Kúpna zmluva č. Z201539918_Z

Uzatvorená v zmysle §409 a nasl. Obchodného zákonníka

I. Zmluvné strany

1.1 Objednávateľ:

Obchodné meno:	Hlavné mesto Slovenskej republiky Bratislava
Sídlo:	Primaciálne námestie 1, 81499 Bratislava-Staré Mesto, Slovenská republika
IČO:	00603481
DIČ:	2020372596
IČ DPH:	
Číslo účtu:	SK7275000000000025827813CEKOSKBX
Tel:	+421 259356342

1.2 Dodávateľ:

Obchodné meno:	TooNet, s.r.o.
Sídlo:	Seberiniho 1, 82103 Bratislava, Slovenská republika
IČO:	44962070
DIČ:	2022885601
IČ DPH:	SK2022885601
Číslo účtu:	
Tel:	+421903281193

II. Predmet zmluvy

2.1 Všeobecná špecifikácia predmetu Zmluvy:

Názov:	Nákup informačno komunikačnej technológie
Kľúčové slová:	aktívne sieťové prvky (switche, firewall a VPN systémy na obnovu informačno komunikačnej infraštruktúry WAN/LAN siete.
CPV:	32410000-0 - Lokálne siete (LAN); 32412110-8 - Sieť internet; 32413100-2 - Sieťové smerovače; 32420000-3 - Sieťové zariadenia; 32422000-7 - Sieťové komponenty; 32424000-1 - Infraštruktúra siete; 32430000-6 - Sieť WAN; 60000000-8 - Dopravné služby (bez prepravy odpadu)
Druh/y:	Tovar; Služba
Kategória služieb:	2. Služby pozemnej dopravy, vrátane služieb pancierových automobilov a kuriérskych služieb okrem prepravy poštových zásielok

2.2 Funkčná špecifikácia predmetu Zmluvy:

- Náhrada morálne zastaranej a fyzicky opotrebovanej komunikačnej infraštruktúry. srdcom novej infraštruktúry bude next generation firewall od spoločnosti Palo Alto Networks a zariadenie FortiNet.
- Palo Alto firewal bude zabezpečovať nasledovné služby:
- Ochrana siete pomocou TCP IP a aplikačného firewallu vrátane NAT, port forwardingu, smerovania,
- DNSProxy,
- IPSECaSSLVPN,
- URL filtráciu - filtrovanie prístupu na webové stránky na základe identity používateľa,
- Filtrácia aplikácii a služieb na základe identity používateľa,
- Ochranu komunikácie pred zraniteľnosťami (Antispam, Antivir, Anti-spyware, IPS),
- QoS.
- Na firewalle bude vytvorených nikoľko oddelených bezpečnostných zón:
- - Internet

- - DMZ - vypublikované služby
- - DMZ - email relay
- - LAN - lokálne pracovné stanice
- - MNGT - manažment zariadení a serverov
- - Servers - segment pre pripojenie serverov
- - Wifi - segment pre verejnú WiFi
- - VPN vzdialený používatelia

- Medzi zónami (DMZ) bude povolená iba nevyhnutná a schválená komunikácia, ktorá bude kontrolovaná na prítomnosť škodlivého obsahu.
- Všetka šifrovaná komunikácia (IPSEC VPN, SSL VPN a HTTPS) bude ukončovaná na firewale na vstupe z Internetu a bude smerovaná na zariadenie FortiNet, autentifikovaná, následne skontrolovaná a prepustená do internej siete objednávateľa.
- Na prepínačoch budú nakonfigurované prostredníctvom VLAN jednotlivé segmenty do ktorých sa pripoja jednotlivé zariadenia.
- Pre zabezpečenie ochrany emailovej komunikácie bude implementované zariadenie FortiMail.
- Cez toto zariadenie bude smerovaná všetka emailová komunikácie, ktorá tu bude skontrolovaná či nejde o spam a na prítomnosť vírusov a malware. V prípade že email je v poriadku bude následne doručený do emailovej schránky príjemcu.
- Pre vyriešenie problémov s WiFi prístupmi bude použitý kontrolér pre riadenie prístupu. Acces pointy (AP) budú zabezpečovať dve hlavné funkcie: poskytovať bezdrôtovú komunikáciu s koncovými užívateľmi a vytvorenie IPSEC tunela medzi AP a centrálnym kontrolérem.
- Uvedená architektúra umožní centrálnu správu a vytvorenie viacerých SSID pre rozdelenie používateľov (napr voľná wifi, zmluvný klienti, VIP) a nastavenie rôznych parametrov ako napr riadenie šírky pásma, používanie aplikácií a pod.
- Toto riešenie umožní aplikovanie ďalších služieb ako autentifikácia používateľov, propagácia služieb (web stránka mesta, reklama, akcie) vyhodnocovanie správania používateľov a pod.
- Poskytované služby je možné rozšíriť prostredníctvom aplikácie s lokalizačnými službami, ktorá značne zlepší dojem návštevníkov poskytnutím špecializovaného obsahu pre lokáciu smerových inštrukcií, notifikácii a pod.

2.3 Technická špecifikácia predmetu Zmluvy:

Technické vlastnosti	Jednotka	Minimum	Maximum	Presne
Firewall & Proxy:	0			0
Palo Alto Networks PA-3020, PN: PAN-PA-3020	ks			1
Partner enabled premium support year 1, PA-3020, PN: PAN-SVC-BKLN-3020	ks			1
Bright cloud URL Filtering subscription year 1, PA-3020, PN: PAN-PA-3020-URL2	ks			1
Threat prevention subscription for device renewal, PA-3020, PN: PAN-PA-3020-TP	ks			1
Instalation & configuration services Palo Alto	hod	1	20	
IPSEC&SSLVPNconection:	0			0
20 X GE RJ45 ports (including 1 x DMZ port,1 x Mgmt port,2 x HA port,16 X internal switch ports),2 x shared media pairs (including 2 x GE RJ45, 2 x GE SFP slots),32GB onboard storage.Max managed FortiAPs (Total/Tunnel)64/32,Hardware plus 1 year 8x5 FortiCare and FortiGuard UTM Bundle,PN:FG-100D-BDL	ks			1
10 X GE RJ45 ports (including 7 x Internal ports, 2 x WAN ports, 1 X DMZ port). Max managed FortiAPs (Total / Tunnel) 10/5, PN: FG-60D	ks			2
FortiGate 60D 1 Year 8x5 Enhanced FortiCare, PN: FG-10-0060D-311-02-12	ks			2
FortiGate 30D 5 x GE RJ45 ports (Including 1 x WAN port, 4 x Switch ports). Max managed FortiAPs (Total / Tunnel) 2 / 2, PN: FG-30D	ks			3
FortiGate 30D 1 Year 8x5 Enhanced FortiCare, PN: FG-10-00034-311-02-12	ks			3
Instalation & configuration services FortiGate	hod	1	20	
Email filtering:	0			0
FortiMail-VM software "virtual appliance" designed for virtualization platforms. 2 x vCPU cores, PN: FML-VM02	ks			1

FortiMail VM02 8x5 FortiCare plus FortiGuard Bundle Contract 1 Year, PN:FC-10-0VM02-965-02-12	ks			1
HP ProLiant DL360 G9 E5-2650v3 2.3GHz 10-core 2P 64GB-R P440ar/2GB 4x1Gb 2x800W RPS Perf Server, 2x300GB 10K rpm, 2x1,2 TB SAS 10K rpm HDD, PN: 755263-B21	ks			1
Synology RackStation RS3412xs, PN: RS3412xs	ks			1
WD SE Raid Edition 3000 GB, PN: WD3000F9YZ	ks			4
VMware vSphere Essentials Plus Kit, PN: VMware	ks			1
Vmware vSphere Essentials Plus Kit Production Support & Subscription, PN: WMware	ks			1
Instalation & configuration services FortiMail filtering	hod	1	20	
Prepínače:	0			0
Summit X460-G2 48 x 10/100/1000BASE-T, 4x1000/10GBaseX unpop'd SFP+ ports, Rear VIM Slot (unpop'd). Rear Timing Slot(unpop'd),2 unpop'd PSU slots,fan module slot(unpop'd),ExtremeXOS Edge license, PN:16702	ks			2
Summit X460-G2 48 FAN Module for Summit X460-G2 Series Switches-front to back airflow, PN:10945	ks			2
Summit X460-G2 48 300W AC Power Supply module for Summit X460,X460-G2 & E4G-400 Series Switches-Extended Temperature Range from-10 to+50 degrees Celsius, PN:10930A	ks			2
Summit X460-G2 48 PWP TAC & OS Summit 16702, PN:97004-16702	ks			2
Summit X440-48t 48 x 10/100/1000BASE-T,4x1000BASE-X unpopulated SFP(4 SFP ports shared with 10/100/1000BASE-T ports),SummitStack Stacking ports,1 AC PSU,ExtremeXOS Edge license,connector for external power supply, PN:16505	ks			14
Summit X440-48t PWP TAC & OS Summit 16505 , PN:97004-16505	ks			14
Summit X440-48p 48 X10/100/1000BASE-T PoE-plus,4X1000BASE-X unpopulated SFP(4 SFP ports shared with 10/100/1000BASE-T ports),SummitStack Stacking ports,1 AC PSU,ExtremeXOS Edge license,connector for external power supply, PN:16506	ks			10
Summit X440-48p PWP TAC & OS Summit 16506 , PN: 97004-16506	ks			10
SummitStack/UniStack Stacking cable, 0.5M , PN:16106	ks			20
Instalation & configuration services Extreme switches	hod	1	20	
WiFi:	0			0
Extreme networks AP3825I DUAL RADIO 11AC 3X3:3 MIMO INT ANT 2 EN, PN:WS-AP3825I	ks			5
Extreme networks AP3805I 11AC DUAL RADIO INT ANT, PN:WS-AP3805I	ks			5
Extreme networks controler WS-C35 IDENTIFI WIRELESS APPLIANCE, PN:30135	ks			1
Extreme networks NMS - 50 DEVICES / 500 THIN APS, PN:NMS-50	ks			1
Extreme networks Identity and Access 1,000 end-system license, PN:IA-ES-1 K	ks			1
Extreme networks controler WS-C35 PWP NBD AHR 30135, PN:95604-30135	ks			1
Extreme networks NMS - 50 PWP Software Subscription, PN:95603-S20129	ks			1
Extreme networks Identity and Access 1,000 PWP Software Subscription, PN:95603-S20098	ks			1
Instalation & configuration services WIFI	hod	5	20	

Technické vlastnosti	**Hodnota / charakteristika**
Sieťový manažment extreme networks NMS 50:	
Architektúra –všeobecné požiadavky	• Klient – serverová aplikácia
Architektúra –všeobecné požiadavky	• Serverová časť plnohodnotne podporovaná na operačných systémoch MS Windows a Linux

Architektúra –všeobecné požiadavky	• Plnohodnotná klientská časť podporovaná na operačných systémoch MS Windows, Linux aj MAC OSX
Architektúra –všeobecné požiadavky	• Podpora klientskej časti pre systémy iPad, iPhone, Android – stav monitorovaných zariadení
Architektúra –všeobecné požiadavky	• Vyhľadávanie užívateľov, prístup k udalostiam a k logom
Architektúra –všeobecné požiadavky	• Licencie pre správu všetkých dodávaných sieťových aktívnych prvkov
Architektúra –všeobecné požiadavky	• Viacúrovňová správa prístupov, podpora súbežnej práce viacerých používateľov
Architektúra –všeobecné požiadavky	• Podpora autentizácie pomocou protokolov LDAP a RADIUS
Architektúra –všeobecné požiadavky	• Hardwarová platforma
Funkcionalita	• Podpora IPv4 aj IPv6
Funkcionalita	• Podpora SNMPv1, SNMPv2, SNMPv3, AES pro SNMPv3 (netSNMP)
Funkcionalita	• Podpora hromadného skriptovania pomocou protokolov Telnet aj SSH
Funkcionalita	• Periodická záloha vlastnej konfigurácie
Funkcionalita - Pre všetky dodávané aktívne prvky musí podporovať:	• zálohovanie a obnovu konfigurácie
Funkcionalita - Pre všetky dodávané aktívne prvky musí podporovať:	• aktualizáciu firmwaru
Funkcionalita - Pre všetky dodávané aktívne prvky musí podporovať:	• zobrazovanie a nastavenie dátumu, času, zobrazenie uptime
Funkcionalita - Pre všetky dodávané aktívne prvky musí podporovať:	• konfiguráciu VLAN pomocou šablón
Funkcionalita - Pre všetky dodávané aktívne prvky musí podporovať:	• konfiguráciu MSTP pomocou šablón MSTP regiónov
Funkcionalita • SNMP manažment všetkých dodávaných sieťových aktívnych prvkov	• načítanie informácií z MIB – STP info, STP štatistika portov, vyťaženie zdrojov,
Funkcionalita• SNMP manažment všetkých dodávaných sieťových aktívnych prvkov	• načítanie informácií z MIB – inventár, VLAN, LACP, MSTP, vyťaženie rozhraní
Funkcionalita• SNMP manažment všetkých dodávaných sieťových aktívnych prvkov	• možnosť definície vlastných pohľadov
Funkcionalita• SNMP manažment všetkých dodávaných sieťových aktívnych prvkov	• vizualizácia zariadení – porty, sloty
Funkcionalita	• SNMP Trap server, Syslog server, BootP server
Funkcionalita	• Podpora RMON – čítanie, zobrazovanie
Funkcionalita	• Možnosť reakcie na prijatý SNMP Trap, Syslog správu a výpadku konektivity pomocou protokolov SMTP
Funkcionalita	-Syslog, SNMP Trap a spustením skriptov
Funkcionalita	• Možnosť naimportovania MIB zariadení tretích strán
Funkcionalita	• Vyhľadávanie v sieti podľa IP, subnetu, MAC, užívateľského mena
Funkcionalita	• Zisťovanie architektúry siete na základe IP rozsahov a rekurzívneho dotazovania susedov
Funkcionalita	• Detekcia a zobrazenie topológie siete pomocou Spanning Tree a MSTP inštancie, CDP, LLDP, OSPF
Funkcionalita	Správa ACL (Access Control List)-import/export do/zo zariadení, zmena, zvýraznenie zbytoč. pravidiel
Riadenie prístupu k sieti – extreme networks IA-ES-1K	
Musí poskytovať:	možnosť definície prístupových politík ako umožniť, zamietnuť, stanoviť priority,
Musí poskytovať:	nastaviť rýchlostné limity, tagy, presmer. a audit sieťovej prevád. na základe identity používateľa,
Musí poskytovať:	jednotné riadenie prístupov na základe prístup. rolí nezávislé na prístup. platforme (pevné, bezdr

Musí poskytovať:	času a miesta pripojenia, typu koncového zariadenia a ďalších jeho premenných parametrov
Musí poskytovať:	automatizované vynucovanie prístupových politík
Musí poskytovať:	komplexný prehľad všetkých spravovaných prístupových zariadení v infraštruktúre
Musí poskytovať:	riadiace pohľady (dashboard) s možnosťou rozvinutia pohľadu na podrobnejšie informácie
Musí poskytovať:	podrobné informácie o identite a prístupu
Musí poskytovať:	vyhľadávanie zariadení
Musí poskytovať:	interaktívne mapy topológie
Musí poskytovať:	zobrazenie zariadenia
Musí poskytovať:	logovanie aktivít
Musí poskytovať:	vytváranie reportov pre historické a aj aktuálne dáta
Musí poskytovať:	Open XML API pre integráciu s aplikáciami tretích strán
Riadenie prístupu k sieti – extreme networks IA-ES-1K	• Automatické zisťovanie koncového bodu a sledovania polohy pomocou identifikácie nových MAC adries,
Riadenie prístupu k sieti – extreme networks IA-ES-1K	nových IP adries, nových 802.1x alebo webových autentizácií
Riadenie prístupu k sieti – extreme networks IA-ES-1K	Kerberos alebo RADIUS žiadostí z prístup. zariadení
Riadenie prístupu k sieti – extreme networks IA-ES-1K	• Profilovanie prístup zariadení na viacerých úrovniach – typ OS, typ zariadenia, IP, MAC
Riadenie prístupu k sieti – extreme networks IA-ES-1K	miesto pripojenia, história pripojenia
Riadenie prístupu k sieti – extreme networks IA-ES-1K	• Podpora automat.priradenia prístup. profilov poskytovania sieťových služieb pre pristupujúce
Riadenie prístupu k sieti – extreme networks IA-ES-1K	zariadenia podľa kontextu – miesto pripojenia, čas pripojenia, typ OS, typ zariadenia
Riadenie prístupu k sieti – extreme networks IA-ES-1K	• Možnosť definovania vlastného portálu pre automatický prístup a oddelenie spravovaných mob. zar.
Riadenie prístupu k sieti – extreme networks IA-ES-1K	• Podpora vlastného registračného portálu pre prístup návštev k sieti
Riadenie prístupu k sieti – extreme networks IA-ES-1K	• Podpora riadenia prístupu návštev k sieti pomocou sponzora (bez IT zamestnanca)
Riadenie prístupu k sieti – extreme networks IA-ES-1K	- sponzor povolí prístup hosťa k sieti na základe predchádzajúcej registrácie hosťa
Riadenie prístupu k sieti – extreme networks IA-ES-1K	• Podpora LDAP a RADIUS overovania
Riadenie prístupu k sieti – extreme networks IA-ES-1K	• Schopnosť kontrolovať Bonjour a inú multicast prevádzku pre maximalizáciu výkonu siete
Riadenie prístupu k sieti – extreme networks IA-ES-1K	• Zariadenie na hardwarovej platforme
Riadenie prístupu k sieti – extreme networks IA-ES-1K	• Možnosť riadenia prístupov k sieti na prístupových zariadeniach tretích strán
Riadenie prístupu k sieti – extreme networks IA-ES-1K	• Licencie pre prístup 800 jedinečných zariadení za deň
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Jednoducho integrovateľný do existujúcej sieťovej infraštruktúry
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Certifikácia Wi-Fi CERTIFIED
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Súlad s lokálnymi štandardmi pre bezdrôtovú komunikáciu
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Podpora IEEE Standard 802.11h – DFS2
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Podpora súčasného, dual-band prístupu technológií 802.1 a/n/ac (5GHz) a 802.1 b/g/n (2.4 GHz)
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Plug and Play inštalácia prístupových bodov
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Bezpečná vzdialené správa pomocou protokolov HTTPS a SSH
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Centrálna konfigurácia a aktualizácia SW vybavenia

Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Autentizačné a šifrovacie štandardy WEP, WPA (TKIP), WPA2 (AES), 802.1x, 802.11i
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Automatický výber kanálu a vysielacieho výkonu podľa stavu RF priestoru a vyťaženia kanálu
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Riadenie vysielacieho výkonu po 12 a viac úrovniach
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Možnosť automatického presmerovania klienta medzi rádiami – band steering
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Automatická redistribúcia klientov medzi prístupovými bodmi podľa vyťaženia prístupového bodu
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Podpora rýchleho a bezpečného roamingu (pre authentication, OKC)
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Terminovanie klientskej prevádzky pri prístupovom bode, pri radiči (L2) alebo na radiči (L3)
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Distribuovaný RF manažment medzi prístupovými bodmi aj v prípade výpadku radiča
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Podpora Air Time Fairness pre rôzne typy prístupových zariadení
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Podpora hlasových, videových a dátových aplikácií na rovnakom SSID
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Prioritizovanie hlasových tokov pred dátovými pri označených aj neoznačených tokoch
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Podpora IEEE 802.11e, vrátane WMM, TSPEC a U-APSD
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• V prípade výpadku radiča, prístupové body musia vedieť naďalej pracovať samostatne –
Bezdrôtový prístup – kontroler Extreme networks WS-C35	terminovanie klientskej prevádzky pri prístupovom bode, šifrovanie, BlackList, L3 a L4
Bezdrôtový prístup – kontroler Extreme networks WS-C35	filtrovanie, asymetrický rate limit, QoS, RF manažment pre lokálne prepínanú prevádzku
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Podpora QoS (DiffServ, IP ToS, IP Precedence) pri pevnom a aj bezdrôtovom prístupe
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Možnosť priradenia rôznych prist. a bezpeč. profilov (ACL, QoS, Rate Limit, atď.) -
Bezdrôtový prístup – kontroler Extreme networks WS-C35	na klienta bez nutnosti použ. inej SSID
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Možnosť konverzie multicastov do unicastov
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Podpora multicastov Bonjour/LLMNR/UPnP – identifikácia, obmedzenie, riadenie
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Podpora 8 SSID na rádio
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Možnosť terminovania rôznej SSID do rovnakej VLAN
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• RADIUS AAA
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Podpora dynamickej autorizácie – RFC 3576
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Podpora WDS s možnosťou vyčlenenia rádia pre chrbticový spoj a aj s možnosťou používania
Bezdrôtový prístup – kontroler Extreme networks WS-C35	rovnakého rádia pre chrbticový spoj a aj pre klientsku prevádzku.
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Možnosť používania interného aj externého Captive Portalu pre autentizáciu klientov
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Možnosť editácie interného Captive Portálu
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Možnosť definície lokálnych účtov pre návštevy bez podpory IT personálu.
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• Hardvé. radič, s mož. zapojenia vo vysokej dostupnosti, pričom záložný radič bude prevá. vo vir. p
Bezdrôtový prístup – kontroler Extreme networks WS-C35	• API pre location-based aplikácie tretích strán
Bezdrôtový prístupový bod typ A – WS-AP3825I	• Vysokovýkonný prístupový bod pre vnútorné používanie
Bezdrôtový prístupový bod typ A – WS-AP3825I	• Určené pre nasadenie v oblastiach s vysokou hustotou prístupových klientov
Bezdrôtový prístupový bod typ A – WS-AP3825I	• Podpora noriem 802.11 a/b/g/n/ac

Bezdrôtový prístupový bod typ A – WS-AP3825I	• Verzia s možnosťou pripojenia vonkajších antén pomocou konektora RP-SMA
Bezdrôtový prístupový bod typ A – WS-AP3825I	• Súprava pre montáž na stenu
Požadovaný parameter/vlastnosť	Hodnota
Počet rádií	min. 2
MIMO	3x3:3 SS
Priepustnosť 2,4 GHz	40Mbps
Priepustnosť 5 GHz	1,2Gbps
Priepustnosť RFC2285	70 000 pps
Počet SSID na rádio	min. 5
Simultánne hlasové hovory	10 a viac
Počet asociovaných klientov na rádio	min. 100
Bezpečnostné štandardy	WPA, WPA2 (AES), 802.11i, 802.1x, IPSec, IKEv2, PKCS #10, X509 DER / PKCS #12
Vysielací výkon 2,4GHz	22 dBm
Vysielací výkon 5GHz	22 dBm
Zisk 2,4 GHz	3 dBi
Zisk 5 GHz	3 dBi
Počet 10/100/1000 Base-T rozhraní	min. 2
Režimy rozhraní	Active/Active, Active/Passive, LACP
Napájanie	PoE
Max odber	14 W
Váha	Max. 700 g
Bezdrôtová modulácia	802.11ac: BPSK, QPSK, 16QAM, 64QAM, 256QAM with OFDM
Bezdrôtová modulácia	802.11ac Packet aggregation: A-MPDU, A-MSDU
Bezdrôtová modulácia	802.11ac Very High-Throughput (VHT): VHT20/40/80
Bezdrôtová modulácia	802.11ac Advanced Features: LDPC, STBC, Maximum
Bezdrôtová modulácia	Likelihood (ML) Detection
Bezdrôtová modulácia	802.11n: BPSK, QPSK, 16QAM, 64QAM with OFDM
Bezdrôtová modulácia	802.11n High-throughput (HT) support: HT 20/40
Bezdrôtová modulácia	802.11n Packet aggregation: A-MPDU, A-MSDU
Bezdrôtová modulácia	802.11n Advanced Features: LDPC, STBC and TxBF
Bezdrôtová modulácia	802.11a: BPSK, QPSK, 16QAM, 64QAM with OFDM
Bezdrôtová modulácia	802.11g: DSSS and OFDM
Bezdrôtová modulácia	802.11b: DSSS
Bezdrôtový prístupový bod typ B – WS-3805I	• Vysokovýkonný prístupový bod pre vnútorné používanie
Bezdrôtový prístupový bod typ B – WS-3805I	• Podpora noriem 802.11 a/b/g/n/ac
Bezdrôtový prístupový bod typ B – WS-3805I	• Verzia s možnosťou pripojenia vonkajších antén pomocou konektora RP-SMA
Bezdrôtový prístupový bod typ B – WS-3805I	• Súprava pre montáž na stenu
Požadovaný parameter/vlastnosť	Hodnota
Počet rádií	min. 2
MIMO	2x2:2 SS

Priepustnosť 2,4 GHz	300 Mbps
Priepustnosť 5 GHz	860 Gbps
Priepustnosť RFC2285	35 000 pps
Počet SSID na rádio	min. 5
Simultánne hlasové hovory	10 a viac
Počet asociovaných klientov na rádio	min. 100
Bezpečnostné štandardy	WPA, WPA2 (AES), 802.11i, 802.1x, IPSec, IKEv2
Bezpečnostné štandardy	PKCS #10, X509 DER / PKCS #12
Vysielací výkon 2,4GHz	24 dBm
Vysielací výkon 5GHz	24 dBm
Zisk 2,4 GHz	3 dBi
Zisk 5 GHz	4,5 dBi
Počet 10/100/1000 Base-T rozhraní	min. 1
Napájanie	PoE
Max odber	10 W
Váha	Max. 400 g
Bezdrôtová modulácia	802.11ac: BPSK, QPSK, 16QAM, 64QAM, 256QAM s OFDM
Bezdrôtová modulácia	802.11ac Packet aggregation: A-MPDU, A-MSDU
Bezdrôtová modulácia	802.11ac Very High-Throughput (VHT): VHT20/40/80
Bezdrôtová modulácia	802.11ac Advanced Features: LDPC, STBC, Maximum
Bezdrôtová modulácia	Likelihood (ML) Detection
Bezdrôtová modulácia	802.11n: BPSK, QPSK, 16QAM, 64QAM with OFDM
Bezdrôtová modulácia	802.11n High-throughput (HT) support: HT 20/40
Bezdrôtová modulácia	802.11n Packet aggregation: A-MPDU, A-MSDU
Bezdrôtová modulácia	802.11n Advanced Features: LDPC, STBC and TxBF
Bezdrôtová modulácia	802.11a: BPSK, QPSK, 16QAM, 64QAM with OFDM
Bezdrôtová modulácia	802.11g: DSSS and OFDM
Bezdrôtová modulácia	802.11b: DSSS
Pevný prístup	• Spravovanie zariadení pomocou konzoly, SSHv2, Telnet, HTTP/HTTPS, SNMP v1, v2c v3
Pevný prístup	• Možnosť definovania komplexnosti hesla pre lokálnych administrátorov
Pevný prístup	• Musia mať vyčlenený port pre Out of Band manažment
Pevný prístup	• Možnosť vytvárania niekoľkých virtuálnych smerovačov
Pevný prístup	• Všetky zariadenia musia byť spolu integrovateľné do rovnakého stohu
Pevný prístup	• Podpora odzrkadlenia prevádzky na monitorovací port
Pevný prístup	• Podpora protokolov IPv4 a IPv6
Pevný prístup	• Podpora min. 4095 Vlanov
Pevný prístup	• Podpora Jumbo Frame 9216 Byte
Pevný prístup	• Podpora štandardu RFC 3619 - EAPS
Pevný prístup	• Podpora štandardu IEEE 802.1ab - LLDP
Pevný prístup	• Podpora štandardu IEEE 802.3ad - LACP

Pevný prístup	• Podpora protokolu 802.1x s možnosťou autentizácie viacerých užívateľov na jednom porte
Pevný prístup	• Možnosť vytvorenia agregovanej linky cez niekoľko zariadení, ktoré nie sú zapojené do rovn. stohu
Pevný prístup	• Operačný systém všetkých zariadení musí používať rovnaký binárny súbor
Pevný prístup	• Operačný systém zariadení musí byť rozšíriteľný pomocou modulov bez nutnosti rešt. zariadenia
Pevný prístup	• Operačný systém zariadení musí vedieť spúšťať lokálne scripty
Pevný prístup	• Používanie ACL nemôže zaťažiť sprocesovanie dátových tokov
Pevný prístup	• Zariadenia musia vedieť chrániť sieť na základe analýzy prevádzky – DoS (Ping of Death, Ping
Pevný prístup	Sweep, Ping Flood, Port Sweep, TCP Flood, atď.) , Flood útoky na porty (prihlasovacie služby,
Pevný prístup	RPC, NFS, File Sharing, X Windows, Name služby, Mailové služby, Webové služby, atď.)
Pevný prístup	• Zariadenia musia vedieť naštartovať z viacerých binárnych súborov uložených lokálne
Pevný prístup	• Zariadenia musia vedieť načítať si konfiguráciu z viacerých lokálne uložených konfiguračných súbor
Prepínač typ A – X460-G2-48t-10GE4	• Možnosť osadenia redundantnými ventilátormi
Prepínač typ A – X460-G2-48t-10GE4	• Prepínač s možnosťou stohovania s prepínačom typ B a C
Prepínač typ A – X460-G2-48t-10GE4	• Možnosť osadenia redundantnými zdrojmi napájania
Požadovaný parameter/vlastnosť	Hodnota
Počet 10/100/100BASE-T portov	48
Počet 1000/10000BASE-X portv (SFP+)	min.4
USB port	min. 1
Agregované prepínacie pásmo	min. 300 Gbps
Forwading Rate	min. 200 Mpps
Počet MAC adries	min. 90 k
Oneskorenie (64-byte)	< 5 micros
Výška	1 RU
Maximálna hĺbka	45 cm
Maximálna spotreba	130 W
Maximálne BTU	440
Prepínač typ B – X440-48t	• Prepínač s možnosťou stohovania s prepínačom typ A a C
Požadovaný parameter/vlastnosť	Hodnota
Počet 10/100/100BASE-T portov	48
Z toho Combo portov	min. 4
Počet 100/1000BASE-X portv (SFP)	min. 4
Stohovacie porty	min. 2
Agregované prepínacie pásmo	min. 120 Gbps
Forwading Rate	min. 90 Mpps
Počet MAC adries	min. 10 k
Oneskorenie (64-byte)	< 6 micros

Výška	1 RU
Maximálna hĺbka	30 cm
Maximálna spotreba	70 W
Prepínač typ C - X440-48p	• Prepínač poskytujúce napájanie koncových zariadení podľa štandardov 802.3af (PoE) a 802.3at (PoE+)
Prepínač typ C - X440-48p	• Prepínač s možnosťou stohovania s prepínačom typ B a C
Prepínač typ C - X440-48p	• Podpora externej napájacej jednotky
Prepínač typ C - X440-48p	
Požadovaný parameter/vlastnosť	Hodnota
Počet 10/100/100BASE-T portov	48
Počet MAC adries	min. 10 k
Počet 100/1000BASE-X portv (SFP)	min. 4
Z toho Combo portov	min. 4
Stohovacie porty	min. 2
Oneskorenie (64-byte)	< 6 micros
Agregované prepínacie pásmo	min. 120 Gbps
Forwading Rate	min. 90 Mpps
Výška	1 RU
Maximálna hĺbka	30 cm
Maximálna spotreba	650 W
Minimálny PoE rozpočet	350 W
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Stavový firewall novej generácie (Next Generation Firewall).
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Musí byť v prevedení HW appliance
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Musí mať jednotný systém aplikácie záplat a aktualizácií (aktualizácie alebo fixy musia
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	pokrývať operačný systém aj firewall)
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Zariadenie musí vedieť identifikovať aplikáciu z obsahu dátového toku a nie len podľa použ. portu
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Musí umožniť tvorbu vlastných signatúr pre detekciu aplikácií
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Musí vedieť k IP adrese priradiť identitu užívateľa. Identitu užívateľa musí vedieť získať
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	z adresárových služieb (MS Active Directory, LDAP) z terminálových služieb (MS Terminal
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	Services, Citrix XenAPP), zo Syslog správ a cez API rozhranie
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Výrobca musí poskytovať neustálu aktualizáciu IPS signatúr,
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	signatúr pre ochranu pred škodlivým kódom a URL databázy
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Musí vedieť vykonať SSL/TLS dekrypciu šifrovanej prevádzky pre potreby jej analýzy.
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Musí umožniť prevádzku vo vysokej dostupnosti v režime Active-Standby a Active-Active
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Musí vedieť poskytovať QoS pre definovanú prevádzku, a to aj na základe aplikácie
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	a kategórie aplikácií, URL a URL kategórie, používateľa
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	Musí vedieť generovať informácie o dátových tokoch NetFlow v9/IPFIX

Centrálny Firewall-Všeobecné požiadavky – Palo Alto netwoks PA3020Centrálny Firewall-Všeobecné požiadavky – Palo Alto netwoks PA3020	• Podpora statického smerovania a smerovacích protokolov RIP, OSPF, OSPF v3, BGP
Centrálny Firewall-Všeobecné požiadavky – Palo Alto netwoks PA3020	a smerovania multicastov
Centrálny Firewall-Všeobecné požiadavky – Palo Alto netwoks PA3020	• Musí umožniť vytváranie virtuálnych firewallov
Centrálny Firewall-Všeobecné požiadavky – Palo Alto netwoks PA3020	• Musí umožniť definíciu bezpečnostných zón a ich používanie pri tvorbe bezpečnostných politík.
Centrálny Firewall-Všeobecné požiadavky – Palo Alto netwoks PA3020	prideľovanie IP adries zariadeniam
Centrálny Firewall-Všeobecné požiadavky – Palo Alto netwoks PA3020	• Musí podporovať protokol IPv6 (NAT64, NPTv6, IPv6 over IPSec medzi IPv4 koncovými bodmi,
Centrálny Firewall-Všeobecné požiadavky – Palo Alto netwoks PA3020	• Možnosť prevádzky DNS Proxy servera
Centrálny Firewall-Všeobecné požiadavky – Palo Alto netwoks PA3020	• Podpora DHCP v režime Server alebo Relay. Pri funkcii DHCP servera musí umožňovať statické
Centrálny Firewall-Všeobecné požiadavky – Palo Alto netwoks PA3020	• Musí vedieť vytvárať IPSec VPN tunelov s podporou IKEv1 a IKEv2.
Centrálny Firewall-Všeobecné požiadavky – Palo Alto netwoks PA3020	• Musí podporovať agregáciu rozhraní pomocou protokolu LACP.
Centrálny Firewall-Všeobecné požiadavky – Palo Alto netwoks PA3020	IPv4 over IPSec medzi IPv6 koncovými bodmi, DHCPv6 Relay, SLAAC, NPTv6).
Tvorba bezpečnostných politík	• Musí umožniť tvorbu bezpečnostných politík na základe aplikácie alebo aplikačnej skupiny
Tvorba bezpečnostných politík	• Musí umožniť tvorbu bezpečnostných politík na základe užívateľskej identity a príslušnosti
Tvorba bezpečnostných politík	užívateľa v užívateľskej skupine.
Tvorba bezpečnostných politík	• Musí podporovať sandboxovú analýzu neznámych hrozieb.
Tvorba bezpečnostných politík	• Musí vedieť poskytovať IPS ochranu založenej na štatistickej analýze, heuristickej analýze,
Tvorba bezpečnostných politík	analýze protokolu, pasívneho DNS monitoringu a vlastnej signatúry.
Tvorba bezpečnostných politík	• Musí vedieť detegovať a blokovať škodlivý kód ako sú počítačové vírusy, spywary, botnety,
Tvorba bezpečnostných politík	počítačové červy a trojské kone.
Tvorba bezpečnostných politík	• Musí vedieť kontrolovať webovskú prevádzku na základe URL kontroly. URL kontrolu musí
Tvorba bezpečnostných politík	vedieť vykonávať voči lokálnej databáze ale aj voči databáze uloženej v cloude.
Tvorba bezpečnostných politík	• Musí podporovať definovanie bezpečnostnej politiky na kontrolu webovej prevádzky
Tvorba bezpečnostných politík	na základe samostatnej URL a kategórie URL
Tvorba bezpečnostných politík	• Musí umožňovať vytváranie vlastnej kategorizácie webových stránok.
Tvorba bezpečnostných politík	• Musí umožniť aplikovanie bezpečnostných politík na smerované/prekladané (L3) a aj
Tvorba bezpečnostných politík	transparentné (L2) dátové toky a to pre IPv4 ako aj pre IPv6.
Tvorba bezpečnostných politík	• Musí umožniť vytváranie bezpečnostných politík na základe času a denného obdobia.
Tvorba bezpečnostných politík	• Musí umožniť vytváranie bezpečnostných politík pozostávajúcich z objektov
Tvorba bezpečnostných politík	• Musí byť schopné vykonať validáciu bezpečnostnej politiky pred jej aplikáciou do prevádzky.
Tvorba bezpečnostných politík	• Musí byť schopné porovnať aktuálnu konfiguráciu voči niektorej známej z minulosti
Správa zariadenia	• Oddelené CPU pre správu zariadenia a pre poskytovanie firewallových služieb
Správa zariadenia	• Samostatné Ethernetové rozhranie pre Out-of -Band správu zariadenia
Správa zariadenia	• Správa zariadenia pomocou webového grafického používateľského rozhrania (GUI) a cez

Správa zariadenia	príkazový riadok protokolom SSHv2. SSH prístup musí vedieť umožniť aj pomocou verejného
Správa zariadenia	kľúča. GUI prístup musí vedieť umožniť aj pomocou osobného certifikátu.
Správa zariadenia	• Musí umožniť definovanie administrátorských rolí a prístup ad. umož.podľa ich zaradenia k rolám
Správa zariadenia	• Musí umožňovať v rámci definície role sprístupniť alebo zakázať CLI
Správa zariadenia	• Musí umožniť tvorbu administrátorských kont lokálne. Administrátorské prístupy musí vedieť
Správa zariadenia	overiť aj pomocou RADIUS protokolu a z LDAP databáze
Správa zariadenia	• Musí vedieť zaslať udalosti o stave zariadenia a o stave bezpečnostných politík pomocou
Správa zariadenia	protokolov Syslog, SNMP a SNTP.
Správa zariadenia	• Musí umožňovať zaznamenávanie všetkých administrátorských zásahov pre potreby auditu.
Integrácia	• Zariadenie musí byť zintegrované so všetkými (pevné aj bezdrôtové) dodávanými sieťovými prvkami.
Integrácia	• Zariadenie musí umožňovať autentifikovať používateľov prostred. Radius, Ldap a Kerberos protokolu
Integrácia musí umožniť	• v prípade, že firewall zistí, že používateľ porušuje bezpečnostné politiky,
Integrácia musí umožniť	sieťový prvok musí vedieť zmeniť prístupovú poli. užívateľa do siete.
Integrácia musí umožniť	• zistenie identity koncového užívateľa na základe 802.1x overenia,
Integrácia musí umožniť	• ukončiť všetky dátové toky na firewally v prípade, že užívateľ sa od siete odpojil,
Integrácia musí umožniť	• aplikovanie bezpečnostných politík podľa lokality pripojenia užívateľa do siete.
Bezpečnostný monitoring	• Zariadenie musí byť schopné vytvárať štatistické reporty z prevádzky podľa rôznych kritérií
Bezpečnostný monitoring	ako napr najnavšt.stránky, aplikácie, objem dát podľa používateľov, IP adries, geolokácie a pod
Bezpečnostný monitoring	• Musí obsahovať reporting o zachytených hrozbách, podľa používateľov, spojení, zdrojov a pod
Bezpečnostný monitoring	• Musí obsahovať sadu preddefinovaných reportov a taktiež možnosť vytvárať vlastné reporty
Bezpečnostný monitoring	• Musí byť schopné zobraziť trendy vývoja hrozieb, vyťaženia a pod
Bezpečnostný monitoring	• Musí obsahovať analýzu podozrivej komunikácie hostov v sieti pre detekovanie komunikácie
IBezpečnostný monitoring	na známe C&C server
Bezpečnostný monitoring	• Musí obsahovať korelačný engine generujúci udalosti koreláciou viacerých elementárnych
Bezpečnostný monitoring	• Výsledok sandbox analýzy musí byť dostupný z content logu a naopak, aby bolo možné
Bezpečnostný monitoring	udalostí zachytených firewallom
Bezpečnostný monitoring	identifikovať priamo používateľa alebo PC na ktoré bol stiahnutý alebo zaslaný škodlivý kód
Výkonnostné parametre	Výkonnostné parametre
Parameter	Počet
Počet interfejsov 10/100/1000 RJ45	Min 12
Počet optických (SFP) interfejsov	Min 8
Počet VLANs	Min 4096
Počet logických interfejsov (L2, L3, tunnel)	Min 1000
FW priepustnosť	Min 2Gbps
IPS+AV priepustnosť	Min 2Gbps

VPN priepustnosť	Min 500Mbit
Počet nových spojení /s	Min 50 000
Počet konkurentných spojení	Min 250 000
Počet VPN tunnelov	Min 500
Možnosť pridať virtuálne systémy	Min 5
Počet bezpečnostných pravidiel	Min 2500
Počet NAT pravidiel	Min 2500
Počet bezpečnostných profilov	Min 150
Počet aplikačných profilov	Min 250
Počet QoS tried	Min 8
Počet súčasne používaných syslog serverov	Min 4
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	• Stavový firewall novej generácie (Next Generation Firewall).
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	• Zariadenie musí vedieť identifikovať aplikáciu z obsahu dátového toku a nie len podľa použ. portu
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	• Musí umožniť tvorbu vlastných signatúr pre detekciu aplikácií
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	• Musí vedieť k IP adrese priradiť identitu užívateľa. Identitu užívateľa musí vedieť získať
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	z adresárových služieb (MS Active Directory, LDAP) z terminálových služieb (MS Terminal
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	Services, Citrix XenAPP)
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	• Výrobca musí poskytovať neustálu aktual. IPS signatúr, signatúr pre ochranu pred škod.
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	kódom a URL databázy
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	• Musí vedieť vykonať SSL/TLS dekrypciu šifrovanej prevádzky pre potreby jej analýzy.
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	• Musí umožniť prevádzku vo vysokej dostupnosti v režime Active-Standby a Active-Active
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	• Musí vedieť poskytovať QoS
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	• Musí vedieť generovať informácie o dátových tokoch NetFlow v9
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	• Podpora statického smerovania a smerovacích protokolov RIP, OSPF, OSPF v3, BGP
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	a smerovania multicastov.
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	• Musí umožniť definíciu bezpečnostných zón a ich používanie pri tvorbe bezpečnostných politík.
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	• Musí umožniť vytváranie virtuálnych firewallov
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	• Podpora DHCP v režime Server alebo Relay. Pri funkcii DHCP servera musí umožňovať statické
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	prideľ.IP adries zariadeniam
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	• Možnosť prevádzky DNS Proxy servera
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	• Musí vedieť vytvárať IPSec VPN tunelov s podporou IKEv1 a IKEv2.
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	• Musí podporovať protokol IPv6 (NAT64, NPTv6, IPv6 over IPSec medzi IPv4 koncovými bodmi,
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	IPv4 over IPSec medzi IPv6 koncovými bodmi, DHCPv6 Relay, SLAAC, NPTv6).
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	• Musí umožniť tvorbu bezp. politík na základe užív. identity a príslušnosti užívateľa v užív.skupin

Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	• Musí podporovať sandboxovú analýzu neznámych hrozieb.
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	• Musí vedieť detegovať a blokovať škodlivý kód ako sú počítačové vírusy, spywary, botnety,
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	počítačové červy a trójské kone.
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	• Musí vytvárať záznamy o všetkých realizovaných spojeniach, vrátane mena používateľa
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	• Správa zariadenia pomocou web. grafického použ. rozhrania (GUI) a cez príkazový riadok
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	protokolom SSHv2. SSH prístup musí vedieť umožniť aj pomocou verejného kľúča.
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	• Musí umožniť definovane administrátorských rolí a prístup admini. umožňovať podľa ich
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	zaradenia k rolám.
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	• Musí umožniť tvorbu administrátorských kont lokálne. Administrátorské prístupy musí vedieť
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	overiť aj pomocou RADIUS protokolu a z LDAP databáze
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	• Musí vedieť zaslať udalosti o stave zariadenia a o stave bezpečnostných politík pomocou
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	protokolov Syslog, SNMP a SMTP.
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	• Musí umožňovať zaznamenávanie všetkých administrátorských zásahov pre potreby auditu. •
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• VPN gateway musí byť vo forme appliance
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Jednotný systém pre aktualizácie a fixy OS a VPN
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Musí podporovať IPSEC a SSLVPN
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Zariadenie musí podporovať portal mode – sprístupnenie vybraných aplikácií cez browser bez
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	nutnosti administrátorských oprávnení
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Výrobca musí mať free ssl a ipsec vpn klienta alebo existuje podporovaný klient tretej strany
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Portál musí byť konfigurovateľný pre skupinu alebo používateľa
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Musí podporovať v portál móde min nasledovné aplikácie:
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	http-https
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	file sharing (SMB/CIFS)
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	remote desktop protocol - RDP
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	ftp
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	Ssh
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• musí podporovať používateľom definovateľné bookmark-y
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Musí umožňovať úpravu prihlasovacej stránky
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Musí podporovať tunnel mode pre plný tcp/ip prístup
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• IP adresácia klienta konfigurovateľná pre skupinu
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Podpora prideľovania parametrov cez Radius atribúty
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Musí podporovať operačné systémy Windows, Linux a MacOS,
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Musí podporovať mobilné platformy iOS, Android a Windows
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Musí podporovať možnosť split tunel, konfigurovateľné pre skupinu

SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Musí disponovať funkcionalitou pre scan klienta (procesy, súbory a registre)
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Musí disponovať funkcionalitou pre obmedzenie počtu súčasných prihlásení jedného klienta
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Musí podporovať autentifikáciu voči lokálnej databáze, LDAP, RADIUS a PKI
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Musí podporovať skupiny používateľov lokálne, LDAP, RADIUS
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Musí disponovať dvojfaktorovou autentifikáciou
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• OTP kód musí byť dostupný vo forme tokenu (HW alebo SW), emailu a SMS
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Musí obsahovať funkcionalitu NG firewallu, pravidlá je možné definovať na používateľov
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	alebo skupiny, aplikácie a je možné aplikovať IPS a AV profil
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Výrobca musí poskytovať neustálu aktualizáciu IPS signatúr, signatúr pre ochranu pred
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	škodlivým kódom a URL databázy
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Musí umožniť prevádzku vo vysokej dostupnosti v režime Active-Standby a Active-Active
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Musí vedieť poskytovať QoS pre definovanú prevádzku
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Musí vedieť generovať informácie o dátových tokoch NetFlow v9
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Musí umožniť vytváranie virtuálnych firewallov.
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Možnosť prevádzky DNS Proxy servera
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Musí vedieť vytvárať IPSec VPN tunelov s podporou IKEv1 a IKEv2.
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Musí podporovať sandboxovú analýzu neznámych hrozieb.
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Musí vedieť detegovať a blokovať škodlivý kód ako sú počítačové vírusy, spywary, botnety
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	počítačové červy a trojské kone.
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Musí vytvárať záznamy o všetkých realizovaných spojeniach, vrátane mena používateľa
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Správa zariadenia pomocou webového grafického používateľského rozhrania (GUI) a cez
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	príkazový riadok protokolom SSHv2. SSH prístup musí vedieť umožniť aj pomocou verejného
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	kľúča.
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Musí umožniť definovane administrátorských rolí a prístup administrátorov umožňovať podľa
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	ich zaradenia k rolám
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Musí umožniť tvorbu administrátorských kont lokálne. Administrátorské prístupy musí vedieť
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	overiť aj pomocou RADIUS protokolu a z LDAP databáze.
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Musí vedieť zaslať udalosti o stave zariadenia a o stave bezpečnostných politík pomocou
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	protokolov Syslog, SNMP a SMTP.
SSL VPN gateway - Všeobecné požiadavky - FortiGate 100D	• Musí umožňovať zaznamenávanie všetkých administrátorských zásahov pre potreby auditu
Výkonnostné parametre	Výkonnostné parametre
Parameter	Počet
Počet interfejsov 10/100/1000 RJ45	Min 18
Počet optických (SFP) interfejsov	Min 2
Počet VLANs	Min 4096

Počet logických interfejsov (L3 + tunnel)	Min 2048
FW priepustnosť	Min 2,5Gbps
IPS priepustnosť	Min 900 Mbps
AV priepustnosť	Min 300 Mbps
Ssl VPN priepustnosť	Min 300 Mbps
Počet nových spojení /s	Min 20 000
Počet konkurentných spojení	Min 500 000
Latencia	Max 50us
Počet ssl VPN tunnelov	Min 300
Počet virtuálnych systémov	min 5
Počet bezpečnostných pravidiel	Min 5000
Počet NAT pravidiel	Min 1000
Počet používateľov použitých v policy	Min 100
Počet bezpečnostných profilov	Min 32
Počet aplikačných profilov	Min 32
Počet súčasne používaných syslog serverov	Min 3
Antispam gateway - FortiMail VM02	Funkčné požiadavky
Antispam gateway - FortiMail VM02	Zariadenie musí byť ako SW alebo HW appliance
Antispam gateway - FortiMail VM02	Musí pracovať ako email relay
Antispam gateway - FortiMail VM02	Musí podporovať transparentný mód
Antispam gateway - FortiMail VM02	Musí umožňovať kontrolu a filtrovanie spamu v prichádzajúcej a odchádzajúcej emailovej komunikácii.
Antispam gateway - FortiMail VM02	Musí umožňovať kontrolu a filtrovanie malvéru a vírusov v prichádzajúcej
Antispam gateway - FortiMail VM02	a odchádzajúcej emailovej komunikácii.
Antispam gateway - FortiMail VM02	Musí umožňovať kontrolu a filtrovanie zakázaných príloh v prichádzajúcej
Antispam gateway - FortiMail VM02	a odchádzajúcej emailovej kom. na základe typu, kategórie alebo šifrovania
Antispam gateway - FortiMail VM02	Musí umožňovať overovanie existencie príjemcu voči zoznamu existujúcich
Antispam gateway - FortiMail VM02	aktívnych emailových adries v Exchange/Active Directory.
Antispam gateway - FortiMail VM02	Musí umožňovať definovať pravidlá s využitím užívateľských účtov a skupín
Antispam gateway - FortiMail VM02	v Active Directory.
Musí umožňovať definovať politiky pre prichádzajúcu emailovú komunikáciu na základe:	pre doména
Musí umožňovať definovať politiky pre prichádzajúcu emailovú komunikáciu na základe:	prer emailová adresa
Musí umožňovať definovať politiky pre prichádzajúcu emailovú komunikáciu na základe:	pre užívateľ
Musí umožňovať definovať politiky pre prichádzajúcu emailovú komunikáciu na základe:	pre užívateľská skupina
Antispam gateway - FortiMail VM02	Musí umožňovať logovanie emailovej komunikácie a nástroje pre vyhľadávanie v logoch
Antispam gateway - FortiMail VM02	Musí obsahovať nástroje pre obmedzenie rýchlosti resp. frekvencie spojení
Antispam gateway - FortiMail VM02	Musí umožňovať nastavenie automatického generovania a zasielania reportov na vybrané emailové adresy
Antispam gateway - FortiMail VM02	Musí obsahovať centrálnu karanténu obsahujúcu odfiltrované emaily podozrivé

Antispam gateway – FortiMail VM02	na spam dostupné z webového manažment rozhrania.
Antispam gateway – FortiMail VM02	Musí obsahovať používateľskú karanténu obsahujúcu emaily podozrivé na
Antispam gateway – FortiMail VM02	spam dostupnú pre používateľa:
Antispam gateway – FortiMail VM02	- cez webové rozhranie s prihlásením pomocou účtu v Active Directory
Antispam gateway – FortiMail VM02	- kliknutím na odkaz v zaslanom notifikačnom emaily.
Antispam gateway – FortiMail VM02	Musí umožňovať nastavenie výnimky smerovanie pre vybrané cieľové domény alebo IP adresy
Antispam gateway – FortiMail VM02	Musí obsahovať centrálnu karanténu obsahujúcu odfiltrované emaily, ktoré
Antispam gateway – FortiMail VM02	obsahovali zakázané prílohy
Antispam gateway – FortiMail VM02	Musí umožňovať pravidelné automatické zálohovanie konfigurácie zariadenia
Antispam gateway – FortiMail VM02	mimo diskový priestor samotného zariadenia.
Antispam gateway – FortiMail VM02	Technické požiadavky
Antispam gateway – FortiMail VM02	Zariadenie musí mať výrobcom deklarované ukončenie podpory zariadenia (EOL) najskôr v roku 2019.
Antispam gateway – FortiMail VM02	Musí mať kapacitu na 1000 používateľov
Antispam gateway – FortiMail VM02	Musí umožňovať príjem emailov pre 20 domén
Antispam gateway – FortiMail VM02	Minimálne 100 aktívnych konkurentných spojení
Antispam gateway – FortiMail VM02	Minim. priepust. zariad. pri antispam a antivirovej kont. musí byť 50k emailov za hodinu(pri 100 kB)
Antispam gateway – FortiMail VM02	Musí umožňovať definovať minimálne 300 pravidiel pre emailovú doménu
Antispam gateway – FortiMail VM02	Musí umožňovať použitie minimálne 50 bezpečnostných profilov
Antispam gateway – FortiMail VM02	Musí umožňovať kontrolu prichádzajúcej emailovej komunikácie na spam s využitím techniky greylisting
Antispam gateway – FortiMail VM02	Musí umožňovať kontrolu prichádzajúcej emailovej komunikácie s využitím reputačných databáz výrobcu
Antispam gateway – FortiMail VM02	Musí umožňovať kont. prich. emailovej kom. s využitím techniky Bounce Address Tag Validation (BATV)
Antispam gateway – FortiMail VM02	Musí umožňovať kontrolu prichádzajúcej emailovej komunikácie s využitím DKIM
Antispam gateway – FortiMail VM02	Musí umožňovať kontrolu prichádzajúcej emailovej komunikácie s využitím SPF záznamov
Antispam gateway – FortiMail VM02	Musí umožňovať použitie “blacklist” a “whitelist” slov a využitie slovníka
Antispam gateway – FortiMail VM02	Musí disponovať kontrolou obrázkov
Antispam gateway – FortiMail VM02	Musí obsahovať heuristickú analýzu a Bayesian
Antispam gateway – FortiMail VM02	Musí umožňovať vytváranie používateľských whitelistov email adries
Antispam gateway – FortiMail VM02	Musí umožňovať využitie externých zdrojov poskytujúcich informácie
Antispam gateway – FortiMail VM02	o blacklistovaných DNS a IP adresách (DNSBL).
Antispam gateway – FortiMail VM02	Zariadenie nesmie byť limitované na počet používateľov
Antispam gateway – FortiMail VM02	Musí umožňovať nastavenie rôznych akcií pre rôzne techniky filtrovania
Antispam gateway – FortiMail VM02	(napr pri DNSBL vykonať iba taging predmetu, pri reputačnej databáze výrobcu uložiť do karantény)
Integračné práce	Dodávateľ tech.v rámci dodávky riešenia vykoná všetky inšt. a konfig. práce pot.pre funkčné riešenia
Všeobecné požiadavky – integrácia centrálneho FW	• Analýza súčasného stavu
Všeobecné požiadavky – integrácia centrálneho FW	• Návrh topológie zapojenia

Všeobecné požiadavky – integrácia centrálneho FW	• Inštalácia nového HW v priestoroch objednávateľa
Všeobecné požiadavky – integrácia centrálneho FW	• Základná konfigurácia FW (IP adresa, názov, zóny, manažment ....)
Všeobecné požiadavky – integrácia centrálneho FW	• Konfigurácia VPN tunelov
Všeobecné požiadavky – integrácia centrálneho FW	• Migrácia objektov, smerovania, NAT
Všeobecné požiadavky – integrácia centrálneho FW	• Migrácia komunikačných pravidiel
Všeobecné požiadavky – integrácia centrálneho FW	• Optimalizácia a vyčistenie komunikačnej matice
Všeobecné požiadavky – integrácia centrálneho FW	• Integrácia so všetkými prvkami sieťovej infraštruktúry
Všeobecné požiadavky – integrácia centrálneho FW	• Vyriešenie komunikačných problémov (prepojenie na externé subjekty, portály a pod. .....)
Všeobecné požiadavky – integrácia centrálneho FW	• Funkčné testy
Všeobecné požiadavky – integrácia centrálneho FW	• Detailná dokumentácia riešenia
Všeobecné požiadavky – SSL VPN brána	• Analýza súčasného stavu
Všeobecné požiadavky – SSL VPN brána	• Návrh topológie zapojenia
Všeobecné požiadavky – SSL VPN brána	• Inštalácia nového HW v priestoroch objednávateľa
Všeobecné požiadavky – SSL VPN brána	• Inštalácia a konfigurácia HW na vybraných lokalitách
Všeobecné požiadavky – SSL VPN brána	• Základná konfigurácia SSL VPN brány (IP adresa, názov, zóny, manažment ....)
Všeobecné požiadavky – SSL VPN brána	• Konfigurácia SSL tunelov
Všeobecné požiadavky – SSL VPN brána	• Migrácia/vytvorenie objektov, smerovania, NAT
Všeobecné požiadavky – SSL VPN brána	• Migrácia/vytvorenie komunikačných pravidiel
Všeobecné požiadavky – SSL VPN brána	• Optimalizácia a vyčistenie komunikačnej matice
Všeobecné požiadavky – SSL VPN brána	• Integrácia s AD
Všeobecné požiadavky – SSL VPN brána	• Integrácia so všetkými prvkami sieťovej infraštruktúry
Všeobecné požiadavky – SSL VPN brána	• Vyriešenie komunikačných problémov (prepojenie na externé subjekty, portály a pod. .....)
Všeobecné požiadavky – SSL VPN brána	• Funkčné testy
Všeobecné požiadavky – SSL VPN brána	• Detailná dokumentácia riešenia
Všeobecné požiadavky – Antispam	• Analýza súčasného stavu
Všeobecné požiadavky – Antispam	• Návrh topológie zapojenia
Všeobecné požiadavky – Antispam	• Inštalácia VmWare prostredia na fyzické zariadenia
Všeobecné požiadavky – Antispam	• Konfigurácia VmWare a pripojenie do LAN
Všeobecné požiadavky – Antispam	• Inštalácia antispam riešenia do virtuálneho prostredia
Všeobecné požiadavky – Antispam	• Konfigurácia antispam (IP adresy, smerovanie, užívatelia, karanténa, DNS ....)
Všeobecné požiadavky – Antispam	• Integrácia s MS Exchange a AD
Všeobecné požiadavky – Antispam	• Funkčné testy
Všeobecné požiadavky – Antispam	• Detailná dokumentácia riešenia
Všeobecné požiadavky – LAN infraštruktúra	• Analýza súčasného stavu
Všeobecné požiadavky – LAN infraštruktúra	• Návrh topológie zapojenia
Všeobecné požiadavky – LAN infraštruktúra	• Fyzická inštalácia zariadení v priestoroch dodávateľa
Všeobecné požiadavky – LAN infraštruktúra	• Pripojenie do existujúcej infraštruktúry

Všeobecné požiadavky – LAN infraštruktúra	• Popripájanie existujúcich systémov (mimo pracovnú dobu teda po 20 tej hodine)
Všeobecné požiadavky – LAN infraštruktúra	• Aktualizácia OS, konfigurácia vlan, trunk portov, priradenie portov do vlan
Všeobecné požiadavky – LAN infraštruktúra	• Konfigurácia manažment prístupov, vytvorenie stackov
Všeobecné požiadavky – LAN infraštruktúra	• Konfigurácie Spanning Tree
Všeobecné požiadavky – LAN infraštruktúra	• Integrácia do centrálneho manažmentu
Všeobecné požiadavky – LAN infraštruktúra	• Konfigurácia 802.1x a integrácia do riadiaceho systému
Všeobecné požiadavky – LAN infraštruktúra	• Integrácia s centrálnym FW
Všeobecné požiadavky – LAN infraštruktúra	• Konfigurácia a integrácia s dohľadovým systémom
Všeobecné požiadavky – LAN infraštruktúra	• Inštalácia a konfigurácia kontroléru
Všeobecné požiadavky – LAN infraštruktúra	• Fyzická inštalácia AP v priestoroch objednávateľ, vrátane privedenia kabeláže
Všeobecné požiadavky – LAN infraštruktúra	• Konfigurácia AP vrátane integrácie s NAC a centrálnym manažmentom
Pobočkový Firewall-Všeobecné požiadavky – Fortigate 30D a FortiGate 60D	Výkonnostné parametre
Parameter	Počet
Počet interfejsov 10/100/1000 RJ45	Min 10
Počet optických (SFP) interfejsov	0
Počet VLANs	Min 4096
Počet logických interfejsov (L2, L3, tunnel)	Min 50
FW priepustnosť	Min 1,5Gbps
IPS+AV priepustnosť	Min 35Mbps
VPN priepustnosť	Min 1Gbps
Počet nových spojení /s	Min 4 000
Počet konkurentných spojení	Min 500 000
Latencia	Max 10us
Počet VPN tunnelov	Min 100
Možnosť pridať virtuálne systémy	min 5
Počet bezpečnostných pravidiel	Min 1000
Počet NAT pravidiel	Min 100
Počet používateľov použitých v policy	Min 100
Počet bezpečnostných profilov	Min 32
Počet aplikačných profilov	Min 32
Počet súčasne používaných syslog serverov	Min 3

2.4 Osobitné požiadavky na plnenie:

Názov
V cene je dovoz, rozbalenie, inštalácia dodávaného tovaru na pracoviska podľa požiadaviek verejného obstarávateľa.
Verejný obstarávateľ si vyhradil právo na poskytnutie bezplatnej vzorky Plnenia predmetu zákazky, resp. do 48 hodín dodať popis a technickú špecifikáciu obstarávaných zariadení v zákazke z dôvodu odkontrolovania požadovaných parametrov zariadení.
Záručná doba 12 mesiacov v mieste inštalácie s odozvou nasledujúci pracovný deň.
Nedodržanie uvedených osobitných požiadaviek na plnenie bude objednávateľ považovať za závažné porušenie zmluvných podmienok zákazky.

Pokuta za nedodržanie uvedených osobitných požiadaviek na plnenie, nedodanie tovaru podľa popisu, špecifikácií a termínoch dodania v objednávkovom formulári je 10% z predpokladanej hodnoty zákazky t.j. 20.000 EUR na účet verejného obstarávateľa do 10 pracovných dní.
Uchádzač predloží do 48 hodín od uzavretia zmluvy úplnú špecifikáciu a cenovú kalkuláciu jednotlivých položiek predmetu zákazky v členení: jednotková cena položky bez DPH, cena za jednotlivé položky spolu (bez DPH, výška DPH, spolu s DPH).
Uchádzač predloží do 48 hodín od uzavretia zmluvy vyhlásenia o zhode a doplňujúce podklady k nim, resp. certifikáty vydané autorizovanými osobami alebo notifikovanými osobami pre všetky položky predmetu zákazky.
Uchádzač dodá predmet zákazky, ktorý je certifikovaný a schválený na dovoz a predaj v Slovenskej republike, resp. v rámci Európskej únie a bude vyhovovať platným medzinárodným normám, STN a všeobecne záväzným právnym predpisom.
Splatnosť faktúr 30 dní.
Objednávateľ je oprávnený pri dodávke skontrolovať predmet zákazky a v prípade dodávky iného tovaru tento tovar neprevziať.
Víťazný uchádzač predloží do 48 hodín od uzavretia zmluvy: expert pre správu FW - Certified Network Security Engineer CNSE 5.1
Víťazný uchádzač predloží do 48 hodín od uzavretia zmluvy: expert pre správu FW - Certified Network Security Professional pre FortiOS v.5
Víťazný uchádzač predloží do 48 hodín od uzavretia zmluvy: expert pre sieťovú bezpecnosť - platný doklad o odbornej a technickej spôsobilosti v oblasti zabezpečenia siete, identifikácie zraniteľností v sieti platný certifikát CompTIA Security+, prípadne ekvivalent tohto certifikátu alebo iný rovnoce
Víťazný uchádzač predloží do 48 hodín od uzavretia zmluvy: expert pre sieťovú infraštruktúru - Predloženie certifikátu CompTIA Network+, prípadne ekvivalentu tohto certifikátu alebo iného rovnocenného dokumentu je nevyhnutné z dôvodu preukázania odbornej spôsobilosti v oblasti analýzy, návrhu a impl
Víťazný uchádzač predloží do 48 hodín od uzavretia zmluvy: expert pre informačnú bezpecnosť - platný doklad o odbornej a technickej spôsobilosti v oblasti zabezpečenia siete, identifikácie zraniteľností v sieti analýzy škodlivého kódu platný certifikát CISM prípadne ekvivalent tohto certifikátu
Maximálna lehota dodania predmetu zákazky je 14 pracovných dní odo dňa nadobudnutia účinnosti zmluvy.
Zmluvné strany súhlasia, že verejný obstarávateľ je oprávnený vypovedať zmluvu do 15 dní od oznámenia výpovede aj bez uvedenia dôvodu.

Názov	Upresnenie

2.5 Prílohy opisného formulára Zmluvy:

Popis	Názov súboru
sieťová infraštruktúra	infrastruktura.pdf

III. Zmluvné podmienky

3.1 Miesto plnenia Zmluvy:

Štát:	Slovenská republika
Kraj:	Bratislavský
Okres:	Bratislava
Obec:	Bratislava
Ulica a číslo:	

3.2 Čas / lehota plnenia zmluvy:

18.12.2015 9:00:00 - 29.12.2015 16:00:00

3.3 Dodávané množstvo/ rozsah zmluvného plnenia:

Jednotka:	ks
Požadované množstvo:	1,0000

3.4 Práva a povinnosti zmluvných strán podľa tejto Zmluvy sa spravujú Obchodnými podmienkami elektronického trhoviska verzia 2.1, účinná zo dňa 1.12.2015 , ktoré tvoria neoddeliteľnú prílohu tejto Zmluvy.

IV. Zmluvná cena

4.1 Celková cena predmetu Zmluvy bez DPH: 197 208,33 EUR

4.2 Sadzba DPH: 20,00

4.3 Celková cena predmetu Zmluvy vrátane DPH: 236 650,00 EUR

V. Záverečné ustanovenia

5.1 Táto Zmluva bola uzavretá automatizovaným spôsobom v rámci Elektronického kontraktačného systému a v zmysle Obchodných podmienok elektronického trhoviska verzia 2.1, účinná zo dňa 1.12.2015, ktoré tvoria jej prílohu č. 1.

5.2 Táto Zmluva nadobúda platnosť dňom jej uzavretia a účinnosť za podmienok definovaných v Obchodných podmienkach elektronického trhoviska uvedených v bode 5.1 tejto zmluvy.

5.3 Táto Zmluva vrátane jej príloh predstavuje úplnú dohodu zmluvných strán o jej predmete. Vedľajšie dohody k tejto zmluve neexistujú.

5.4 Táto Zmluva je vyhotovená v elektronickej podobe v štyroch vyhotoveniach, po jednom pre každú zmluvnú stranu, jedno vyhotovenie bude zaslané na zverejnenie v Centrálnom registri zmlúv Úradu vlády Slovenskej republiky a jedno bude zverejnené v Centrálnom registri zmlúv trhoviska.

5.5 Túto Zmluvu bude možné meniť a dopĺňať za podmienok stanovených príslušnými všeobecne záväznými právnymi predpismi len vo forme písomného a číslovaného dodatku podpísaného oboma zmluvnými stranami.

5.6 Táto Zmluva má nasledovné prílohy:

Príloha č.1 Obchodné podmienky elektronického trhoviska verzia 2.1, účinná zo dňa 1.12.2015, https://portal.eks.sk/SpravaOpet/Opet/VerejnyDetail/

V Bratislave, dňa 9.12.2015 8:42:01

Objednávateľ:
Hlavné mesto Slovenskej republiky Bratislava
konajúci prostredníctvom osoby poverenej zastupovať Objednávateľa v rámci elektronického trhoviska

Dodávateľ:
TooNet, s.r.o.
konajúci prostredníctvom osoby poverenej zastupovať Dodávateľa v rámci elektronického trhoviska