čj. 28054-7/2020-VLRZ/R/ZR
RIS: 2020/OU1/15/000041

K U P N Í S M L O U V A

Vojenská lázeňská a rekreační zařízení
Právní forma: příspěvková organizace
se sídlem 101 00 Praha - Vršovice, Magnitogorská 1494/12
zastoupená ředitelem Ing. Milanem Lauberem, Ph.D.
zapsána: u živnostenského odboru Úřadu městské části Praha 10
IČ: 00000582
DIČ: CZ00000582
bankovní spojení:
číslo účtu: [redacted]
(dále jen kupující)

jednáním ve věcech technických a za převzetí předmětu plnění je pověřen
Ing. Antonín Křáp, tel. 602 236 609

FIRMA: NWS s.r.o.
se sídlem: Haštalská 796/3, 110 00 Praha 1
zastoupená Ing. Pavlem Čeřovským, jednatelem
zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze, oddíl C, vložka 96134
IČ: 27098931
DIČ: CZ27098931
bankovní spojení: [redacted]
číslo účtu: [redacted]
(dále jen prodávající)

uzavřeli níže uvedeného dne, měsíce a roku
dle zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů tuto
kupní smlouvu veřejné zakázky malého rozsahu na dodávky zadané prostřednictvím elektronického tržiště NEN pod evidenčním číslem **N006/20/V00021450**

I.
Předmět plnění

I.1. Prodávající touto smlouvou prodává za podmínek v ní dohodnutých kupujícímu následující předmět plnění a kupující tento předmět kupuje.

I.2. Předmětem plnění je dodávka systému pro ochranu perimetru sítě včetně souvisejících úkonů a nákladů nutných pro řádné a včasné splnění předmětu plnění. Podrobný popis předmětu plnění obsahují přílohy č. 1 a 2 této smlouvy. Součástí předmětu plnění je servisní podpora po dobu 36 měsíců od podpisu předávacího protokolu (článek III.1.).

I.3. Spolu s předmětem plnění bude prodávajícím kupujícímu předáno i povinné a dohodnuté příslušenství a vybavení, návody, záruční listy, jiné doklady a listiny, které jsou nezbytné pro užívání předmětu plnění.

I.4. Prodávající bude garantovat, že předmět plnění bude splňovat podmínky dané příslušnými ustanoveními a zásadami zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

II.
Doba a místo plnění

II.1. Předmět plnění, popsaný v článku I. této smlouvy je prodávající povinen **dodat do 8 týdnů od účinnosti smlouvy** na adresu **101 00, Praha – Vršovice, Magnitogorská 1494/12.** Přesný termín předání je prodávající povinen předem dohodnout s osobou pověřenou k převzetí předmětu plnění.

III.
Povinnosti smluvních stran

III.1. Prodávající je povinen předat předmět plnění kupujícímu (osobě pověřené k převzetí předmětu plnění) v dohodnutém množství a kvalitě v místě plnění. O předání a převzetí předmětu plnění včetně všech souvisejících služeb bude sepsán předávací protokol. Kupující je povinen tento předmět od prodávajícího převzít, potvrdit prodávajícímu jeho převzetí a uhradit sjednanou cenu.

III.2. Převzetím předmětu plnění se stává kupující jeho vlastníkem a přechází na něj nebezpečí škody na prodané věci.

III.3. Prodávající poskytuje kupujícímu záruku za jakost a servisní podporu na předmět plnění v délce **36 měsíců,** s dobou odezvy NBD (do dalšího pracovního dne), počínaje dnem splnění závazku (článek III.1. této smlouvy) z této smlouvy a po tuto dobu garantuje jeho obvyklou funkčnost. V rámci záruční doby prodávající garantuje výměnu za produkt ve stejné konfiguraci nebo zprovoznění u objednatele.

III.4. Prodávající se zavazuje, že ke dni dodání předá kupujícímu e-mailové adresy, telefonní čísla, a www adresu portálu, na kterých bude možné nahlásit reklamovanou vadu. Tento seznam bude nedílnou součástí zápisu o předání a převzetí. Po nahlášení vady musí prodávající elektronicky (e-mailem) potvrdit datum a čas jejího nahlášení.

III.5. Prodávající se zavazuje zajistit v rámci záruční doby servisní podporu s následujícími parametry:

a) přístup k webovému zákaznickému centru s možností sledování servisních reportů prostřednictvím Internetu. Podpora musí být v českém jazyce.
b) podporu telefonem a e-mailem v českém jazyce, v pracovních dnech, v pracovní době (8:00 až 16:00).
c) vady musí být odstraněny v co nejkratším technicky možném termínu, nejpozději však do 5 pracovních dnů od nahlášení.

III.6. Prodávající poskytne kupujícímu po dobu trvání servisní podpory všechny relevantní SW aktualizace nabízené výrobcem tak, aby dodané řešení vyhovovalo zadání a fungovalo bez závad. Prodávající se zároveň zavazuje informovat kupujícího o nových SW verzích a funkčnostech, které mohou rozšiřovat dodané řešení způsobem, který kupující shledá ve shodě s potřebami dalšího rozvoje dodaného řešení.

III.7. Prodávající je povinen řádným způsobem uzavřít dohodu o podpoře s výrobcem zařízení tak, aby v případě závady na dodaných zařízeních, kterou není prodávající schopen sám odstranit, mohl kupující tuto závadu sám eskalovat přímo k výrobci zařízení. Zároveň je prodávající povinen zajistit kupujícímu přístup k dokumentaci výrobce zařízení a znalostní bázi, kterou výrobce v rámci své podpory poskytuje. V databázi výrobce musí být kupující veden jako první uživatel zboží. Kupující požaduje originální a nová zařízení. Zboží musí být nepoužité a nerepasované. Kupující je povinen doložit potvrzení od výrobce o určení dodávaného HW pro český trh (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.

III.8. Kupující má nárok na výměnu předmětu plnění v případě, kdy se na něm v záruční době vyskytnou tři a více závad bránících jeho užívání, nebo má právo postupovat dle č. VI. této smlouvy.

IV.
Kupní cena plnění a platební podmínky

IV.1. Kupní cena předmětu plnění zahrnuje veškeré dodávky a činnosti včetně podpory za 36 měsíců, vyplývající z této smlouvy a ze zadávacích podkladů, a o kterých prodávající podle svých odborných znalostí měl vědět, že jsou k řádnému a kvalitnímu dodání a zprovoznění předmětu plnění potřeba (např. doprava, poštovné, balné atp.) a činí:

453 845,- Kč bez DPH

DPH bude účtováno v aktuální platné sazbě.

IV.2. Kupní cena bude uhrazena prodávajícímu po dodání a převzetí kompletní dodávky předmětu plnění na určené místo plnění bez vad na základě faktury, vystavené prodávajícím. Podkladem pro fakturaci bude předávací protokol podle článku I.3.

IV.3. Zálohy na kupní cenu nebudou ze strany kupujícího poskytnuty.

IV.4. Faktura musí obsahovat náležitosti daňového dokladu dle zákona č. 235/2004 Sb. a dle zákona č. 89/2012 Sb., občanského zákoníku. Dále na ní bude uvedeno číslo smlouvy a lhůta splatnosti, která činí 21 dnů od doručení kupujícímu. V případě, že faktura nebude mít odpovídající náležitosti je kupující oprávněn zaslat tento doklad zpět prodávajícímu k doplnění. Lhůta splatnosti doplněné faktury běží znovu ode dne jejího doručení kupujícímu.

IV.5. Kupující je oprávněn, od jakéhokoli finančního plnění dle tohoto článku odečíst částku připadající na jeho i nesplatné nároky (např. náhrada škody, smluvní pokuta, apod.) vyplývající z této smlouvy.

V.
Smluvní pokuty

V.1. Prodávající se zavazuje zaplatit kupujícímu smluvní pokutu za nesplnění termínu předání předmětu plnění ve výši **0,5 %** z celkové ceny vč. DPH, a to za každý i započatý den prodlení, nedodá-li předmět plnění řádně a včas.

V.2. Za každé nenastoupení k odstranění záručních vad předmětu plnění v dohodnutém termínu se prodávající zavazuje zaplatit smluvní pokutu ve výši 0,1 % z celkové ceny předmětu plnění vč. DPH za každý i započatý kalendářní den prodlení.

V.3. Za nesplnění každého dohodnutého termínu pro odstranění záručních vad předmětu plnění se prodávající zavazuje zaplatit samostatnou smluvní pokutu ve výši 0,1 % z celkové ceny předmětu plnění vč. DPH za každý i započatý kalendářní den prodlení.

V.4. Povinnost zaplatit smluvní pokutu je dána bez ohledu na zavinění prodávajícího. Tím není dotčeno právo kupujícího na náhradu škody.

VI.
Odstoupení od smlouvy

VI.1. Tato smlouva zaniká v následujících případech:

a) Splněním všech závazků z této smlouvy;
b) Písemnou dohodou smluvních stran;
c) Jednostranným odstoupením kupujícího od smlouvy pro její podstatné porušení ze strany prodávajícího;
d) Jednostranným odstoupením kupujícího od smlouvy v případě zahájení insolvenčního řízení vůči prodávajícímu;
e) Kdy je s přihlédnutím ke všem okolnostem zřejmé, že prodávající není schopen dostát svému závazku z této smlouvy, tj. dodat předmět plnění řádně a včas.

VI.2. Za podstatné porušení smlouvy ze strany prodávajícího se považuje:
a) Prodlení prodávajícího s termínem uvedeným v čl. III. Této smlouvy delší než 30 kalendářních dnů;
b) Prodávající neodstranil do 14 kalendářních dnů vadná plnění či nedostatky, na které byl kupujícím písemně upozorněn.

VI.3. Odstoupení od smlouvy musí být provedeno písemně, jinak je neplatné. Odstoupení od smlouvy musí být doručeno druhé smluvní straně.

VII.
Závěrečná ustanovení

VII.1. Smlouva je uzavřena a nabývá platnosti dnem podpisu poslední smluvní stranou.Smlouva nabývá účinnosti dnem jejím zveřejněním v registru smluv v souladu se zákonem č. 340/2015 Sb., zákon o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv) ve znění pozdějších předpisů.

VII.2. Smlouvu lze měnit a doplňovat pouze po dohodě smluvních stran formou písemných dodatků, podepsaných zástupci smluvních stran.

VII.3. Tato smlouva se pořizuje ve dvou vyhotoveních, každé s platností originálu. Každá ze smluvních stran obdrží po jednom vyhotovení. Prodávající se zavazuje, že poskytne kupujícímu smlouvu

včetně příloh ve strojově čitelném formátu. V případě, že tato smlouva bude uzavírána v elektronické podobě, považuje se za její podepsání připojení zaručeného elektronického podpisu osoby v souladu s dikcí nařízení Evropského Parlamentu a Rady č. 910/2014 (nařízení eIDAS). Smlouva je v elektronické podobě uzavřena připojením zaručených elektronických podpisů obou smluvních stran.

VII.4. Text tohoto smluvního ujednání vč. dodatků bude zveřejněn v registru smluv v souladu se zákonem o registru smluv.

VII.5. Smluvní strany prohlašují, že se se smlouvou řádně seznámily a s jejím obsahem souhlasí, což stvrzují svými podpisy.

VII.6. Tato smlouva se řídí úpravou dle zák. č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

V …… dne ……

V Praze dne…….

Za kupujícího:

Za prodávajícího:

_____

ředitel VLRZ
Ing. Milan Lauber, Ph.D.

_____

jednatel *(popř. jiný statutární orgán)*

Seznam příloh:
Příloha č. 1: Specifikace předmětu plnění
Příloha č. 2: Technická specifikace předmětu plnění

Specifikace předmětu plnění

Komponenty pro zabezpečení perimetru sítě:

	Obecný popis	Konkrétní označení
2ks	Next-Generation Firewallu provozovaného ve vysoké dostupnosti včetně aktivované funkcionality IPS (Intrusion Prevention System).	FPR1140-FTD-HA-BUN
1ks	centrální management do virtuálního prostředí VMware (min. pro 2 zařízení).	FS-VMW-2-SW-K9
100ks	licence VPN klienta pro koncová zařízení platná 36 měsíců	L-AC-PLS-3Y-S2

• Nahrání posledního stabilního operačního systému ASA software.
• Sestavení HA clusteru active/passive.
• Přenesení současné konfigurace firewallu Cisco ASA na nově dodané firewally.
• Analýza konfigurace, optimalizace/redukce pravidel.
• Upgrade/re-image operačního systému ASA software na Next-Generation OS.
• Instalace centrálního managementu pro správu operačního systému Next-Generation na nových firewallech.
• Aktivace a ladění Intrusion Prevention System funkcionality.
• Vypracování detailní technické dokumentace.

Veškeré instalace budou probíhat za plného provozu a musí být prodávajícím provedeny tak, aby implementace nového zařízení neměla vliv na stávající provoz sítě.

Technická specifikace

Dodané zařízení musí splnit (nebo převýšit) všechny technické parametry uvedené v následující tabulce.

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Uchazeč dle nabízeného zařízení**
Výrobce zařízení	Uvedení výrobce	Cisco
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	Firepower 1140
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	https://www.cisco.com/c/en/us/products/collateral/security/firepower-1000-series/datasheet-c78-742469.html
Typ zařízení	NGFW/NGIPS	NGFW
Formát zařízení	Appliance, 1RU	HW appliance 1RU
Minimální počet 10/100/1000 BaseT rozhraní dedikovaných pro management	1	1x 1Gbit RJ45
Minimální počet 10/100/1000 BaseT portů	8	8x 1Gbit RJ45
Minimální počet SFP portů	4	ANO 4x1 Gbit SFP
EAL4+ certifikace	ANO	ANO
Podporovaný počet současně otevřených spojení přes FW	400 000	400 000
Rychlost vytváření nových spojení přes FW	22K	22 000
Propustnost aplikačního FW (next-gen FW) – (top parametry)	2,2 Gbps	2,2 Gbit/s
Propustnost aplikačního FW + IPS (next-gen FW, IPS)	2,2 Gbps	2,2 Gbit/s
Podpora L2 (transparentního) módu s podporou NAT a PAT	ANO	ANO
Podpora L3 (routovaného) módu s podporou NAT a PAT	ANO	ANO
Redundance jednotlivých komponent v navrhované síti (fail-over bez přerušení spojení)	ANO	ANO
Podpora stateful failover	ANO, active/standby	ANO
Podporovaný počet VLAN	Min. 1024	1024
Možnost sloučení více fyzických rozhraní do jednoho logického s rozkladem zátěže a podorou LACP	Ano	ANO
Dynamické směrování - podpora alespoň RIP, OSPF, BGP	Ano	ANO
Podpora IPv6 dynamického směrování – alespoň OSPFv3, BGP	Ano	ANO
Podpora Policy based Routing	Ano	ANO

Podpora kontroly paketů TCP provozu s ochranou před útoky jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod.	Ano	ANO
Podpora filtrace IPv4, IPv6	Ano	ANO
Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD	Ano	ANO
Podpora filtrace podle bezpečnostních skupinových rolí přiřazených na přístupových přepínačích	Ano	ANO
Podpora inspekce IPv6 provozu	Ano	ANO
Možnost filtrace komunikace Botnet sítě s využitím databází o důvěryhodnosti adres v Internetu	Ano	ANO
Podpora NAT64 a DNS64	Ano	ANO
Možnost integrace cloudových bezpečnostních bran s transparentním směrováním určitého provozu na tyto prvky a zde prováděnou inspekci na škodlivý kód připadně pro řízení přístupu podle uživatelské identity, typu aplikace, apod.	Ano	ANO
Funkce QoS až na úrovni jednotlivých toků (flow) s podporou LLQ	Ano	ANO
Možnost rozšíření o funkce NextGen FW	Ano	ANO
Možnost rozšíření o funkce NextGen IPS	Ano	ANO
Bezpečnostní pravidla mohou kromě adres a portů zohlednit i identitu uživatele	Ano	ANO
Zohlednění kontextových informací o koncovém zařízení (typ, stav, spod.) a využití ve filtrech	Ano	ANO
API rozhraní pro sdílení kontextových informací s dalšími systémy	Ano	ANO
Možnost začlenit do SDN řešení – kontrolerem řízená infrastruktura (APIC)	Ano	ANO
Funkce VPN		
Maximální počet VPN připojení	alespoň 400	400
Podporované protokoly VPN	SSL/IPSEC (ikev1, ikev2)	ANO
Propustnost IPSEC	Alespoň 1,2 Gbps	1,2 Gbit/s
Možnost Autentizace/Autorizace/Accounting u VPN pomocí Externího serveru	LDAP / RADIUS	ANO (LDAP, RADIUS)
Možnost klasifikace VPN provozu a filtrovaní pomocí SGT	Ano	ANO
Funkce IPS a anti-malware		
Možnost definovat typ provozu předávaný k inspekci do IPS	Ano	ANO
Podpora také IDS režimu – pasivního monitorování (TAP režim)	Ano	ANO
Možnost definovat režim provozu při zahlcení nebo nedostupnosti IPS funkcí (fail open, fail close)	Ano	ANO

Možnost obejití IPS funkcí při zahlcení nebo nedostupnosti	Ano	ANO
Podpora 802.1Q tagovaných rámců	Ano	ANO
Podpora různých IPS politik pro různé typy provozu	Ano	ANO
Inspekce pro IPv4 i IPv6	Ano	ANO
Podpora funkce Adaptivní konfigurace filtrů, která upozorní, případně vypne filtr, který může způsobit zahlcení systému	Ano	ANO
IPS musí obsahovat filtry/signatury popisující exploity, zranitelnosti, krádeže identity, spyware, viry, průzkumné aktivity, ochranu síťové infrastruktury, IM aplikace, P2P sítě a nástroje na kontrolu toku multimédií	Ano	ANO
Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s poškozenou reputací	Ano	ANO
Podpora aplikace pro psaní zákaznických filtrů	Ano	ANO
Podpora importu komunitních filtrů/signatur Snort	Ano	ANO
IPS musí umět detekovat a blokovat útoky průzkumných aktivit	Ano	ANO
IPS musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS	Ano	ANO
IPS musí umět detekovat a blokovat útoky na základě IP adresy, nebo DNS jména „known bad host“ jako je spyware, phishing nebo Botnet C&C	Ano	ANO
IPS musí umět detekovat a blokovat útoky proti síťové infrastruktuře firmy, jako jsou přepínače, routery, firewall, bezdrátové přepínače a podobně. Dále musí poskytovat i ochranu pro protokoly využívané v IP telefonii	Ano	ANO
Odkaz na CVE a dokumentaci ke známým bezpečnostním incidentům přímo hyperlinkovým odkazem z dané bezpečnostní události	Ano	ANO
Možnost vyhledávání typu signatury v centrální databázi dodavatele podle typu a závažnosti útoku	Ano	ANO
Podpora vrstvev IPS politik s možností volit předdefinované politiky v základní vrstvě orientované na bezpečnost nebo naopak minimalizace false-positive	Ano	ANO
Možnost aplikace vrstvy doporučených politik, kterou generuje přímo IPS podle pasivního sledování lokálního prostředí	Ano	ANO
Možnost definice uživatelské vrstvy politik	Ano	ANO
Předefinování pravidel přes vrstvy IPS politik = platí relevantní pravidla v nejvyšší vrstvě IPS politik	Ano	ANO

Různé politiky lze sdílet a aplikovat na různé senzory	Ano	ANO
Podpora aktivní inline ochrany před malware s detekcí známých nebo podezřelých malware nezávislé na aktuálních databázích AV dodavatelů	Ano	ANO
IPS musí být možné nasadit plně transparentně k existujícímu síťovému prostředí a jeho nasazení nesmí být podmíněno rekonfigurací stávajících aktivních prvků	Ano	ANO
Možnost definovat pravidla chování sítě a komponentů, pro automatickou detekci tzv. „compliance violation“	Ano	ANO
Možnost automatické i manuální klasifikace stanice jako “kritické” se zohledněním v pravidlech, reportech apod.	Ano	ANO
Podpora „remediation“ modulů pomocí nichž lze ovládat další prvky infrastruktury a aplikovat filtry, směrování, apod.	Ano	ANO
Otevřené rozhraní pro uživatelsky vytvářené „remediation“ moduly	Ano	ANO
Podpora databází reputací adres v Internetu (Security Intelligence)	Ano	ANO
Funkce Next-Gen FW		
Možnost definovat různé přístupové politiky pro různé typy provozu, např. podle domén, VLAN, konkrétních FW, apod.	Ano	ANO
Podpora pasivního monitorování (TAP režim)	Ano	ANO
Podpora 802.1Q tagovaných rámců	Ano	ANO
Podporovaných aplikací	Min. 3000	Více než 4000
Kategorie aplikací (nebezpečné, důležité, apod.)	Ano	ANO
URL kategorií	80	Více než 80
Katagorizovaných světových URL	280 milionů	Více než 280 miliónů
Řízení přístupu k WWW - Web Usage Control (WCU)	Ano	ANO
Filtrace podle typů aplikací webových i ne-webových	Ano	ANO
Filtrace podle reputace serverů	Ano	ANO
SSL inspekce (dekrypce/enkrypce)	Ano	ANO
Security Inteligence database – známé uzly botnet sítí C&C	Ano	ANO
Security Inteligence database – známé adresy anonymních proxy, otevřených mail relay, apod.	Ano	ANO
Security Inteligence database – známé nebezpečné URL adresy a jmenné domény	Ano	ANO
Možnost integrovat vlastní reputační databáze	Ano	ANO
Podpora komunitních, otevřených standardů popisu apliací (OpenAppID)	Ano	ANO
Filtry mohou zohlednit roli a identitu uživatele	Ano	ANO
Podpora rozhraní pro sběr informací o síťové komunikaci z prvků infrastruktury – přepínače, směrovače (např. netflow)	Ano	ANO

Využití informací z prvků infrastruktury (např. netflow) pro monitorování a detekci chování sítě	Ano	ANO
Řešení musí být schopné pasivního sběru informací o síťových zařízení a zobrazení:	Typ zařízení	ANO
	Operační systém	
	Dodavatel OS	
	Použité síť. protokoly	
	Použité síť. služby	
	Otevřené porty síť. služeb	
	Potenciální zranitelnosti	
Přehled o síťových spojení má poskytovat minimálně tyto informace:	Čas startu a konce flow	ANO
	Akce (allow, deny,..)	
	Důvod případného blokování	
	Zdroj. a cíl. adresa	
	Vstupní a výstupní zóna	
	Vstupní a výstupní rozhraní	
	Zdroj. a cíl. port	
	Aplikační protokol	
	IPS událost, pokud vznikne	
	Riziková úroveň IPS události	
	Použitá síťová aplikace	
	Rizikovost aplikace	
	„Business impact“ aplikace	
	Množství přenesených dat	
Správa		
Vzdálené správa přes grafické rozhraní bez nutnosti instalace zvláštního SW	Ano	ANO
Přístup ke GUI http/https protokolem	Ano	ANO
Možnost vzdáleného přístupem protokolem ssh přímo do FW	Ano	ANO
Možnost přístupu k textovým logům (syslog) přímo ve FW	Ano	ANO
Možnost centrální správy při nasazení více firewallů	Ano	ANO
Při centrální správě: možnost sdílených bezpečnostních politik	Ano	ANO
Distribuce a správa software firewallu, bezpečnostních update (IPS signatury, databáze zranitelností, Security Intelligence databáze, geolokační databáze, apod.), konfigurací, licencí, atd. z grafického rozhraní managementu	Ano	ANO
Zobrazení logů a událostí v grafickém rozhraní správy	Ano	ANO

Možnost zaslání informace o TCP nebo UDP toku procházejícím firewallem (start a konec spojení, identifikovaný uživatel, přenesený objem dat, typ služby, délka trvání spojení) na TACACS nebo RADIUS server.	Ano	ANO
Nástroje pro troubleshooting, testování průchodu paketu firewallem, zachytávání provozu pro pozdější vyhodnocování	Ano	ANO
Funkce IPS a Next-Gen FW vyžadující dlohodobější ukládání dat, korelace, reporty, apod. musí být spravovatelné z centrálního monitorovacího a konfiguračního sytému (centrální dohledové konzole)	Ano	ANO
Centrální dohledová konzole musí být schopna dohledovat a spravovat více IPS senzorů a Next-Gen FW funkcí pro možnost korelace, sdílení politik, centrální sledování zdraví boxů, apod.	Ano	ANO
Centrální dohledová konzole musí být schopna poskytovat aktualizaci a distribuci filtrů/signatur automaticky, manuálně a podle časového harmonogramu	Ano	ANO
Trendy, historické přehledy a statistiky z pohledu aplikací, stanic, komunikace, bezpečnostních incidentů jsou graficky a tabulkově zobrazeny v GUI dohledové konzole	Ano	ANO
Přehledy a statistiky na dohledové konzoli lze efektivně filtrovat podle času, typů incidentů, aplikací, koncových stanic	Ano	ANO
Centrální dohledová konzole musí být schopna vytvářet reporty manuálně a podle časového harmonogramu	Ano	ANO
Pro reporty lze definovat template definující formát a obsah reportu	Ano	ANO
Pro template reportů lze definovat proměnné, které se promítnou v aktuálním reportu	Ano	ANO
V grafickém rozhraní dohledové konzole lze definovat uživatelské dashboardy typu top-N	Ano	ANO
Dashboardy použité v GUI dohledové konzole lze rovnou zahrnout i do reportů	Ano	ANO
Centrální dohledová konzole musí být schopna exportovat reporty do formátů, jako jsou PDF, HTML, CSV, apod.	Ano	ANO
Centrální dohledová konzole musí být schopna integrace s Microsoft AD pro vytváření bezpečnostních politik podle uživatele a skupiny uživatelů.	Ano	ANO
Podpora korelace událostí na centralizované dohledové konzoli s definicí odpovídajících akcí, např. zaslání korelované události na SIEM, generování mailu, lokální události, apod.	Ano	ANO
Podpora posílání událostí formou syslog, email, SNMP na externí platformy	Ano	ANO

Podpora Event Streamer API (eStreamer) pro sdílení informací se externími systémy. Minimálně pro tyto SIEM:	ArcSight	ANO
	BMC Remedy	
	Trustwave	
	NetForensics	
	Novell Sentinel	
	Hawk Network Defense	
	Q1Labs-QRadar	
	Log Rhythm SIEM 2.0	
	LogLogic	
	Splunk	
Pro zprávy odesílané emailem je podpora také autentizovaného SMTP pro komunikaci s mail relay	Ano	ANO
Podpora JDBC API pro přístup z externích systémů k databázím centralizovaného managementu	Ano	ANO
Podpora řízeného přístupu podle rolí administrátorů	Ano	ANO
Definice dostupných funkcí v GUI centralizované dohledové konzole podle role administrátora	Ano	ANO
Možnost založit pro daný incident „ticket“ přímo v prostředí GUI managementu	Ano	ANO
Workflow pro předávání „ticketů“ mezi administrátory	Ano	ANO
Konkrétní bezpečnostní incident až na úrovni paketu lze přiložit k danému „tiketu“ pro další analýzu	Ano	ANO
Možnost definice politik pro sledování odpovídajících parametrů „zdraví“ na senzorech a centralizované konzoli (zařízení CPU, obsazení paměti, komunikace s cloudovými službami, apod.)	Ano	ANO
Zákaznicky definovatelné limity a akce spojené s jejich překročením při vyhodnocení sledovaných parametrů „zdraví“	Ano	ANO
Různé politiky pro sledování „zdraví“ lze aplikovat na různé senzory nebo centralizovanou konzoli	Ano	ANO