Rozšíření soustavy bezpečnostních bran		
NIPEZ	32413100-2	
parametr	vyžadujeme	max./min.
celková cena (datacentrové a pobočkové firewally, management software, HW a SW podpora) bez DPH	5 500 000 Kč	max.
řešení nahrazuje současný cluster frontend firewallů	2x CheckPoint 5400 + Next Generation Security Management Software pro 5 GW	
řešení musí být 100% kompatibilní se stávajícím clusterem backend firewallů	2x CheckPoint 5400 + Next Generation Security Management Software pro 5 GW	
poptávané řešení se skládá z komponent	datacentrové firewally + pobočkové firewally + centrální management + HW a SW podpora	
veškeré poptávané funkcionality v této veřejné zakázce musí být součástí dodávky a Zadavateli nesmí vzniknout žádné další náklady na provoz zařízení tak, jak jej popisuje v této zadávací dokumentaci (např. nutný nákup licencí, balíčků podpory, hardwarových zařízení)	ano	
součástí dodávky je i zařízení/softwarová platforma s funkcí centrálního managementu, reportingu a logování celého řešení	ano	

Všechny požadavky uvedené v této zadávací dokumentaci splňuje např.: 2x firewall CheckPoint 9100 Plus s pětiletou HW podporou, licencí pro 10 virtualních systémů a Next Generation Threat Prevention (CPAP-SG9100-PLUS-SNBT + CPSB-VS-10 + CPSB-NGTP-9100-PLUS-3Y + CPSB-NGTP-9100-PLUS-1Y) + 6x SFP+ transceiver for 10G (CPAC-TR-10SR-D) + 6x SFP+ transceiver for 10G Fiber ports -long range (CPAC-TR-10LR-D)
2x pobočkový firewall CheckPoint 1900 Base s pětiletou HW podporou a Next Generation Threat Prevention (CPAP-SG1900-SNBT + CPSB-NGTP-1900-3Y + CPSB-NGTP-1900-1Y) + 4x SFP+ transceiver for 10G(CPAC-1800-TR-10SR) +
1x Software management a Reporting na 5 let (CPSM-NGSM10 + CPSB-EVS-10-3Y + CPSB-EVS-10-1Y) +
1x SW podpora (CPCES-CO-STANDARD + CPCES-CO-PREMIUM + CPCES-CO-STANDARD-ADD)

Datacentrové firewally		
NIPEZ	32413100-2	
parametr	vyžadujeme	max./min.
počet kusů zařízení typu datacentrový firewall	2 ks	
podporuje virtualizaci firewallů	ano	
virtuální firewally je možno jednotlivě customizovat dle funkčního použití	ano	
každý jednotlivý firewall podporuje tvorbu virtuálních firewallů v počtu	3 ks	min.
formát zařízení	rack-mount	
velikost každého zařízení	1U	max.
součástí dodávky je rack-mount kit pro beznástrojovou instalaci do racku (např. DELL PowerEdge 4220)	ano	
schopnost vytvořit mezi fyzickými firewally cluster typu	Active - Pasive nebo Active - Active	
firewally je možné zapojit do clusteru tak, aby tvořily jeden celek	ano	
zařízení je možné spravovat pomocí příkazového řádku	ano	
zařízení je možné spravovat pomocí grafického rozhraní	ano	
zařízení musí mít schopnost plnohodnotné centrální správy z jednoho bodu	ano	
vzdálený management - součástí dodávky je i zařízení, které umožní Zadavateli vzdálené (z internetu) připojení k zařízení i při vypnutém stavu nebo nefunkčním firmware	ano	
vzdálený management - součástí dodávky je i zařízení, které umožní Zadavateli vzdálené (z internetu) restartování zařízení	ano	

vzdálený management - součástí dodávky je i zařízení, které umožní Zadavateli vzdálené (z internetu) vypnutí a zapnutí zařízení	ano	
všechna zařízení musí mít schopnost plnohodnotné konfigurace z jedné sady pravidel (šablony)	ano	
jednotné grafické rozhraní umožňuje provádění	prohlížení logů + reportů + tvorba pravidel	min.
možnost logovat operace administrátorů	ano	
možnost reportovat události - komunikace na specifikované IP adresy	ano	
možnost reportovat události - zachycený malware	ano	
možnost reportovat události - odmítnutá/navázaná spojení	ano	
možnost reportovat události - odmítnutá/povolená spojení na webové stránky	ano	
zařízení musí být schopné odesílat provozní logy na jedno dedikované zařízení ve formě fyzického zařízení nebo softwarové platformy pomocí protokolu SYSLOG	ano	
zařízení musí být schopno odesílat provozní logy na systém Wazuh	ano	
zařízení musí byt schopno logovat veškeré události, které je schopno sledovat	ano	
podpora řízení oprávnění administrátorských rolí s možností přidělování práv (minimálně read-only a read-write) pro jednotlivé skupiny administrátorů	ano	
velikost diskové kapacity zařízení pro krátkodobé ukládaní log záznamů a updatů firmware	400 GB	min.
počet 1000BASE-T ethernet portů v každém zařízení pro síťovou komunikaci	4 porty	min.
počet SFP+ portů v každém zařízení pro síťovou komunikaci	5 portů	min.
součástí dodávky jsou i SFP+ moduly doporučené výrobcem zařízení	ano	
dodané SFP+ moduly jsou typu	různé druhy	
počet dodaných SFP+ modulů typu 10 Gbps SingleMode, LongRange součástí dodávky pro každé zařízení	3 ks	
počet dodaných SFP+ modulů typu 10 Gbps MultiMode, ShortRange součástí dodávky pro každé zařízení	3 ks	
počet dedikovaných portů ethernet (BASE-T) portů určených pro vzdálený management zařízení	1 port	min.
port pro vzdálený management podporuje Out-of-Band funkcionalitu	ano	
zařízení podporuje práci v módu High Availability bez dalších nákladů na hardware, software nebo licence (potřebný HW, SW a licence pro realizaci HA jsou součástí dodávky)	ano	
počet dedikovaných portů pro funkcionalitu High Availability na zařízení	1 port	min.
interní úložiště na jednotlivých zařízeních podporuje ukládání	logů, záloh konfigurací, snapshotů	min.
možnost provozovat zařízení v routovacím režimu	ano	
možnost provozovat zařízení v routovacím režimu NAT	ano	
možnost provozovat zařízení v routovacím režimu PAT	ano	
možnost provozovat zařízení v režimu HTTP Proxy	ano	
možnost provozovat zařízení v režimu HTTPS Proxy	ano	
možnost kontroly šifrovaného SSL provozu	ano	
licencí)	750 ks	min.
možnost prioritizovat vybrané části síťového provozu přes zařízení (QoS)	ano	
podpora VPN spojení - IPSec	ano	
podpora VPN spojení - L2TP	ano	
podpora SSL VPN v portálovém módu	ano	
podpora IPSec VPN v tunelovém módu	ano	
podpora SSL VPN v tunelovém módu	ano	
počet licencí pro VPN připojení součástí dodávky	4	min.
licence pro VPN připojení licencovány v režimu	současná připojení	
podpora autorizace uživatelů pomocí - RADIUS	ano	
podpora autorizace uživatelů pomocí - lokální databáze	ano	
podpora autorizace uživatelů pomocí - Active Directory	ano	
zařízení typu firewall podporuje statický routing pro protokoly	IPv4 i IPv6	
zařízení typu firewall podporuje dynamický routing pro protokoly	RIP, OSPF, BGP	
zařízení typu firewall podporuje protokol - VRRP (Virtual Router Redundancy Protocol)	ano	

podpora protokolu - SNMP v.1	ano	
podpora protokolu - SNMP v.2	ano	
podpora protokolu - SNMP v.3	ano	
podpora protokolu - SysLog	ano	
podpora protokolu - IPFIX (NetFlow v. 10)	ano	
zařízení typu firewall podporuje standard - IEEE 802.1Q (VLAN)	ano	
zařízení typu firewall podporuje standard - IEEE 802.3ad (Teaming/Link aggregation)	ano	
podpora možnosti přidělení šířky pásma na základě zdrojových IP adres (Trafic shaping)	ano	
vestavěná podpora více-faktorové autentizace pro nativní VPN službu firewallů pro uživatele	ano	
více-faktorové autentizace využívá faktory	uživatelské jméno, heslo, e-mail, SMS	min.
součástí dodávky je i SMS gateway	ne	
celková propustnost každého zařízení (UDP port 1518)	66 Gbps	min.
zařízení podporuje tvorbu pravidel na základě dynamických objektů	ano	
podporované dynamické objekty	Microsoft Office 365, Azure services, Google services, Zoom services	min.
zařízení obsahuje modul IPS (Intrusion Prevention System)	ano	
modul IPS automaticky provádí aktualizaci signatur	ano	
propustnost modulu IPS (Enterprise mix nebo podobná metrika)	17 Gbps	min.
modul IPS umožňuje automatické vypnutí IPS ochrany pro zařízení v případě přetížení hardwaru (využití CPU nebo fyzické paměti) nad definovanou prahovou hodnotu	ano	
zařízení obsahuje modul pro filtrování obsahu webového provozu (Web Filtering)	ano	
modul pro filtrování webového provozu (Web filtering) pracuje na principu kategorizace webového obsahu	ano	
modul pro filtrování webového provozu (Web filtering) kategorizuje webový obsah do kategorií	phishing, spam, p2p file sharing, botnets, spyware, malicious sites, weapons, racism, pornography, games, gambling, child abuse, drugs, violence, hacking	min.
modul Web filtering umožňuje monitorování navštívených kategorií na uživatele	ano	
zařízení musí podporovat funkcionalitu, která uživatele notifikuje v českém jazyce, že jeho přístup na danou webovou stránku byl zablokován na základě Web filteringu	ano	
zařízení obsahuje modul aplikační kontroly	ano	
řízení aplikací na Layer 7 na základě signatury aplikace, nikoliv dle portu	ano	
zařízení obsahuje modul Antivirus	ano	
zařízení obsahuje modul ochrany proti Botnet sítím	ano	
propustnost zařízení (Enterprise mix nebo podobná metrika) threat prevention ochrany (firewall, IPS, aplikační kontrola, antivir, web filtering)	4,5 Gbps	min.
podporovaný počet spojení za vteřinu (CpS)	11 000	min.
podporovaný počet současných živých spojení	1 200 000	min.
propustnost VPN (AES-128)	1,3 Gbps	min.
zdroje napájení - počet	2 ks	
zdroje napájení - redundantní	ano	
firewally jsou dodávány s právem aktualizace firmwaru po dobu	5 let	
podpora - součástí dodávky je i právo na update a upgrade veškerých komponent zařízení	ano	
zařízení jsou dodávána s právem aktualizace bezpečnostních signatur od výrobce po dobu	5 let	
zařízení jsou dodávána s právem aktualizace modulů od výrobce po dobu	5 let	
zařízení jsou dodávána s hardwarovou podporou výrobce na dobu	5 let	

zařízení jsou dodávána s technickou podporou výrobce na dobu	5 let	
zařízení budou dodána do sídla zadavatele již kompletovaná a zahořená	ano	
zařízení musí být určena pro český trh	ano	
zařízení musí být nová	ano	
součástí nabídky bude Prohlášení českého zastoupení výrobce nebo přímo výrobce o tom, že nabízený produkt v rámci této veřejné zakázky, je určený pro trh v České republice a bude podporován výrobcem nebo servisním střediskem výrobce na území České republiky	ano	
podpora a záruka je poskytována výrobcem zařízení nebo jeho autorizovaným partnerem nezávisle na dodavateli firewallu	ano	
podpora - poskytovaná minimálně prostřednictvím telefonní linky nebo webového formuláře musí být dostupná v režimu 24x7	ano	
podpora - musí umožňovat získání aktuálních ovladačů a manuálů adresně pro konkrétní zadané produktové, popř. sériové číslo zařízení	ano	
záruka - rychlost odezvy na nahlášenou závadu do	v den incidentu	
záruka - garance odeslání náhradního dílu na místo provozu zařízení	následující pracovní den	
záruka - dodání do místa provozu zařízení v režimu "Best Effort"	3 pracovní dny	max.
nabídka a Prohlášení musí být v češtině	ano	
zadavatel vylučuje z nabídek technologie firem, které byly označeny BIS ve výroční zprávě 2013 z 27. 10. 2014 v bodě 2.7 Kybernetická bezpečnost jako potenciálně nebezpečné	ano	

Pobočkové firewally		
NIPEZ	32413100-2	
parametr	vyžadujeme	max./min.
počet kusů zařízení	2 ks	
pobočkový firewall - formát zařízení	rack-mount	
pobočkový firewall - velikost zařízení	1U	max.
součástí dodávky je rack-mount kit pro instalaci do racku (např. DELL PowerEdge 4220)	ano	
formát zařízení	rack-mount	
součástí dodávky je rack-mount kit	ano	
schopnost vytvořit mezi firewally cluster typu	Active - Pasive	min.
firewally je možné zapojit do clusteru tak, aby tvořily jeden celek	ano	
zařízení je možné spravovat pomocí příkazového řádku	ano	
zařízení je možné spravovat pomocí grafického rozhraní	ano	
zařízení musí mít schopnost plnohodnotné centrální správy z jednoho bodu	ano	
všechna zařízení musí mít schopnost plnohodnotné konfigurace z jedné sady pravidel (šablony)	ano	
jednotné grafické rozhraní pro provádění	prohlížení logů + reportů + tvorba pravidel	
možnost logovat operace administrátorů	ano	
možnost reportovat události - komunikace na specifikované IP adresy	ano	
možnost reportovat události - zachycený malware	ano	
možnost reportovat události - odmítnutá/navázaná spojení	ano	
možnost reportovat události - odmítnutá/povolená spojení na webové stránky	ano	
zařízení musí být schopné odesílat provozní logy na jedno dedikované zařízení ve formě fyzického zařízení nebo softwarové platformy	ano	
zařízení musí byt schopno logovat veškeré události, které je schopno sledovat	ano	
podpora řízení oprávnění administrátorských rolí s možností přidělování práv (minimálně read-only a read-write) pro jednotlivé skupiny administrátorů	ano	
velikost diskové kapacity zařízení pro krátkodobé ukládaní log záznamů a updatů firmware	400 GB	min.
počet 1000BASE-T ethernet portů v každém zařízení pro síťovou komunikaci	4 porty	min.
počet SFP+ portů v každém zařízení pro síťovou komunikaci	2 porty	min.

součástí dodávky jsou i SFP+ moduly doporučené výrobcem zařízení	ano	
dodané SFP+ porty jsou typu	10 Gbps, multimode, short range	
počet dodaných SFP+ modulů typu 10 Gbps MultiMode, ShortRange součástí dodávky pro každé zařízení	2 ks	
počet dedikovaných portů ethernet (BASE-T) portů určených pro vzdálený management zařízení	1 port	min.
zařízení podporuje práci v módu High Availability bez dalších nákladů na hardware, software nebo licence (potřebný HW, SW a licence pro realizaci HA jsou součástí dodávky)	ano	
počet dedikovaných portů pro funkcionalitu High Availability na zařízení	1 port	min.
interní úložiště na jednotlivých zařízeních podporuje ukládání	logů a záloh konfigurací	
podpora pro více linek WAN	ano	
možnost provozovat zařízení v routovacím režimu	ano	
možnost provozovat zařízení v routovacím režimu NAT	ano	
možnost provozovat zařízení v routovacím režimu PAT	ano	
možnost kontroly šifrovaného SSL provozu	ano	
počet chráněných uživatelů/zařízení všemi moduly, které zařízení obsahuje (počet klientských licencí)	460 ks	min.
možnost prioritizovat vybrané části síťového provozu přes zařízení (QoS)	ano	
podpora VPN spojení - IPSec	ano	
podpora VPN spojení - L2TP	ano	
podpora IPSec VPN v tunelovém módu	ano	
podpora SSL VPN v tunelovém módu	ano	
podpora autorizace uživatelů pomocí - RADIUS	ano	
podpora autorizace uživatelů pomocí - lokální databáze	ano	
podpora autorizace uživatelů pomocí - Active Directory	ano	
zařízení dynamický routing pro protokoly	RIP, OSPF, BGP	
zařízení podporuje práci v HA (High Availability) režimu	ano	
podpora protokolu - SNMP v.2	ano	
podpora protokolu - SNMP v.3	ano	
podpora protokolu - SysLog	ano	
zařízení podporuje standard - IEEE 802.1Q (VLAN)	ano	
zařízení podporuje standard - IEEE 802.3ad (Teaming/Link aggregation)	ano	
podpora možnosti přidělení šířky pásma na základě zdrojových IP adres (Trafic shaping)	ano	
celková propustnost každého zařízení (UDP port 1518)	33 Gbps	min.
zařízení podporuje tvorbu pravidel na základě dynamických objektů	ano	
podporované dynamické objekty	Microsoft Office 365, Azure services, Google services, Zoom services	min.
zařízení obsahuje modul IPS (Intrusion Prevention System)	ano	
modul IPS automaticky provádí aktualizaci signatur	ano	
propustnost modulu IPS (Enterprise mix nebo podobná metrika)	8,5 Gbps	min.
modul IPS umožňuje automatické vypnutí IPS ochrany pro zařízení v případě přetížení hardwaru (využití CPU nebo fyzické paměti) nad definovanou prahovou hodnotu	ano	
zařízení obsahuje modul pro filtorvání obsahu webového provozu (Web Filtering)	ano	
modul pro filtrování webového provozu (Web filtering) pracuje na principu kategorizace webového obsahu	ano	
modul pro filtrování webového provozu (Web filtering) kategorizuje webový obsah do kategorií	phishing, spam, p2p file sharing, botnets, spyware, malicious sites, weapons, racism, pornoraphy, games, gambling, child abuse, drugs, violence, hacking	min.
modul Web filtering umožňuje monitorování navštívených kategorií na uživatele	ano	

zařízení musí podporovat funkcionalitu, která uživatele notifikuje v českém jazyce, že jeho přístup na danou webovou stránku byl zablokován na základě Web filteringu	ano	
zařízení obsahuje modul aplikační kontroly	ano	
řízení aplikací na Layer 7 na základě signatury aplikace, nikoliv dle portu	ano	
zařízení obsahuje modul Antivirus	ano	
zařízení obsahuje modul ochrany proti Botnet sítím	ano	
propustnost zařízení (Enterprise mix nebo podobná metrika) threat prevention ochrany (firewall, IPS, aplikační kontrola, antivir, web filtering)	2,2 Gbps	min.
podporovaný počet spojení za vteřinu (CpS)	11 000	min.
podporovaný počet současných živých spojení	1 200 000	min.
propustnost VPN (AES-128)	1,3 Gbps	min.
zdroje napájení - počet	2 ks	
zdroje napájení - redundantní	ano	
firewally jsou dodávány s právem aktualizace firmwaru po dobu	5 let	
podpora - součástí dodávky je i právo na update a upgrade veškerých komponent zařízení	ano	
zařízení jsou dodávána s právem aktualizace bezpečnostních signatur od výrobce po dobu	5 let	
zařízení jsou dodávána s právem aktualizace modulů od výrobce po dobu	5 let	
zařízení jsou dodávána s hardwarovou podporou výrobce na dobu	5 let	
zařízení jsou dodávána s technickou podporou výrobce na dobu	5 let	
zařízení budou dodána do sídla zadavatele již kompletovaná a zahořená	ano	
zařízení musí být určena pro český trh	ano	
zařízení musí být nová	ano	
součástí nabídky bude Prohlášení českého zastoupení výrobce nebo přímo výrobce o tom, že nabízený produkt v rámci této veřejné zakázky, je určený pro trh v České republice a bude podporován výrobcem nebo servisním střediskem výrobce na území České republiky	ano	
podpora a záruka je poskytována výrobcem zařízení nebo jeho autorizovaným partnerem nezávisle na dodavateli firewallu	ano	
podpora - poskytovaná minimálně prostřednictvím telefonní linky nebo webového formuláře musí být dostupná v režimu 24x7	ano	
podpora - musí umožňovat získání aktuálních ovladačů a manuálů adresně pro konkrétní zadané produktové, popř. sériové číslo zařízení	ano	
záruka - rychlost odezvy na nahlášenou závadu do	v den incidentu	
záruka - garance odeslání náhradního dílu na místo provozu zařízení	následující pracovní den	
záruka - dodání do místa provozu zařízení v režimu "Best Effort"	3 pracovní dny	max.
nabídka a Prohlášení musí být v češtině	ano	
zadavatel vylučuje z nabídek technologie firem, které byly označeny BIS ve výroční zprávě 2013 z 27. 10. 2014 v bodě 2.7 Kybernetická bezpečnost jako potenciálně nebezpečné	ano	

Centrální management		
NIPEZ	32413100-2	
parametr	vyžadujeme	max./min.
v případě, že bude dodáno jako hardwarový prvek a ne jako virtual appliance musí být ve formátu rackmount	ano	
v případě, že bude dodáno jako hardwarový prvek a ne jako virtual appliance musí být velikost	1U	max.
centrální management musí zpracovávat logy ze všech firewallů (datacentrové, pobočkové i stávající firewally Zadavatele)	ano	

centrální management musí umět sdružovat logy ze všech firewallů do jednoho reportu (datacentrové, pobočkové i stávající firewally Zadavatele)	ano	
centrální management musí umožňovat odesílání logů do externího úložiště pomocí protokolu SYSLOG v reálném čase	ano	
zařízení musí být schopno odesílat logy na systém Wazuh	ano	
centrální management musí umožňovat reportování aktivit na síti v reálném čase	ano	
centrální management musí umožňovat prohlížení událostí firewallů v reálném čase	ano	
centrální management musí umožňovat reportování trendů na síti nad událostmi, které je zařízení schopno sledovat	ano	
logovací server musí podporovat fulltext prohledávaní logů	ano	
logovací server musí podporovat indexaci logů pro prohledávání	ano	
management nástroj musí umožňovat statistiky počtu spojení pro jednotlivá pravidla za účelem optimalizace bezpečnostní politiky	ano	
centrální management musí umožňovat automatickou verifikaci politiky proti redundanci	ano	
centrální management musí umožňovat automatickou verifikaci politiky proti překryvu pravidel	ano	
centrální management musí obsahovat certifikační autoritu za účelem vydávaní a správy PKI certifikátů pro jednotlivé firewally a VPN (může být zabezpečeno produktem třetí strany, musí být součástí nabídky)	ano	
firewallová pravidla musí být možno vytvářet jednoduše a intuitivně v grafickém prostředí využíváním objektů aplikace	ano	
možnost definovat pravidla pro jednotlivé firewally (virtuální i fyzické)	ano	
možnost definovat společná pravidla pro více firewallů	ano	
podpora řízení oprávnění administrátorských rolí s možností přidělování práv (minimálně read-only, read-write) pro jednotlivé skupiny administrátorů	ano	
podpora práce více administrátorů najednou	ano	
sada objektů pro tvorbu pravidel a politik	uživatel, skupina, IP adresa, dynamický objekt, síť, protokol, aplikace, kategorie webového obsahu, čas	min.
podpora vyhledávaní v pravidlech firewallů na základě vstupních údajů typu	uživatel, skupina, IP adresa, dynamický objekt, síť, protokol, aplikace, kategorie webového obsahu, text	
pro tvorbu pravidel a politik je možné použít i název služby	ano	
integrovaný monitoring v grafickém rozhraní musí být schopen sledovat parametry firewallu v reálnem čase	ano	
integrovaný monitoring musí být schopen sledovat veličiny - využití paměti	ano	
integrovaný monitoring musí být schopen sledovat veličiny - využití CPU	ano	
integrovaný monitoring musí být schopen sledovat veličiny - počet navázaných spojení	ano	
integrovaný monitoring musí být schopen sledovat veličiny - počet nově otevřených spojení za sekundu, propustnost	ano	
integrovaný monitoring musí být schopen sledovat veličiny - propustnost	ano	
Zadavatel umožňuje pro provoz Management serveru firewallů použít virtuální prostředí Zadavatele	ano	
virtuální prostředí Zadavatele	Hyper-V 2019	