Tabulka č. 1 – Skener zranitelnosti			
Parametr	**Popis požadovaného parametru**	**Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
1	Rozšiřující modul pro Q Radar SIEM		
2	Plná integrace do rozhraní Q Radar SIEM		
3	SW modul bez dodatečného HW instalovaný přímo na Q Radar 2100 appliance		
4	Licence pro skenování 255 samostatných systémů		

Tabulka č. 2 : Netflow sonda			
Parametr	**Popis požadovaného parametru**	**Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
1	Řešení umožňující dlouhodobé monitorování sítě na bázi protokolu NetFlow (nutná podpora NetFlow v5 a NetFlow v9) a IPFIX		
2	Neviditelné na L2 a L3 vrstvě (monitorovací porty nemají IP, je zcela pasivní)		
3	Pasivní zapojení monitorovacích portů přes TAP nebo mirror (span) port core switche (v případě poruchy nemůže zařízení ovlivnit síť)		
4	Podpora pro IPv4, IPv6, VLAN		
5	Monitoring 1 Gbps provozu		
6	4x1 Gbps metalické porty		
7	Rack mount zařízení, 1U velikost		
8	Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS		
9	Možnost rozšíření o rozšiřující moduly – modul detekce anomálií		
10	Součástí základní modul pro analýzu sítě: vytváření dlouhodobých grafů a přehledů o komunikaci na síti s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (HTTP, IMAP, SSH)		

Tabulka č. 3 - NetFlow kolektor			
Parametr	**Popis požadovaného parametru**	**Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
1	Hardwarová appliance, disková kapacita 6TB v RAID poli		
2	Jeden administrativní port 10/100/1000 Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu a přenos NetFlow dat		
3	Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS;		
4	Víceuživatelský přístup - včetně možnosti definovat k jakým datům má jednotlivý uživatel přístup;		
5	Podpora autentizace vůči LDAP		
6	HOT SWAP disky, RAID včetně SMART detekce		
7	Integrace dohledového systému pro kontrolu dostupnosti (SNMP);		
8	Podpora verze NetFlow protokolu – programové vybavení kolektoru musí umožnit sběr a vyhodnocení NetFlow dat ve verzi 5 a 9;		
9	Podpora pro sběr a analýzu sFlow a NetStream dat;		
10	Podpora standardů NEL a NSEL, monitorování MAC adres;		
11	Podpora pro příjem a analýzu informací o detekovaných aplikacích dle NBAR2 standardu;		
12	Podpora pro příjem a analýzu HTTP provozu - včetně položek typu URL, hostname,		
13	Podpora pro příjem a analýzu VoIP statistik (jitter, latence, ztrátovost)		
14	Možnost přeposílání přijímaných NetFlow statistik ke zpracování na další kolektory včetně možnosti filtrace na úrovni NetFlow paketů		
15	Uživatelsky definovatelný dashboard (konfigurace per uživatel)		
16	Vytváření dlouhodobých grafů a přehledů s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (HTTP, IMAP, SSH)		
17	Generování statistik a podrobných výpisů nad volitelnými časovými intervaly		
18	Reporty v podobě průběhových i koláčových grafů		
19	Online reporty včetně možnosti exportu do PDF a CSV formátu		

20	Automatické zasílání reportů emailem (reporty v českém a anglickém jazyce)		
21	Řízení uživatelského přístupu k jednotlivým typům reportů (uživatel je oprávněn zobrazovat pouze statistiky, ke kterým mu bylo nastaveno oprávnění administrátorem)		
22	Výpis tzv. top N statistiky podle různých kritérií (počet přenesených bytů, paketů, toků atd.) umožňující vypsat nejaktivnější či anomální počítače podílející se na síťovém provozu		
23	Upozornění administrátorům v případě vzniku uživatelem definované situace (např. nadměrný přenos dat, výskyt nebezpečné anomálie, použití zakázané aplikace atd.) prostřednictví emailu, SNMP trapu a syslogu		
24	Vytváření profilů pro ukládání dat vyhovující nadefinovaným filtrům (např. HTTP, FTP, SMTP, SSH provoz);		
25	Podrobné textové výpisy jednotlivých toků s možnostmi filtrování a agregace		
26	Drill-down – možnost dohledat každý jednotlivý tok zaznamenaný sondami		
27	Detekce aktivních zařízení na sítí - pro podporu konceptu BYOD		
28	Podpora geolokace na základě IP adresy		
29	Otevřené rozhraní s možnostmi skriptování a zpracování dávkových úloh		

Tabulka č. 4 - Modul detekce anomálií na síti (NBA)

Parametr	Popis požadovaného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
1	SW modul bez nutnosti pořízení dodatečného HW		
2	Sběr a zpracování statistik o síťovém provozu (NetFlow, sFlow, jFlow);		
3	Detekce nežádoucích vzorů chování na síti (útoky, anomálie datového provozu, nežádoucí aplikace, detekce virů a botnetů ve vnitřní síti, detekce odchozího spamu, provozních problémů)		
4	Detekce anomálií vzhledem k dlouhodobému profilu chování zařízení na síti		
5	Předdefinovaná sada pravidel pro odhalování obecných anomálií v síti		
6	Vyhodnocování na základě implementace standardu Bidirectional flows (RFC 5103)		
7	Přehledný dashboard s okamžitou indikací problémů a top statistik		
8	Integrace informací ze služeb DNS, WHOIS, geolokační služby		

9	Výstup událostí protokolem Syslog pro možnost integrace do řešení Q Radar SIEM		

Tabulka č. 5 - UTM

Parametr	Popis požadovaného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
1	Antispam, Antivirus, Antispyware		
2	URL filtrace - automatické řízení web přístupů zaměstnanců		
3	Integrované plnohodnotné IPS, s konfigurací automatického vypnutí IPS ochrany v případě přetížení HW (využití CPU nebo fyzické paměti) nad definovanou prahovou hodnotu		
4	Ochrana VoIP provozu aplikačními proxy pro SIP a H.323		
5	Filtrování internetového spojení (URL, IM, P2P, RAT, Anonymizers, …)		
6	IPSec VPN, průchodnost VPN 250 Mb/s		
7	Licence pro konkurentní klientské připojení do VPN pomocí IPSec - min 20 kusů		
8	Licence pro konkurentní klientské připojení do VPN pomocí SSL - min 20 kusů		
9	Podpora VLAN		
10	Cluster management (active/active nebo active/standby) s možnosti nasazení do virtuálního prostředí		
11	Propustnost až 1.1 Gb/s pro aplikační kontroly		
12	Non open-source		
13	Antivirus a ochrana před spyware a červy na úrovni brány včetně schopnosti skenovat e-mail (SMTP), a webové (HTTP, HTTPs) přenosy v reálném čase a zjišťovat potenciální hrozby skryté uvnitř legitimního provozu		
14	Vícevrstvá ochrana na úrovni brány, která je zaměřena proti hrozbám a narušením souvisejícím se spyware včetně nepřetržitě aktualizované sady anti-spyware podpisů s možností filtrování webových stránek (další proaktivní ochrana, neboť blokuje webové stránky, u kterých je známo, že distribuují spyware)		

15	Možnost rozšíření systému o emulace neznámých hrozeb (zero-day sandboxing) typů souborů: powerpoint, word, excel, pdf, exe, archivy (zip, tar, 7z) s možností řízení, které soubory budou zasílány na dynamickou sandbox analýzu		
16	Možnost rozšíření řešení o DLP modul – počet předefinovaných datových typů (včetně lokalizovaných datových typů pro ČR), min. 500		
17	Volitelná možnost zapnutí ochran pro útoky cílené na web servery (např. na přetečení buffer nebo tkz. injekce SQL, ...);		
18	Filtrování webových stránek		
19	Site-to-site VPN propojení		
20	Bezpečný flexibilní vzdálený přístup pomocí IPSec a SSL, výkonná IPSec a SSL konektivita		
21	Služba vlastní certifikační autority pro vydávání PKI certifikátů pro uživatele		
22	Integrovaná správa, která umožňuje z jedné konzole centrálně spravovat i více firewalů a ze které mohou administrátoři definovat a spravovat jednotlivé prvky bezpečnostní politiky: bezpečnost firewallu, překlad síťových adres (NAT), kvalitu služeb (QoS), bezpečnost VPN klientů a sítě VPN, aplikační filtrace, IPS, AV&AS		
23	Centralizované automatické aktualizace;		
24	Monitorování v reálném čase a flexibilní vytváření reportů; centrální řízení logů s možností inkorporace zařízení třetích stran;		
25	Jednoduché zálohování a obnova systému (nejen částí, ale celé konfigurace);		
26	Možnost tvorby clusterů a vysoká dostupnost (provoz v případě nedostupnosti primárního rozhraní je směrován na sekundární rozhraní nebo ISP spoj. I během selhání se spojení udržují nepřerušená);		
27	Volitelný modul pro řízení (shaping) provozu VPN s přiřazováním priorit kritickým obchodním aplikacím a uživatelům pro optimalizovaný výkon		
16	Systém musí být plně integrovatelný se systémy IBM Security Q Radar SIEM.		

Tabulka č. 6 - UTM hardware a nasazení			
Parametr	**Popis požadovaného parametru**	**Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
1	Nasazení řešení v režimu HA. (Pro management je možné využít stávající virtualizační VMware infrastruktury)		
3	Minimálně 1x procesor čtyřjádrový architektury x86, L3 cache alespoň 10MB, frekvence alespoň 2,4 GHz (s možností rozšíření na 2 procesory);		
4	Paměť RAM minimálně 12 GB RAM DDR3, rozšiřitelná až na 768 GB;		
5	Minimálně 2x HDD 500 GB 7200 rpm SATA, HW RAID řadič s podporou RAID 0/1/1+0;		
6	Minimální podporovaná velikost diskové kapacity pro dlouhodobé ukládaní log záznamů na Management serveru pro UTM (jeli disková kapacita omezena licencí, licence pro požadovanou velikost musí byt součástí nabídky) - min. 16 TB;		
7	Rozšiřitelnost až na 16 disků u Management serveru pro UTM (pouze v případě nevyužití stávající infrastruktury)		
8	Interní USB port kompatibilní se standardy ACPI 2.0, PCI 2.2 a USB 2.0;		
9	8x UTP 1Gb Ethernet port, minimálně na dvou nezávislých NIC čipech;		
10	2x 10Gb Ethernet port;		
11	2x redundantní napájecí zdroj;		
12	Vzdálená správa: vzdálený přístup přes dedikované ethernet rozhraní, ochrana heslem, zabezpečení komunikace SSL, AES/3DES, RC4, vzdálený přístup umožňuje provést tyto operace se serverem: power on/off, reset, remote control, update BIOS, výběr bootovacího zařízení, remote control umožňuje sledovat		

	start serveru (bios), start OS a běh OS (grafické i textové rozhraní), možnost vyvolat NMI přerušení nedostupného OS, virtuální KVM konsole, podpora virtuálních médií (CD, DVD, ISO image, USB disk, vzdálený adresář), možnost využití běžných www prohlížečů integrovaných v desktopovém OS pro správu serverů (IE, Firefox);		
13	Prediktivní analýza poruch na pevné disky, procesory a paměť;		
14	Certifikovaný Hardware pro provoz dodávaného UTM;		
15	Provedení do racku, rozměr max. 2RU;		