoň jednou denně		
49	Řešení umožňuje vytvořit a spravovat logické skupiny napříč několika funkčními (AD) skupinami		
50	Umožňuje administrátorovi řídit politiku na úrovni uživatele a skupiny		
51	Kontrola bezpečnostního stavu připojované stanice na úrovni předepsaných politik a možnost ověřit „compliance klienta“ (verze OS, název a verze antiviru, apod.)		
52	Dashboard poskytuje možnost zobrazení všech souvisejících událostí		
53	Namapováni škodlivé/podezřelé aktivity podle kategorie použité techniky na MITRE ATTACK matici		
54	Možnost vyhledat infikované stanice podle zvoleného IOC (Indicator of Compromise)		
55	Možnost vyhledávat jednotlivá IOC přes všechny koncové stanice		
56	Možnost spuštění automatické analýzy z detekce incidentu síťového bezpečnostního prvku		
57	Schopnost karantény nebo izolování celého počítače		
58	Možnost generovat agregovaný report, který obsahuje data o koncových bodech a síťová data		
59	Schopnost automaticky generovat podrobný forenzní report z detekovaných incidentů		
60	Automatický report rozsahu vniknutí škodlivého softwaru		
61	Reporty obsahují seznam zasažených souborů/dat v případě útoku		
62	Možnost stažení reportů uživatelem i administrátorem		
63	Řešení poskytuje úplný stromový přehled událostí a útoků		

64	Řešení umožňuje automatizovanou analýzu událostí		
65	Spouštění automatické analýzy od incidentů produktů třetích stran		
66	Zobrazení reputace souboru ve forenzní zprávě		
67	Možnost integrace se SIEM, SOAR		

Ochrana mobilních stanic:

Dodávka bude realizovaná pro 800 koncových zařízení (OS Android/iOS)

Požadavek	Parametr / funkcionalita	Odpověď respondenta	Odkaz pro důkaz/další informace
1	Detekce mobilního malwaru		
2	Řešení musí být schopné chránit proti hrozbám v síťové komunikaci (například SSL stripping, MiTM = Man in the middle apod.)		
3	Řešení musí být schopné chránit před útoky na integritu mobilních operačních systémů		
4	Řešení musí být schopné chránit před známými a neznámými škodlivými aplikacemi		
5	Zahrnuje centrální správu a sledování stavu všech spravovaných zařízení a analýzu rizika používaných mobilních aplikací		
6	Možnost vytvářet white a black listing mobilních aplikací		
7	Detekce „rooting“ a „jailbraking“ zařízení		
8	Uživatel nemůže změnit konfiguraci aplikace		
9	Řešení nesbírá a nevyužívá žádná privátní uživatelská data (zprávy, emaily, lokace, kontakty, historie…)		
10	Možnost blokovat přístup na nevhodné stránky (URL filtering) podle kategorizace stránek		
11	Řešení musí být schopné detekovat phishing nejen na základě reputace IP/URL, ale také na základě analýzy obsahu stránky		

12	Možnost integrace s MDM / EMM systémy třetích stran.		
13	Podpora zařízení typu BYOD a firemních zařízení		
14	Podpora OS Android a iOS		
15	Klient je dostupný v oficiálních obchodech Apple AppStore/Google Play store		

b) DDoS – požadavky a technické parametry

Klíčové požadované funkcionality

DDoS ochrana zajistí:

- Detekci a mitigace DDoS útoků:
    - Síťových floodů
    - Aplikačních floodů (především pak SSL floodů a to i bez nutnosti poskytnout klíč a certifikát)
    - Efektivní ochrana před známými zranitelností serverů i známými DDoS nástroji pomocí signatur. Možnost využití GEO lokace. Ochrana před známými útočníky pomocí specializované IP reputační databáze zaměřené na aktivní DDoS útočníky, botnety, TOR exity, skenery atd.
    - Průzkumných útoků (horizontální a vertikální scanning)
    - Možnost importu vlastních ACL
    - Volumetrické DDoS útoky (možnost využití globální sítě scrubingových center s kapacitou 30 Tbps.
- Pravidelné reporty
- Integraci s dalšími bezpečnostními řešeními (především pak SIEM)
- Online přístup k monitoringu
- Součástí předmětu plnění musí být standardní záruka výrobce v délce trvání 60 měsíců, poskytovaná bez dalších poplatků.

Požadavek	Popis	Odpověď respondenta	Odkaz pro důkaz/další informace
	Hardware		

1	Licenční model založený na legitimním provozu (s možností navýšit tuto kapacitu SW klíčem)		
2	Síťová rozhraní: 4 x 10 GE SR (možnost do budoucna rozšířit o dalších x 1G UTP nebo 4 x 10 GE LR)		
3	Kapacita mitigace DDOS útoku: 20Gbps		
4	Propustnost legitimního provozu - 5 Gbps (možnost navýšení kapacity pomocí SW klíče na 10 Gbps)		
5	Hardwarová SSL karta, min. CPS 40 K CPS (RSA 2K)		
6	Zpoždění < 60 µs (microseconds)		
7	Provedení to 19' racku (max. 1U)		
8	Redundantní napájení (hot swap)		
9	Zabudovaný interní bypass pro UTP i optické porty(v případě poruchy nebo vypnutí boxu bude provoz stále procházet). S možností vypnout/zapnout bypass z konfigurace boxu.		
	Síťové požadavky		
10	Plná podpora IPv6 / IPv4 (pro klasifikaci, pro management i směrování)		
11	VLAN (802.1Q)		
12	Podpora enkapsulace VLAN, MPLS, L2TP, GRE, GTP, IP-in-IP		
13	Nasazení v transparentním režimu (L2, tj. bez IP na inspekčních portech)		
14	Nasazení v L3 módu (s podporou BGP, GRE)		
15	Dedikované management porty (musí být jiný než inspekční port), min. 2		

	Management		
16	Centrální management, reporting, monitoring ve formě virtuálu (VMWare, KVM).		
17	Možnost vygenerovat report pro konkrétní útok (podle zdroje, cíle, podle času, způsobu mitigace atd.) a to včetně vzorků paketů (pcap)		
18	Možnost vytvořit plánované reporty (např týdní, měsíční) a jejich zasílání mailem		
19	RBAC (Role based access control) s granularitou až na úroveň jednotlivých pravidel		
20	Možnost definovat alerty (např. na základě velikosti útoků, trvání útoku apod.) a jejich zasílání mailem		
21	Podpora SSH		
22	Podpora REST API		
23	Podpora SNMP v1/2/3		
24	Podpora SNMP trap		
25	Mail (např.pro zasílání alertů)		
26	Podpora SYSLOG		
27	Podpora NTP		
28	Autentizace uživatele:		
	- RADIUS		
	- TACACS+		
	- LDAP		
29	Do budoucna možnost integrace s detektory (i jiných výrobců) na bázi neflow		
	Bezpečnost a moduly ochrany		
30	Modul založený na behaviorální analýze (NBA - network behavioral analysis). Schopnost naučit se úrovně legitimního provozu a detekovat DDOS útoky na základě		

	odchylek v provozu (bandwith, pps) a zároveň "rate invariant" charakteristik		
31	IPS - Intrusion Prevention system (dektece a blokování na základě signatur)		
32	IP reputace (zaměřena na DDoS, web útočníky, scannery, TOR exity)		
33	Ochrana před floody (SYN, ICMP, TCP, UDP, UDP fragemented, IGMP)		
34	PPS (packet per second) nastavení per pravidlo		
35	Omezení počtu nově navazovaných spojení (CPS - connection per second) - per zdroj, per cíl, per zdroj a cíl		
36	Omezení počtu aktivních spojení (CEC - Concurrent established connections) nastavení		
37	Paketová anomálie (min. Incorrect IPv4 Checksum, Invalid IPv4 Header, Inconsistent IPv6 Headers, Invalid TCP Flags, stejná zdrojová a cílová adresa)		
38	ACL - access control list		
39	Blokování na základě zdroje (IP) tzv. block list		
40	Možnost nastavit výjimku pro konkrétní zdroj (IP), kdy nebude monitorován/blokován bezpečnostní moduly (allow list)		
41	Možnost konfigurovat pravidla s individuálním bezpečnostním nastavením		
42	GEO pravidla		
43	Možnosti blokování - zahození paketů (drop), reset (zdroj, cíl, zdroj i cíl), suspend (zdrojové IP, zdrojový port, cílová IP, cílový port a libovolná		

	kombinace), challenge-response pro TCP, HTTP a DNS		
44	Detekce a mitigace v plně automatickém módu bez nutnosti manuálního zásahu		
	IPS - Intrusion Prevention system		
45	Signatury (s updatem min. jednou týdně)		
46	Detekce Anomálií		
47	Možnost definovat vlastní signatury		
	NBA - network behavioral analysis		
48	Detekce a blokování vertikálního a horizontálního scanningu		
49	Detekce a blokování útoků typu "brute force" tj. útoků na prolomení přihlášení		
50	Detekce a blokování neznámých útoků (zero day)		
51	Schopnost detekovat a blokovat šíření škodlivého software (malware) ve fázi šíření na úrovní sítě		
52	Čistění útoků na základě dynamických paketových signatur vytvářených během útoků s L3 až L7 parametry		
53	Behaviorální analýza (NBA - network behavioral analysis) pro L3/L4 útoky i pro L7 (DNS, HTTPS,…)		
54	Ochrana před "pulzními" útoky (tzv. burst attacks), kdy útočník opakuje útok v náhodných intervalech a to i při měnících se vektorech útoku		
55	Detekce a mitigace HTTPS floodů pomocí behaviorální analýzy a bez nutnosti dešifrování provozu, a to i v případě asymetrického provozu		

56	Detekce a mitigace HTTPS floodů pomocí dešifrování pouze prvního požadavku a vložení challenge (302, JS) a to i v případě asymetrického provozu		
57	Detekce a mitigace HTTPS flood na základě plné dekrypce provozu		
58	Podpora TLS fingerprintingu pro mitigaci HTTPS útoky		
59	Ochrana před útoky na DNS podle vektorů: • Random domain flood (NXDomain, water torture atd.) • NS challenge pro floody z podvržených (spoofed) zdrojů • Anti-poisoning FQDN learning mechanism • Podpora zone transfer		
60	Ochrana před DNS watertorture útoky (dotazy na náhodné, neexistující jména subdomén) pomocí automatického učení se jmen existujících jmen subdomén		
61	Ochrana před DNS watertorture útoky (dotazy na náhodné, neexistující jména subdomén) pomocí manuálního importu extujích jmen subdomén		
62	Ochrana před DNS watertorture útoky (dotazy na náhodné, neexistující jména subdomén) na základě synchronizace s DNS (zone transfer)		
	DoS and DDoS protection		
63	Detekce a blokování ICMP floodů		
64	Detekce a blokování IGMP floodů		
65	Detekce a blokování TCP - tj. SYN, SYN ACK, FIN, RESET (včetně útoků z podržených IP adres (IP-spoofing)) pomocí behaviorální analýzy a generovaní dynamických paketových signatur		

66	Detekce a blokování UDP i UDP fragment floodů na základě automatického učení a adaptivních filtrů		
67	Detekce a blokování paketů nenáležících žádnému spojení (tyv. out of state)		
68	Detekce a blokace DDoS útoků na zákldě challenge / response metody. Min. podpora SYN-cookies, L7 chalenges (HTTP 302, JAVA script, DNS)		
69	Detekce a blokování útoků typu "carpet bombing"		
	ACL - access control list		
70	Block list		
	Allow list		
	Filtrování provozu na základě VLANů, IP, L4 (např. TCP/UDP proty), L7 parametry (např. HTTP "User agent")		
	Podpora výrobce		
71	Updaty signatur		
72	Updaty IP reputace (minimálně v kategoriích DDoS útočníci, botnety, web útočníci, scannery, TOR exity)		
73	Updaty TLS fingerprintů		
74	Updaty ASN		
75	Online podpora výrobce během útoků při mitigaci ve scrubbingových centrech.		
	Topologie, nasazení		
76	V cestě (Transparentní / L2)		
77	Out of path (na TAPu/SPAN portu)		
78	Možnost kombinovat obě možnosti (v cestě/out of path) současně		
79	L3 mód (s podporou BGP / GRE)		

80	Možnost rozšít v budoucnu o podpora BGP Flowspec (pro přesměrování i pro mitiaci)		
81	Možnost přepínat jednotlivá pravidla do "reporty only" a "block and report" módu		
82	Možnost definovat min. 50 pravidel (per subnet, per VLAN)		
83	Možnost nasadit i jako virtuální appliance (VMWare, KVM, Hyper-V)		
84	Může fungovat i za CDN		
	Scrubingová centra (možnost mitigace pomocí služby výrobce)		
85	scrubingová centra výrobce řešení (tj. jeden výrobce pro onpremise HW a pro službu)		
86	Dedikovaná kapacita pro DDOS mitigaci 30 Tbps (nelze uvádět kapacitu jiných služeb (např. CDN))		
87	Žádné omezení na velikost útoku		
88	Propustnost legitimního (vyčištěného) provozu - 1 Gbps (v příchozím směru) s možností navyšovat v kroku 100 Mbps		
89	Počet chráněných subnetů minimálně 4		
90	Uveďte počet a seznam scrubningových center		
91	Služba obsahuje minimálně tyto KPI: Time to detect, time to alert, time to divert, time to mitigate, consistency of mittigation, availability.		
92	Je možné kombinovat služby typu: On Demand (přesměrování během útoku, detekce pomocí netflow), Always On (trvalé přesměrování), Hybrid (detekce a mitigace do velikosti lokální linky pomocí on premise boxu a přesměrování jen pro volumetrické útoky)		

93	Minimálně 2 scrubingová centra na území EU		
94	Možnosti přesměrování: BGP, DNS		
95	Podpora výrobce během útoku v ceně služby (s garantovaným response time)		
	Certifikace a audity služby		
96	Splňující ISO 22301		
97	Splňující ISO 27001		
98	Splňující ISO 27701		
99	Splňující ISO 27017		
100	Splňující ISO 27018		
101	Splňující ISO 27032		
102	Splňující ISO 28000		
103	Splňující EU GDPR		
104	Splňující PCI-DSS		
105	Splňující HIPAA		
106	Splňující DORA		
107	Splňující US SSAE16 SOC-1 Type II, SOC-2 Type II		

c) Firewall a komplexní ochrana perimetru včetně VPN

Popis a technické parametry

Předmětem veřejné zakázky je robustní řešení síťových firewallů typu Next Generation Firewall (NGFW), které bude plně kompatibilní s námi provozovanou technologií Check Point – integrovatelné do současného centrálního managementu. Požadujeme modulární řešení založené buď na chassis s jednotlivými interními firewall moduly, nebo virtuální chassis se samostatnou management a switchning appliance propojující jednotlivé samostatné firewall moduly. Řešení musí umožňovat efektivní distribuci provozu v rámci switching fabric, být připraveno na vysokou propustnost a poskytovat odpovídající úložnou kapacitu i při výpadku jednoho disku. Důraz klademe na výkonnost, škálovatelnost a provozní spolehlivost celého řešení. Požadujeme zařízení vhodná pro instalaci do 19" racku, s podporou vysoké dostupnosti, redundantního napájení a možností vzdálené správy přes Out-of-Band rozhraní (např. ILO/LOM). Detailní technické požadavky jsou uvedeny v přiložené tabulce.

Klíčové požadované funkcionality a vlastnosti:

- Dodávka HW pro DC1 (Active) i DC2 (Standby) – včetně orchestrátorů a Security Group konfigurace
- Dodávka potřebných licencí
- Kompletní implementace včetně migrace stávajících politik a nastavení geo-clusteru
- Nasazení management serverů na HW/virtualizační platformě zákazníka v obou DC (zákazník zajišťuje kompatibilní HW dle HCL)
- Pilotní provoz s plnými akceptačními testy (dodavatel + zákazník) včetně testu geo-failoveru · Výkonové a funkční testy dle definovaných scénářů (Public/DMZ, pobočky/DPL, IPSec + RA VPN) + test geo-failoveru DC1 → DC2 a zpět
- Nastavení pravidelných záloh managementu a firewallů v obou lokalitách
- Školení administrátorů a bezpečnostního týmu (včetně geo-redundance a failover procedur)
- Inspekce provozu na 7. vrstvě (Next Generation Firewall): analýza aplikační vrstvy s využitím identifikace aplikací a uživatelů.
- IPS (Intrusion Prevention System): Detekce a blokování známých i neznámých útoků pomocí signatur i heuristiky.
- Antibot a Antivirus: Ochrana proti malware a komunikaci s C&C servery.
- URL Filtering: Kontrola a filtrování přístupu na webové stránky dle kategorií a reputace.
- Identity Awareness: Umožňuje granularitu bezpečnostních pravidel na úrovni konkrétních uživatelů nebo skupin.
- Threat Emulation a Threat Extraction: Ochrana proti pokročilým útokům typu zero-day.
- SSL Inspection: Dešifrování a inspekce šifrovaného provozu (HTTPS).
- QoS a kontrola šířky pásma: Optimalizace provozu a zajištění priorit pro důležité aplikace.
- Monitoring, logování a reporting: Podpora centrální správy a integrace do SIEM systémů
- Vícezónová segmentace a podpora virtuálních systémů (VSX).
- Součástí předmětu plnění musí být standardní záruka výrobce v délce trvání 60 měsíců, poskytovaná bez dalších poplatků.
- Orchestrace bezpečnostních bran pro horizontální škálování pomocí zapojení více bezpečnostních gatewayí do jedné virtuální jednotky. Toto řešení přináší:
  - Lineární škálovatelnost výkonu až na stovky Gbps.
  - Vysokou dostupnost a redundanci bez výpadků (active-active cluster) jak na úrovní jednoho datacentra, tak s využitím druhého datacentra (geo-redundance).
  - Automatické vyvažování zátěže mezi jednotlivými bezpečnostními uzly.
  - Jednoduchou správu – jeden management pro celé clusterové řešení.

Možnost provozovat různé typy služeb (NGFW, IPS, VPN, Threat Prevention) na jednotlivých uzlech zároveň.

Požadavek	Popis	Odpověď respondenta	Odkaz pro důkaz/další informace
1	Firewallové moduly sloužící k filtrování musí vystupovat jako jeden logický firewall.		
2	Typ zařízení: firewally typu Next Generation Firewall – dedikovaná zařízení (appliance nebo chassis moduly).		
3	Instalace do standardního 19" kabinetu s originálním rack mount kitem, velikost 1U		
4	Lokální HDD, min 2x 960 GB NVMe, v případě výpadku centrálního management log serveru		
5	Redundance napájení fw modulu. V případě chassis, redundance napájení chassis.		
6	Out of band management (ILO/LOM) FW modulu pro vzdálenou správu v případě výpadku nebo poruchy zařízení, musí být dostupný i v případě vypnutého zařízení připojeného k napájení.		
7	Připojení do switching fabric rozhraní s kapacitou min. 4x 10/25 Gbps		
8	Switching fabric rozhraní musí rovnoměrně balancovat provoz na jednotlivé fyzické firewally (appliance nebo chassis moduly).		
9	Switching fabric rozhraní musí být součástí jednotné platformy (od stejného výrobce jako firewall moduly).		
10	Switching fabric rozhraní mohou být sdíleny více logickými firewally.		
11	Možnost připojení switching fabric rozhraní do infrastruktury s celkovou kapacitou alespoň 20x 10/25Gbps a 6x 100Gbps per DC.		
12	Switching fabric rozhraní musí podporovat navyšování výkonu přidáním dalších fyzických firewall modulů bez nutnosti rekonfigurace, anebo změn v L3 infrastruktuře.		

13	Switching fabric rozhraní musí podporovat přidání dalších firewall modulů pro lineární zvýšení propustnosti alespoň o 5 ks pro každé datacentrum.		
14	Nabízené řešení musí být typu HW appliance/chassis a nikoliv pouze SW nebo VM.		
15	Požadované funkcionality: Firewall, IPS, Aplikační kontrola, filtrování URL, AntiMalware, ochrana proti Botnet, HTTPs inspekce, DNS security, VPN(IPSec).		
16	Požadovaná celková Firewall (1518 byte UDP / Lab) propustnost řešení alespoň 360 Gb/s, při výpadku 1 FW. Požadované výkonové parametry se týkají jednoho datacentra.		
17	Požadovaná NGFW (Next-Generation Firewall) propustnost (Enterprise mix) řešení alespoň 125 Gb/s, při výpadku 1 FW. Požadované výkonové parametry se týkají jednoho datacentra.		
18	Požadovaná Thret prevention propustnost (Enterprise mix) řešení alespoň 35 Gb/s. Požadované výkonové parametry se týkají jednoho datacentra.		
19	Škálovatelnost – možnost plynulého navyšování propustnosti logického FW přidáváním dalších firewall modulů bez nutnosti výměny stávajícího HW za nový HW. Navyšování propustnosti musí být lineární.		
20	Požadovaná kapacita řešení alepoň 15M současných spojení, při výpadku 1 FW. Požadované výkonové parametry se týkají jednoho datacentra.		
21	Požadovaná kapacita platformy alespoň 1,4M nových spojení za sekundu, při výpadku 1 FW. Požadované výkonové parametry se týkají jednoho datacentra.		
22	Možnost rozdělit logický firewall na alespoň 10 virtuálních kontextů		
23	Podpora IPv4 a IPv6		
24	Podpora dynamického směrování RIPv2, OSPFv2, OSPFv3, BGP		
25	Podpora NAT (včetně IPv4,IPv6)		

26	Podpora AD, LDAP, RADIUS integrace		
27	Systém musí umožňovat získávání identit uživatelů a stanic z AD bez nutnosti instalace software na AD server		
28	Systém musí umožňovat sdílení identit mezi jednotlivými firewally bez nutnosti dalších komponent		
29	Možnost integrovat s AD na úrovni FW pravidel (user based firewall)		
30	Podpora SNMPv2c, v3		
31	Počet rozpoznávaných aplikací alespoň 7500.		
32	Ovládání firewallů přes API (napojení na automatizační systémy – může být i prostřednictvím management serverů).		
33	Podpora linux nástrojů (min. SCP, BASH, VI, TOP), spouštění linux skriptů a nástrojů třetích stran		
34	Bezpečnostní logy musí být ukládány na fyzicky oddělenou management platformu.		
35	Management musí být fyzicky oddělený od firewall platformy		
36	Komunikace mezi firewallem a centrálním managementem je šifrovaná a autentizovaná		
37	Jednotný centrální management: správa politik a analýza logů v jedné konsolidované virtuální appliance (Hyper-V, ESXi) nebo hardware		
38	Podpora administrátorských profilů pro delegaci oprávnění (čtení, zápis)		
39	Možnost přidělení práv administrátorům nebo API účtu jen pro definovaný seznam přístupových firewall pravidel		
40	Ochrana vzájemného ovlivňovaní nebo kolize při současném připojení vícero administrátorů pomocí zamykání individuálních pravidel a objektů.		
41	Možnost multi-faktorové autentizace pro přístup k management systému		
42	Možnost seskupování firewall pravidel do logických skupin a pod-skupin na základě		

	zdroje, cíle, služby/aplikace pro dlouhodobou konzistenci pravidel		
43	Možnost časově omezit platnost pravidel		
44	Funkcionalita "policy tracer" - vyhledávaní firewall pravidla dle kombinace definovaných atributů (min. zdrojová IP, cílová IP, uživatel, služba, aplikace,...)		
45	Možnost kontroly politik proti chybám a duplicitám		
46	Každé pravidlo musí nabízet statistiku počtu užití (hit count)		
47	Možnost verzování politik a možnost generování rozdílových reportů mezi jednotlivými verzemi.		
48	Vizualizace a prohledávaní logů přímo v politice na vybraném pravidle (min. zdroj, cíl, služba, aplikace, uživatel, čas)		
49	Zobrazení historie a změn přímo v politice na vybraném pravidle (min. kdo, jaká změna a kdy byla na pravidle provedena)		
50	Prohledávaní logů, min. podpora: "keyword" prohledávaní, "field" prohledávaní a "wildcard" prohledávaní		
51	Práce s bezpečnostními logy – možnost prohledávání všech typů logů (fw, ips, malware) v jedné záložce s definováním vlastních permanentních filtrů.		
52	Indexování logů umožňující rychlé prohledávaní		
53	Systém nabízí předdefinované IPS politiky		
54	Možnost definice IPS pravidel a výjimek dle kombinace src IP + dst IP + protokol + signatura		
55	Rekonfigurace a ladění threat engine přímo z log výstupů firewallu (definice vyjimek IPS signatur apod.)		
56	Podpora automatizace centrální správy pomoci REST API		
57	Logování včetně TCP stavových informací k jednotlivým spojením v rámci centrálního log serveru (min. SYN, SYN.ACK, Established, FIN, FIN.ACK, RST)		

58	Integrovaný monitoring musí poskytovat grafické rozhraní pro sledování parametrů v reálnem čase a historii alespoň 30 dní (využití paměti, CPU, počet navázaných spojení, počet nově otevřených spojení za sekundu, propustnost, atd …).		
59	Podpora služby vlastní certifikační autority pro vydávaní PKI certifikátů pro bezpečné přihlašovaní uživatelů a administrátorů a pro VPN klientský přístup		
60	Kontrola politiky dle standardů, min. ISO 27000 a GDRP (může být dodané produktem třetí strany)		
61	Funkcionalita korelace logů, analýzy a správy bezpečnostních událostí s předefinovanými reporty		
62	Integrace na Vmware vSphere, min. dynamické získávaní VM objektů a jejich aplikace ve firewall politice		
63	Přiřazení povolené či zakázané aplikace musí být nativní součástí vytváření standardního bezpečnostního pravidla bez nutnosti vytvářet profil.		
64	Možnost upgrade/update software firewallu, bezpečnostních update (IPS signatury, geolokační databáze apod.), konfigurací atd. z grafického rozhraní managementu		
65	Možnost zasílat předdefinované reporty emailem. (podpora také autentizovaného SMTP pro komunikaci s mail relay)		
66	Řešení poskytuje dynamické objekty se seznamem IP adres reprezentující externí služby typu Office365, Cloudové služby (AWS, Azure apod.), DropBox, ZOOM a další, a různé geografické lokality až na úrovni jednotlivých zemí		
67	Možnost použít tyto dynamické objekty ve FW pravidlech, NAT pravidlech a definici HTTPS inspekce		
68	Dynamické objekty se musí automaticky aktualizovat bez nutnosti zásahu administrátora		
69	Možnost integrace se SIEM, SOAR		

70	Je-li management licence omezena počtem řízených objektů bezpečnostních bran, musí podporovat řízení min. 25 objektů bran		
71	Je-li management licence omezena diskovou kapacitou, licence pro min. 16TB musí být součástí nabídky		
72	Management musí být schopen ukládat a zpracovávat logy ze všech firewallů, objem logů za den min. 15 GB/den		
73	Management log server musí zpracovat min. 40.000 logů/sekundu		
74	Dlouhodobé ukládání historických log záznamů, min. interní kapacita úložiště 16TB		
75	Podpora pravidelného automatického zálohovaní konfigurace, s možností zálohy na vzdálený SCP/FTP server.		
76	Počet publikovaných Critical/High CVE zranitelností OS firewallu za poslední 3 roky před zahájením zadávacího řízení, max. 5		
78	Podpora minimálně 200 VPN klientů, pokud je licenčně omezeno, licence musí být součástí nabídky		

d) SASE – popis a technické parametry

Předmětem veřejné zakázky je komplexní SASE řešení, které umožňuje i centralizovanou správu přes cloud a podporuje bezpečnostní politiku včetně integrace s identity providery, správou skupin a možností automatizace prostřednictvím API. Požadujeme moderní přístup k řízení přístupu uživatelů (včetně guest účtů), správu více IDP současně a možnost synchronizace uživatelských skupin. Detailní technické požadavky, které musí poptávané řešení splňovat, jsou uvedeny v přiložené tabulce.

Součástí předmětu plnění musí být standardní záruka výrobce v délce trvání 60 měsíců, poskytovaná bez dalších poplatků.

Dodávka bude realizovaná pro 1000 uživatelů.

Požadavek	Popis	Odpověď respondenta	Odkaz pro důkaz/další informace

1	Řešení umožňuje správu centralizovaným managementem prostřednictvím webové konzole bez potřeby místní infrastruktury		
2	Řešení umožňuje centrální logovaní		
3	Data musí být vždy umístěna v rámci EU		
4	Řešení musí poskytovat funkcionality: firewall, antimalware, antibot ochranu, 0-day ochranu, aplikační a URL kontrolu, kontrolu na úrovní DNS dotazů, https inspekci, sandboxing a DLP		
5	Jeden koncový klient pro „vzdálený/privátní“ přístup i pro přístup k internetu.		
6	Bezpečnostní politiky jsou uplatňované na různých úrovních (například na úrovni koncových zařízení, webového prohlížeče nebo cloudu)		
7	Řešení umožňuje propojení typu any-to-any (jakékoli připojené interní místo může komunikovat s jakýmkoli jiným místem a vzdáleným uživatelem, jakýkoli vzdálený uživatel se může připojit k jakémukoli připojenému internímu místu)		
8	Minimálně 50 PoP (Points of Presence) globálně umístěných v několika regionech		
9	Řešení poskytuje dedikovanou veřejnou statickou IP adresu		
10	Lokalizace webového obsahu i v zemích bez místní PoP		
11	Řešení využívá hybridní inspekci provozu (na úrovní lokálního klienta a současně i cloudu)		
12	Lokální agent podporuje funkčnost Secure web gateway i v případě, že se odpojí od VPN		

13	Integrace s Azure AD, Okta a lokálním AD		
14	Podpora SAML 2.0		
15	Podpora vícefaktorového ověřování uživatelů (MFA)		
16	Řešení umožňuje současné využití interní uživatelské db a zdroje identit (IDP) třetích stran.		
17	Nutnost využití více zdrojů identit současně		
18	Podpora synchronizace uživatelů a skupin mezi různými IDP		
19	Podpora SCIM (včetně synchronizace s Azure a Okta)		
20	Definice politik objekty typu: uživatel, skupina, IP, FQDN a porty/aplikace		
21	Možno definovat aplikace na základě informací z IDP		
22	Jednotná definice aplikací na základě různých bezpečnostních politik		
23	Aplikace musí mít možnost definovat aliasy pro uživatelsky přívětivý přístup.		
24	Možnost vkládat uživatelsky definované http hlavičky pro web aplikace		
25	Správa doménových certifikátů a ssh klíčů pro uživatelsky přívětivý přístup k aplikacím v režimu "agentless"		
26	Zero trust politiky na základě uživatelské identity, stavu zařízení umožňují řízení přístupu na bázi jednotlivých aplikací		
27	Možnost definovat více zcela nezávislých síťových prostředí s oddělenou přístupovou bránou a směrováním		
28	Možnost definovat privátní DNS servery pro interní provoz		

29	ZTNA v režimu "agentless" pro protokoly nativní RDP, RDP, ssh, vnc, http/https		
30	Podpora připojení k interním systémům pomocí nativního RDP a také RDP over HTTPS		
31	"Agentless" režim umožňuje oddělení skutečných přístupových údajů aplikací od přístupových údajů k platformě		
32	Možno vytvářet bypasss pravidla		
33	Sledování aktivity a relací v reálném čase		
34	Podpora inspekce HTTPS provozu (inspekce musí být prováděna přímo na agentu, aby byla zachována ochrana soukromí uživatele)		
35	Možnost rozšíření o specializovaný monitoring pro aplikace generativní AI včetně všech bezpečnostních vlastností		
36	Možnost rozšíření o specializovaný browser s podporou izolace sítě a ZTNA		
37	Proaktivní analýza s využitím vlastních indikátorů kompromitace (IoC)		
38	DLP funkcionalita podporuje předdefinované datové typy (minimálně HIPAA, PCI, PII)		
39	Možnost definice vlastních datových typů pomocí regex		
40	Podpora tunelování: IPSec, OpenVPN a Wireguard		
41	Podpora DPD		
42	Podpora IKEv1 a IKEv2		
43	Podpora šifrovacích algoritmů minimálně aes256, sha256		

44	Podpora DH protokolu založeného na eliptických křivkách (ECDH)		
45	Podpora redundance tunelů v rámci rozdílných regionů		
46	Podpora módu "Always on" u agentů		
47	Podpora split tunneling režimu, včetně možností include/exclude jak pro IP tak i FQDN		
48	Automatizovaný bezpečný přístup přes nechráněnou Wi-Fi síť (když je detekována nechráněná Wi-Fi síť, klient musí směrovat veškerý provoz přes VPN).		
49	Řešení musí mít zabudované kontroly/ochrany, které zabrání koncovým uživatelům provádět změny (možnost zabránit odpojení agenta od vpn)		
50	Řešení umožňuje získat informace a kontrolovat stav koncového zařízení (např. operační systém, antivirová ochrana, certifikát, členství v doméně, zranitelnosti na základě CVE, atd)		
51	Řešení podporuje možnosti kontroly stavu zařízení pro Windows OS: verze OS, certifikát, běžící procesy, běžící antivirová ochrana, existence souborů, šifrování disku, registry, asociace s Active Directory, firewall a antivirová ochrana registrovaná ve Windows Security Center.		
52	Řešení podporuje možnosti kontroly stavu zařízení pro macOS: verze OS, certifikát, běžící procesy, běžící antivirová ochrana, existence souborů, šifrování disku.		
53	Řešení podporuje možnosti kontroly stavu zařízení pro Linux OS: běžící procesy, běžící antivirová ochrana, existence souborů.		
54	Řešení podporuje možnosti kontroly stavu zařízení pro mobilní platformy: rooted/ jailbreak zařízení, Android		

	device security settings, Samsung Knox stav, aktivovaný režim ladění		
55	Kontinuální validace stavu zařízení po navázání připojení		
56	Řešení nabízí ucelený asset inventář (podrobnosti o zařízení, včetně přehledu připojených zařízení, sériového čísla, umístění a stavu online/offline)		
57	Podpora integrace se systémy MDM/EMM/UEM/MAM		
58	Zero touch provisionning prostřednictvím MDM		
59	Možnost reportovat informace o rizikovém stavu klienta do MDM		
60	Podpora integrace s SIEM		
61	Podpora zařízení typu BYOD		
62	Řešení musí podporovat funkcionalitu API security připojených SaaS aplikací		
63	Možnost integrace s bezpečnostními řešeními Check Point		
64	Automaticky aktualizovaný agent v uživatelských zařízeních		
65	Centrální správa aktualizací verzí agentů		
66	Podpora RBAC (Role based access control) pro administrátory řešení		
67	Podpora automatizace pomocí REST API		
68	Podpora operačních systémů Windows, Linux, MacOS, Chromebook a iOS, Android		
69	Výrobce garantuje dostupnost řešení (SLA) minimálně 99,999%		
70	Výrobce poskytuje podporu v režimu 24x7		

e) WAF

Poptáváme komplexní WAF (WEB application firewall) řešení, které umožňuje centralizovanou správu a podporuje bezpečnostní politiku.

Součástí předmětu plnění musí být standardní záruka výrobce v délce trvání 60 měsíců, poskytovaná bez dalších poplatků.

Požadavek	Popis	Nabízené řešení splňuje / nesplňuje požadavek (doplní Uchazeč) ANO/NE	Odkaz pro důkaz/další informace
1	**Platforma**		
2	Nasazení ~~redundantních~~ SW zařízení ve funkci load-balancer s podporou autentizace uživatelů, SSL akcelerátoru a webového aplikačního firewallu.		
3	Datová propustnost zařízení alespoň 22 Mbps		
	Operační systém		
5	Full-Proxy architektura (plné oddělení klientského a serverového spojení)		
6	Podpora IPv4		
7	Plná podpora IPv6, IPv4/IPv6 gateway (Podpora Ipv4 a Ipv6 na straně klienta i na straně serveru včetně všech možných kombinací)		
8	Podpora ověření certifikátů vydaných podřízenou CA (intermediate CA)		
9	Podpora Spanning Tree Protokolu (STP)		
10	Možnost přidat vlastní funkce pomocí skriptování - umožnění plnohodnotné manipulace a správy veškerého IP aplikačního provozu s cílem zachytit, zkontrolovat, transformovat a nasměrovat příchozí nebo odchozí provoz pomocí skriptovacího jazyka/syntaxe.		

11	Podpora HTTP/2		
12	Podpora IPSec IKEv2		
13	Podpora konfigurace a správu zařízení přes REST API		
14	Podpora SNMP (v1/v2c/v3)		
15	Možnost aktivovat následující funkce na jedné HW platformě: • L4-7 loadbalancing • ICSA certifikovaný Web aplikační firewall • ICSA certifikovaný síťový firewall • Autorizace a autentizace aplikací, SSL VPN • DNS služby a DNS firewall		
16	Možnost používat knihovny JavaScript třetích stran k úpravě a správě provozu		
17	Podpora Active-Active a Active-Pasive módu		
	Web aplikační Firewall		
20	Integrace s nástrojem na detekci zranitelností webových aplikací		
21	Detekce a blokování širokého spektra útoků na aplikační vrstvě, minimálně podle OWASP top10		
22	Modul aplikačního firewallu poskytne ochranu minimálně proti těmto aplikačním útokům: • Webové hrozby AJAX / JSON • DoS a DDoS na 7. vrstvě • Útok hrubou silou tj. zahlcení velkým množstvím přihlašovacích údajů (útok typu „Brute-force“) • Nechtěné provední akce uživatelem v aplikaci, ve které je právě autentizovaný (útok typu „Cross Site Request Forgery“)		

	• Vložení kódu do webové aplikace s cílem jí změnit (útok typu „Cross-site scripting XSS“) • Vložení kódu do formulářových polí aplikace s cílem získat data z back-end serverů (útok typu „SQL injection“) • Manipulace s parametry HTTP (HPP) • Převzetí relace uživatele útočníkem (útok typu „Session highjacking“) • Přetečení bufferu serveru (útok typu "Buffer overflow“) • Manipulace s cookies a jejich podvržení útočníkem • Manipulaci se skrytými poli (útok typu "Hidden field manipulation“) • Vložení škodlivého požadavku útočníka do původního požadavku uživatele (útok typu „Request smuggling“) • XML bomby / DoS • Nepovolené snímání obsahu z webových stránek (útok typu „Web scraping“)		
23	Možnost doprogramovat si filtrovaci pravidla pro aplikace		
24	Automatická korelace zranitelností do jednoho bezpečnostního incidentu		
25	Možnost vytvoření bezpečnostních politik způsobem hierarchie nadřízené a podřízené politiky.		
26	Ochrana AJAX a JSON aplikací		
27	Podpora Captcha metody		
28	Automatické odlišení skutečných uživatelů od robotů		
29	Ochrana proti automatizovanému provozu/útokům z (ro)botů nejen pomocí		

	signatur, ale také pomocí aktivního zjišťování zda se jedná o browser vs. bot (pomocí tzv. „challenge“, neboli úkolů, díky kterým WAF identifikuje bot vs uživatel), pokud umí bot simulovat chování skutečného prohlížeče a zamezení propuštění takové komunikace na aplikační server.		
30	Integrovaný XML firewall		
31	Podpora maskování/odstranění citlivých informací – čísla kreditních karet, číslo pojištění…		
32	Automatické nahrávání a aplikování nových signatur		
33	Podpora pozitivního a negativního bezpečnostního modelu		
34	Blokování útočníků na základě geolokace (až na úroveň regionů)		
35	Podpora ICAP pro antivirovou kontrolu – pro SOAP a SMTP		
36	Ochrana SMTP a FTP na aplikační úrovni		
37	Podpora SSL (šifrování a dešifrování)		
38	Podpora různých typů reportů – PCI, geolokační reporty		
39	Podpora standardů PCI DSS, HIPAA, Basel II a SOX		
40	Integrované bezpečnostní politiky pro Microsoft Outlook Web Access, Lotus Domino Mail Server, Oracle E-Business Financials a Microsoft SharePoint		
41	Podpora pro analýzu HTTP provozu (Top URL, Top klienti, nejpoužívanější HTTP metody, návštěvnost stránek podle geogr. Regionu)		
42	Možnost importu zranitelnosti aplikací z alespoň některých z následujících skenerů: • Cenzic Hailstorm		

	• WhiteHat Sentinel • IBM Rational AppScan • QualysGuard Web Application Scanning		
43	Podpora aplikačního firewallu ve virtuálních kontextech		
44	Podpora aplikačního firewallu		
45	Rozšířená podpora CSHUI – detekce aktivity klávesnice a myši, detekce změn URL od klienta za krátkou dobu		
46	Ochrana proti Session Highjacking pomocí jednoznačné identifikace prohlížeče uživatele (Browser Fingerprintingu)		
47	Podpora TLS Fingerprinting - schopnost detekovat útočníka za NAT a neblokovat všechny uživatele za stejnou NATovanou adresou.		
48	Detekce a ochrana před DoS útoky na specifické URL, které mohou zatížit back-end systémy (např. vyhledávácí URL apod.)		
49	Vynucení přístupu uživatele k chráněné aplikaci přes přihlašovací stránku aplikace		
50	Podpora nastavení bezpečnostních politik podle IP adresy, doménového jména a URI		
51	Podpora a filtrování WebSocket provozu		
52	Blacklistování IP adres, které se opakovaně snaží překonat bezpečnostní opatření v politice		
53	Ochrana dat a přihlašovacích údajů proti Man in the Browser útokům, kdy během zadávání do citlivých polí formuláře na webové aplikaci dochází k šifrování dat na aplikační vrstvě na straně klienta, jenž následně dekryptuje pouze WAF.		
54	Podpora mikroslužeb ve WAF politikách		

55	Ochrana pro DoS/DDoS útokům na aplikační úrovni pomocí průběžné analýzy stresu aplikace, analýzy povahy aplikačního provozu tzv. behaviorální analýzy a vylaďování ochrany aplikace za pomocí uplatňování dynamických signatur. WAF mapuje a zaznamenává standardní chování uživatelů v rámci aplikace. V případě zvýšeného stresu aplikace, dojde k identifikaci odchylek v provozu a na jejich základě se dynamicky vygeneruje signatura, která jednoznačně identifikuje zdroje škodlivého provozu, který může být zablokován nebo zpomalen.		
56	Podpora importu souboru Swagger pro definici security politiky pro ochranu API.		
57	Podpora využití CI/CD pipeline pro nasazování security politik WAF na webových aplikacích.		
58	Podpora integrace s nástroji chatu (Slack / Teams…) a hlášení stavu systému a logování pomocí těchto nástrojů.		
59	Možnost integrace na externí platformy SIEM pomocí logování na úrovni TCP dumpu.		
60			
61	Možnost připojení k monitorovacím nástrojům třetích stran prostřednictvím otevřeného API		
62	Podpora REST API		
63	Autentizace klientů přes LDAP/Radius		
64	Povolení/zakázání ICMP pro VIP		
65	Podpora vysokorychlostního granulárního logování / logování per aplikace / bez omezení výkonnosti zařízení		
66	Podpora alespoň pro 19 metod rozvažování zátěže		
67	Podpora filtrace paketů		

68	Podpora ToS, QoS (marking/preservation/mimic)		
69	Podpora SNMP (v1/v2c/v3)		
70	Podpora rozvažování zátěže založené na poměrech (ratio) s CARP perzistencí		
71	Podpora SSL certifikátů podepsaných SHA-2 algoritmem		
72	Podpora práce s 4096-bit klíči		
73	Současná podpora ECC a RSA certifikátu		
74	Podpora pro TLS 1.2 a TLS 1.3		
75	Podpora ECC a DH šifer v HW		
76	Podpora SSL Forward proxy		
77	Stavové filtrovaní paketů (ACL)		
78	Podpora vlastních skriptů pro monitorování zdraví a dostupnosti služeb		
79	Podpora monitorování služeb na základě výkonu konkrétních hostů		
80	TCP optimalizace síťových toků		
81	Komprese a cachování specifických služeb		
82	Podpora optimalizace dynamické velikosti TLS bloků (TLS record size)		
83	**Řízení uživatelských přístupů**		

f) Zabezpečení a detekce zranitelností zdrojového kódu

Klíčové požadované funkcionality:

- Centralizovaná platforma pro správu zdrojového kódu, přístupů a CI/CD pipeline.
- Detailní RBAC řízení přístupů, ochrana větví a tagů, povinné použití MFA.
- Povinný Merge Request proces, code review, security review a podepisování commitů.
- Kompletní auditní logování všech aktivit uživatelů a systémů v SCM.
- Centrální úložiště nálezů ze SAST analýzy s řízením SLA a vazbou na Security Gate.
- Soulad minimálně se standardy ISO 27001, ISO 27034, NIS2, OWASP SAMM/ASVS a NIST SSDF.
- Vynucení bezpečných workflow, kontroly integrity a minimalizace přístupových práv.
- Součástí předmětu plnění musí být standardní záruka výrobce v délce trvání 60 měsíců, poskytovaná bez dalších poplatků.

Požadavek – Parametr / funkcionalita:

Požadavek	Parametr / funkcionalita	Odpověď respondenta	Odkaz pro důkaz/další informace
1	Řešení musí být postaveno na centralizované SCM platformě (self-managed / SaaS – dle koncepce) umožňující jednotnou správu zdrojového kódu, verzování a CI/CD pro 24 vývojářů.		
2	SCM musí podporovat zásady Secure-by-Design a Least Privilege v rámci celého vývojového procesu včetně využití projektových, skupinových a podskupinových oprávnění		
3	Platforma musí poskytovat detailní řízení přístupů na úrovni projektů, skupin a podskupin.		
4	Řešení musí podporovat role dle RBAC (Guest, Reporter, Developer, Maintainer, Owner).		
5	Platforma musí umožňovat ochranu větví a tagů (Protected Branches, Protected Tags).		
6	Přístup do SCM musí být zabezpečen vícefaktorovou autentizací (MFA).		
7	Všechny změny kódu musí probíhat výhradně přes Merge Request proces.		
8	Každý Merge Request musí obsahovat povinné code review a security review.		
9	Commity musí být povinně digitálně podepisovány (GPG nebo SSH).		
10	Auditní záznamy SCM musí umožnit dohledat uživatele, čas, akci a objekt (projekt, branch, pipeline, oprávnění).		
11	Řešení musí umožňovat integraci nástrojů pro statickou analýzu kódu v rámci CI/CD pipeline.		
12	Řešení musí umožňovat vyhodnocení výsledků analýzy v kontextu změn zdrojového kódu (např. MergeRequest)		

13	SCM a bezpečnostní nástroje musí být konfigurovány v souladu s rámci ISO 27001, ISO 27034, Směrnicí Evropského parlamentu a Rady EU č. 2022/2555, opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (dále či výše jen NIS2), OWASP SAMM/ASVS, NIST SSDF.		
14	Platforma musí vynucovat bezpečné workflow, kontrolu integrity a minimalizaci přístupových práv.		
15	Řešení musí umožňovat auditní transparentnost a dohledatelnost všech schvalovacích a bezpečnostních procesů.		

g) **Zabezpečení systému pro řízení drážního provozu**

Klíčové vlastnosti řešení

Zavedení odděleného síťového provozu pomocí virtuální firewall instance formou služby, které umožňují plnou izolaci jednotlivých síťových segmentů v rámci jedné fyzické infrastruktury. Každý kontext představuje samostatnou logickou instanci firewallu se separátními politikami, routováním, logováním a monitoringem.

Cíl dodávky

- zajistit robustní segmentaci provozu mezi jednotlivými zónami (IT / OT / DMZ / výrobní sítě) prostřednictvím nezávislých virtuálních firewall instancí
- umožnit detekci a blokování nestandardní nebo anomální komunikace v rámci všech segmentů
- poskytovat plnou izolaci síťových toků bez vzájemného ovlivňování mezi kontexty

Požadované funkce a schopnosti

- Segmentace na úrovni virtuálních firewall instancí včetně definice separátních politik, routingu a logických zón
- Doporučení a optimalizace bezpečnostních politik přiřazených ke každému virtuálnímu firewallu
- Centrální management přes chytrou konzoli / dashboard se správou jednotlivých kontextů
- Logování a reporting v rámci NIS2 / zákona č. 264/2025 Sb. (dále jen „ZKB“)
- Integrace do stávajícího SIEM (Syslog, CEF, LEA) s granularitou per-kontext

Rozsah dodávky a služeb

- Kompletní implementace logických virtuálních firewallů včetně převedení existujících politik (pokud existují)
- Konfigurace směrování, NAT, zón a veškerých logických instancí firewallu
- Nastavení provozních režimů a testování včetně fail-open / fail-close podle požadavků
- Školení administrátorů a IT/OT bezpečnostního týmu na správu kontextové architektury

Nasazení IDS/IPS a OT monitoringu

Nastavení specializovaného bezpečnostního řešení obsahujícího platformu pro kontinuální monitoring prostředí s hlavním cílem:

- zajištění úplné viditelnosti aktiv a komunikace

Požadavky na funkce a schopnosti řešení:

- Pasivní monitoring síťové komunikace
- Detekce anomálií komunikace (nestandardní toky, neobvyklé příkazy, laterální pohyb)
- Detekce neautorizovaných přístupů, neoprávněného remote access
- Pokročilé alerty v reálném čase s kontextem (asset, protokol, uživatel, závažnost, exploitovatelnost)
- Integrace do stávajícího SIEM/SOAR (Syslog, CEF, API)
- On-premise nasazení

Rozsah dodávky služeb

- Proof of Concept / Pilot na vybrané části OT sítě (povinný)
- Integrace do stávajících bezpečnostních a provozních systémů
- Školení administrátorů OT bezpečnosti a operátorů

Integrace s centrálním SIEM systémem

Dodavatel zajistí plnohodnotnou integraci OT bezpečnostního řešení s centrálním SIEM systémem zadavatele formou integrační služby na klíč.

Požadovaný rozsah integrace

- Návrh a implementace optimálního způsobu exportu logů a událostí (Syslog TLS / CEF / LEA / Log Exporter / API podle typu řešení)
- Export všech relevantních událostí včetně:
  - firewall/IPS blokování a detekce
  - audit logy samotného bezpečnostního řešení
- Zajistit spolehlivý přenos logů i při výpadku konektivity (buffering, queuing)
- Testování integrace včetně zátěžového testu a ověření úplnosti a správnosti logů
- Předání kompletní dokumentace integrace, parserů a údržbového manuálu

Zavedení politik řízení přístupů

Dodavatel zajistí kompletní službu návrhu, implementace a otestování politik řízení přístupů do OT/provozní sítě na bázi standardu IEEE 802.1X (port-based NAC) v souladu s požadavky NIS2, Zákona o kybernetické bezpečnosti (SR 1.1 – Identification & Authentication Control, SR 1.5 – Authenticator Management, SR 2.6 Restricted Network Access).

Požadovaný rozsah služby (na klíč):

- Analýza stávající sítě z hlediska podpory 802.1X
- Návrh autentizační architektury
- Vytvoření detailních 802.1X politik včetně:
  - autentizace koncových zařízení certifikáty (machine certificates – preferováno)
  - autentizace uživatelů přes LDAP/AD + MFA
  - fallback mechanismy (MAC Authentication Bypass – MAB pro legacy zařízení, která 802.1X nepodporují)
  - dynamické přiřazování VLANů / SGT / ACL podle role, lokality a typu zařízení
- Návrh a implementace zásad pro:
  - automatické odstraňování neautorizovaných zařízení ze sítě (quarantine/remediation VLAN)
  - time-based access (povolení přístupu jen v údržbových oknech)
  - logging a alerting všech autentizačních událostí do centrálního SIEM
- Integrace s existujícím PKI / Microsoft CA pro vydávání a revokaci certifikátů
- Pilotní nasazení na vybraném segmentu/lokalitě (povinné)
- Vytvoření finálních politik pro vybraný rozsah max. do 10 profilů
- Testování odolnosti (fail-open vs. fail-close, vliv na provoz, zátěžový test)
- Vytvoření dokumentace:
  - 802.1X Policy Design Document
  - Postup pro enrolování nových zařízení
- Zaškolení OT a bezpečnostního týmu

Výstupy, které dodavatel předá:

- Plně funkční 802.1X autentizace na min. 90 % vybraných zařízení (zbytek přes MAB nebo statické výjimky)
- Playbook pro správu a řešení incidentů

Zavedení systému vzdáleného přístupu s vícefaktorovou autentizací

Dodavatel zajistí kompletní dodávku, implementaci a integraci řešení pro bezpečný vzdálený přístup interních uživatelů, dodavatelů a třetích stran do OT/IT/IoT prostředí zadavatele formou služby na klíč v souladu s NIS2 (čl. 21), ZKB (SR 2.1, SR 2.6, SR 1.7).

Požadovaný rozsah dodávky a služeb

- On-premise architektura
- Implementace Zero-Trust přístupu:
  - Vícefaktorová autentizace (MFA/2FA) pro všechny vzdálené přístupy (možná integrace s Azure AD)

    - Proxy-based přístup bez VPN klienta (HTTP/S)
    - Politiky podle role, lokality a typu zařízení
- Integrace s návaznými systémy zadavatele:
    - Active Directory / LDAP / Azure AD
    - Centrální SIEM (odesílání všech session logů, alertů a auditů v CEF/Syslog)
    - Stávající firewall (jump host eliminace, přímý přístup přes PAM)
- Pilotní nasazení (Proof of Concept) na vybrané skupině uživatelů/dodavatelů
- Návrh a implementace politik přístupu pro vybrané prostředí (oddělení interních uživatelů, dodavatelů, údržby)
- Testování bezpečnosti, výkonnosti a odolnosti (failover, zátěžový test)
- Vytvoření dokumentace:
    - Bezpečnostní procedury pro vzdálený přístup
    - Uživatelské a administrátorské manuály

  Školení:
    - Administrátorské
    - Bezpečnostní tým / SOC

Zajištění zálohování a obnovy konfigurací OT zařízení

Dodavatel zajistí kompletní službu centralizovaného zálohování, verzování a obnovy na klíč.

Požadovaný rozsah služby (na klíč):

- Nastavení automatického periodického zálohování (min. 1× týdně)
- Verzování záloh s porovnáním rozdílů (diff) a možností rollbacku na předchozí schválenou verzi
- Testovaná procedura obnovy (recovery) na testovacím prostředí i přímo v provozu
- Automatická validace záloh (integrity check)
- Integrace s centrálním SIEM – alerting při neautorizované změně konfigurace nebo neúspěšném backupu
- Pilotní nasazení na vybrané lokalitě
- Dokumentace:
    - Popis backup řešení
- Školení odpovědného týmu a krizového štábu (2 MD)

Požadavek	Popis	Odpověď respondenta	Odkaz pro důkaz/další informace
1	Robustní segmentace pomocí virtualni firewall instance		
2	Možnost detekce a blokace neschválené komunikace v síti		
3	Integrace s centrálním SIEM systémem na straně zadavatele (Syslog TLS/CEF/LEA/Log Exporter)		
4	Zavedení politik řízení přístupů k síti (802.1X, machine certificates, MFA, MAB fallback, dynamické ACL/VLAN)		

5	Nastavení systému bezpečného vzdáleného přístupu (Zero-Trust, MFA, bez VPN klienta)		
6	Integrace vzdáleného přístupu s AD/Azure AD, SIEM		
7	Centralizované automatické zálohování konfigurací (verzování, diff, šifrované úložiště, integrity check)		
8	Dodání kompletní dokumentace včetně politik		
9	Školení administrátorů, OT týmu a SOC (min. 2 MD)		