

## Bezpečnost infrastruktury GDS

### 1.1 Obecná charakteristika

Bezpečnost infrastruktury a celkového řešení je klíčovým požadavkem. Infrastruktura musí umět zajistit integritu a důvěrnost komunikace na celé trase přenosu. Infrastruktura musí být schopna ověřit uživatele před přístupem do sítě, rozpoznat parametry připojení (zařízení, jeho vlastnosti, místo, kontext připojení), přidělit uživatelům přístupová práva k síti, zaznamenávat a vyhodnocovat informace o jejich aktivitách s vazbou na resortní identity management (dále jen IDM). V každém místě sítě musí být možné identifikovat uživatele, který data odeslal.

Infrastruktura musí být odolná proti útokům typu Denial of Service, útokům cíleným na jednotlivé uzly, přenosové trasy, kritické služby i útokům vedeným na síť jako celek. Infrastruktura musí poskytovat informace o bezpečnostních incidentech a směřovat je do centrálních dohledových systémů.

### 1.2 Upřesnění požadavků na řešení – Jednotné řízení přístupu do sítě pro uživatele i připojená zařízení

Infrastruktura a řídicí systém musí splňovat následující požadavky:

- Systém musí umožňovat centralizovanou definici pravidel pro řízení přístupu. Pravidla mohou být realizována v síťové infrastruktuře, například na přístupových LAN přepínačích. Pravidla nesmí záviset na síťové topologii a adresování, jsou určována rolemi uživatelů a stavem jejich zařízení.
- Uživatelé musí být ověřováni jednotně v pevných sítích, v bezdrátových sítích a při vzdáleném přístupu přes VPN s vazbou na IDM.
- Uživatelé nebo zařízení v LAN sítích musí být ověřováni metodou 802.1x, přes web rozhraní a MAC adresou.
- Pro AAA funkce musí být využíván RADIUS protokol.
- Systém musí podporovat autentizační metody PAP, MS-CHAPv1/v2, PEAP, PEAP-TLS, EAP-MD5, EAP-GTP, EAP TLS, EAP-MSCHAP, EAP FAST.
- Uživatelé mohou být ověřováni pomocí X.509 certifikátů, podpora Common Access Card (CAC).
- Systém musí spolupracovat s vnějšími systémy: Active directory, LDAP, Radius Token Server, Remote Supervisor Adaptor (RSA), resortní IDM.
- Ověřovací systém v součinnosti s infrastrukturou musí rozpoznávat typ připojených zařízení bez nutnosti instalovat softwarový modul na tato zařízení.
- Systém musí dokázat klasifikovat připojená zařízení podle jejich hardwarových a softwarových vlastností a stavu (typ zařízení, verze OS, aktualizace OS, instalované aplikace a jejich verze, spuštěné služby, certifikáty) a podle místa připojení.
- Klasifikaci zařízení a informace o uživateli lze využít k řízení přístupu na okraji sítě i na hranici bezpečnostních zón (například na hranici datového centra apod.).

- Řešení musí umožňovat pravidelnou kontrolu stavu připojených stanic. Pro neaktualizovaná koncová zařízení systém musí omezit přístup, zajistit jejich izolaci, a to i v průběhu jejich připojení. Řešení musí vynutit aktualizaci připojených zařízení a automaticky obnovit přístupová práva po aktualizaci.
- Přístupová pravidla lze měnit i v průběhu připojení stanic s využitím RADIUS CoA (Change of Authorization).
- Systém musí umožnit okamžitě zablokovat nebo omezit přístup jednotlivých uživatelů (zařízení) a definované skupiny uživatelů (zařízení).
- Řešení musí podporovat přidělování dočasných přístupových oprávnění.
- Řešení musí podporovat monitorování připojených stanic, zaznamenávání informací o průběhu jejich přihlašování, o jejich činnosti, souhrnné i podrobné výkazy o aktivitách připojených stanic a uživatelů, zpracování výstrah v reálném čase.
- Architektura ověřovacího systému musí být distribuovaná, odolná proti výpadkům.
- Systém musí být rozšiřitelný až do 50000 připojených zařízení.
- Řešení musí umožňovat definici rolí administrátorů a jejich oprávnění k řídicímu systému.
- Centrální ověřovací a řídicí systém musí splňovat FIPS 140-2 Common Criteria EAL2.
- Systém musí být využitelný pro řízení přístupu k aktivním prvkům sítě.

### **1.3 Důvěrnost a integrita komunikace**

Řešení musí umožnit šifrovanou komunikaci na celé trase přenosu až po úroveň koncových stanic.

### **1.4 Odolnost proti útokům**

LAN přepínače – hardwarové zdroje i softwarové funkce – musí být odolné proti útokům typu Denial of service. LAN přepínače musí být odolné proti záplavám rámci typu unicast, multicast i broadcast. LAN přepínače musí být odolné proti záplavám rámci s náhodně generovanými MAC adresami. Přepínače musí umět omezit počet MAC adres viditelných za jednotlivými porty přepínače.

LAN přepínače chrání protokoly DHCP a ARP proti útokům. Zablokují komunikaci neautorizovaného DHCP serveru. Zabrání manipulaci útočníka s ARP tabulkami připojených stanic.

LAN přepínače rozpoznají nepovolenou manipulaci koncových stanic s přidělenými IP adresami a takovou komunikaci zablokují.

### **1.5 Monitorování útoků**

LAN přepínače musí umožňovat přesměrování rámce na vybrané porty nebo do monitorovací VLAN sítě.

LAN přepínače musí umožňovat odesílání sumarizovaných informací o tocích dat v síti do monitorovacích systémů.

LAN přepínače mohou mít vestavěný analyzátor paketů pro účely analýzy provozu.

## 2 IP ekosystém

Nově budovaná datová síť musí splňovat přísné požadavky na bezpečnost a spolehlivost. Kromě robustní infrastruktury se budou do systému integrovány následující součásti:

- DNS / DHCP server,
- AAA server,
- NTP server – zdroj přesného času.

### 2.1 DNS / DHCP server

Základem nově budované infrastruktury je dynamické přidělování IP adres. Po přidělení nebo uvolnění IP adresy jsou automaticky aktualizovány záznamy v DNS serveru.

Přidělování IP adres musí být navrženo jako centrální systém s architekturou HA. Požadujeme instalaci dvou centrálních databázových serverů. Každý server bude umístěn v jiném datovém centru. Datová centra jsou umístěna v různých lokalitách.

Na centrálním serveru musí být zároveň provozována centrální evidence všech IP zařízení v systému. Tato evidence je online aktualizovaná z jednotlivých DNS / DHCP serverů.

Pro zabezpečení vysoké dostupnosti musí být lokality, kde jsou instalovány přepínače P1-MPLS až P3-MPLS, D1-L3 a D2-L3, vybaveny DNS/DHCP serverem, který zabezpečuje přidělování IP adres. Lokality P2-MPLS, P3-MPLS a D1-L3 slouží zároveň jako záloha pro lokality P1-MPLS a D2-L3.

DNS/DHCP server musí:

- DHCP – současně přidělovat IP adresy IPv4 a IPv6,
- DHCP – umožňovat zasílání tzv. options dle RFC 2132,
- DHCP – zajistit zabezpečený update DHCP serverů,
- DNS – pracovat v režimu Master/Slave,
- DNS – zajistit zabezpečený update DNS serverů.

Přístup do centrální databáze je ověřován přes centrální AAA server. Uživatelé jsou rozděleni do skupin, kdy každá skupina má přístup do předem definovaných adresního prostoru. Připojení k systému je realizováno pomocí zabezpečeného připojení.

DNS/DHCP servery jsou pomocí SNMP protokolu dohlíženy z centrálního dohledového systému.

DNS/DHCP server musí obsáhnout adresní prostor 10.0.0.0/8. Maximální počet přidělovaných IP adres bude maximálně 30 000. Celý systém musí být pouze licenčně rozšiřitelný na konečný stav 50 000 IP adres.

Jednotlivé DNS/DHCP servery dělíme dle výkonu do dvou skupin:

- vysoká zátěž – server umožňuje minimálně 30 000 DNS dotazů za sekundu a přiřazení 3 000 IP adres za sekundu,

- standardní zátěž – server umožňuje minimálně 10 000 DNS dotazů za sekundu a přiřazení 500 IP adres za sekundu.

## 2.2 AAA Server

Základem bezpečnosti v nově budované síti je znemožnění přístupu k síti nežádoucím uživatelům a kontrola legitimních uživatelů. Pro ověřování budou použity prostředky AAA (Authentication, Authorization, Accounting).

AAA server musí být navržen jako centrální systém s architekturou HA. Požadujeme instalaci dvou centrálních databázových serverů. Každý server bude umístěn v jiném datovém centru. Datová centra jsou umístěna v různých lokalitách.

AAA server bude poskytovat ověřování pro:

- přístup do sítě poskytovaný protokolem IEEE 802.1X,
- přístup k aplikacím jako je např. dohledový systém, administrace systémů,
- přístup k zařízením jako jsou např. datové a hlasové prvky GDS.

Autentizace identity uživatele bude ověřena autentizační autoritou, tzn. serverem RADIUS s použitím protokolů EAP. Server AAA provede autorizaci a tak přidělí přístupová práva uživateli, který úspěšně absolvoval proces autentizace, respektive nepřidělí těchto práv uživateli, který autentizačním požadavkům nevyhověl. V neposlední řadě musí AAA server provádět sběr provozních informací o autorizovaném uživateli, kde se bude jednat např. o údajích o přeneseném množství dat, trvání připojení k síti a identifikaci přístupového bodu, ze kterého bylo k síti přistupováno apod.

Protokol EAP musí zabezpečit vzájemnou autentizaci nejen klienta k autentizačnímu serveru, ale i autentizačního serveru ke klientovi. Požadujeme minimálně podporu následujících protokolů EAP:

- EAP – MD5 (RFC 3748),
- EAP – PSK (RFC 4764),
- EAP – TLS (RFC 5216).

Pro autorizaci musí AAA server umožnit zasílání atributů dle standardu RFC3580. Tyto atributy musí být možné upravovat tak, aby odpovídali atributům, kterým rozumí jednotliví výrobci technologií.

AAA server musí umožnit autorizaci a následnou autentizaci minimálně dle:

- hesla,
- identifikační karty,
- X.509 digitálního certifikátu,
- MAC adresy.

Databázi uživatelů požadujeme ukládat buď v interní databázi, centrální LDAP databázi nebo v Microsoft Active Directory.

AAA server je pomocí SNMP protokolu dohlížen z centrálního dohledového systému. Požadujeme AAA server dodat v licenci pro 30 000 uživatelů s možností upgradu na 50 000 bez nutnosti změny hardwaru.

Zatížení AAA serveru je nutné spočítat z celkového počtu obsazených portů v síti (počítaná neobsazenost 5%). Obnovu autentizace předpokládáme každých 20 minut.

### **2.3 NTP server – zdroj přesného času**

Zdroj přesného času bude distribuován napříč celou infrastrukturou. V hlavním i záložním datovém centru bude nainstalován hlavní a záložní NTP Stratum 3 server. Oba NTP servery jsou připojeny k centrálním zdrojům hodin mikrovlnného SDH přenosového prostředí.

Hlavní a záložní NTP server bude distribuovat čas do všech P1-MPLS až P3-MPLS zařízení, D1-L3 a D2-L3 zařízení. Tato zařízení budou synchronizovat ostatní koncová zařízení. Přiřazený NTP server se bude distribuovat pomocí DHCP protokolu.

### **2.4 Zabezpečení IP ekosystému v jednotlivých lokalitách**

V lokalitách musí být zabezpečeny základní služby IP a hlasové sítě, které jsou centralizovány, ale pro zabezpečení vysoké dostupnosti jsou distribuovány. Jedná se především o:

- DNS/DHCP server,
- Nouzový AAA Server,
- Pomocný RSHS.

Tyto služby budou virtualizovány a provozovány na HW zařízením s vysokou dostupností a spolehlivostí. HW zařízením s vysokou dostupností a spolehlivostí se rozumí:

- certifikovaný hardware výrobcem virtualizovaného prostředí,
- redundantní hot-swap napájecí zdroje,
- redundantní hot-swap ventilátory,
- Hot-swap SAS pevné disky s podporou řadiče RAID,
- redundantní NIC.

Dostupnost hlasové služby

## **3 Funkcionality bezpečnostních prvků GDS**

### **3.1 TAP (test access point/traffic access ports)**

Zařízení musí být neintrusivní pro 100% bezpečnost, monitorování provozu na lince v reálném čase, všech 7 vrstev a jakékoliv velikosti paketů včetně chyb. Musí být neviditelné pro síťové okolí a nesmí zasahovat do nastavení auto negotiation rychlosti nebo duplexu. Dále musí mít vlastnost trvalého síťového připojení a tím garantovat stálou síťovou konektivitu i v případě selhání napájení (při výpadku napájení nejsou pakety přeposílány do monitorovacího zařízení, nicméně monitorovaná linka je nepřerušena) a nulovou ztrátovost paketů při výpadku napájení.

Regenerační TAPy poskytují permanentní pasivní monitorovací porty pro 100% náhled do síťové linky přes několik na sobě nezávislých monitorovacích portů (jsou vybaveny dvojicí síťových a několika dvojicemi monitorovacích portů). Je kompatibilní se všemi bezpečnostními a síťovými management nástroji. Každé monitorovací zařízení připojené do

regeneračního TAPu vidí stejný provoz ve stejnou chvíli a poskytuje kompletní obraz linky pro sledování bezpečnosti síťového provozu.

Klasické tapy na rozdíl od regeneračních TAPů jsou vybaveny pouze dvojicí monitorovacích portů (pro připojení pouze jednoho bezpečnostního monitorovací nástroje).

Z důvodu připojení linky dělíme TAPy na TAP metalický s přenosovou kapacitou do 1 Gbs a TAP optický s přenosovou rychlostí 10 Gbs.

Další technické parametry jsou uvedeny v specifikačním listě.

### **3.1.1 Obecné požadavky**

- 100% pohled na tok dat (všech 7 vrstev a jakékoliv velikosti paketů včetně chyb),
- monitorování provozu na lince v reálném čase,
- redundantní napájení,
- garance stálé síťové konektivity i v případě selhání napájení,
- bezpečný jednosměrný datový tok k monitorovacím portům,
- in-line zapojení,
- indikace linky.

## **3.2 NetFlow monitoring**

Bezpečnostní zařízení musí umožňovat dlouhodobé detailní monitorování dění na počítačové síti. Získané informace o dění na síti a chování uživatelů musí umožnit v reálném čase sledovat a vyhodnocovat bezpečnostní hrozby v síti. Je nezbytné, aby bezpečnostní zařízení bylo nezávislé na použité síťové infrastruktuře a svou funkcí neovlivňovalo sledovanou síť. Ze strany monitorované sítě nesmí být zařízení detekovatelné. Vytváření síťových statistik musí být prováděno pomocí nezávislých a k tomuto účelu určených zařízení.

Bezpečnostní zařízení musí pracovat s technologií NetFlow ve verzi v5,v9 (nebo IPFIX RFC 3917, RFC 3955). Tato technologie je v současné době nejpresnější a nejmodernější prostředkem pro monitorování sítě a oproti konkurenčním technologiím nabízí výhody zpracování všech paketů bez vzorkování, imunitu vůči šifrovanému provozu, škálovatelnost i pro vysokorychlostní a zatížené sítě a průmyslovou standardizaci. Díky standardizaci je možné jeden zdroj statistik využít i v dalších systémech.

### **3.2.1 Obecné požadavky**

- ucelené škálovatelné řešení umožňující dlouhodobé monitorování sítě na bázi technologie NetFlow (nutná podpora NetFlow v5 a NetFlow v9, IPFIX),
- nezávislost na použitých aktivních prvcích, nesmí docházet k ovlivňování chování sítě,
- specializovaná dedikovaná zařízení (sondy) pro vytváření detailních statistik IP toků o dění na síti, standardizovaný protokol pro výměnu dat o IP tocích (NetFlow ve verzi v5,v9 nebo IPFIX RFC 3917, RFC 3955),
- dlouhodobé ukládání statistik IP toků a jejich centrální sledování a vyhodnocování bezpečnostních hrozeb v síti, prokazování bezpečnostních incidentů,
- podpora IPv4, IPv6, VLAN, MPLS, Ethernet 10Mb/s až 10Gb/s, otevřené rozhraní s možností integrace libovolných nástrojů i třetích stran,
- systém ověřený instalacemi na páteřních datových linkách (10GE) u poskytovatelů v EU,

- systém ověřený v ČR, NATO nebo US DoD,
- detekci vnitřních i vnějších útoků,
- efektivní dohledání a řešení incidentů v síti,
- podpora upozornění na detekované problémy v síti pro zvýšení bezpečnosti sítě,
- přehledné a podrobné grafické uživatelské rozhraní,
- spolupráce s dalšími implementovanými technologiemi v sledované síti,
- možnost připojení do stávající datové infrastruktury pomocí rozhraní TAP (test access point),
- flexibilní architektura, škálovatelnost, možnost dalšího rozšíření.

### 3.3 NetFlow kolektor

NetFlow kolektor musí být výkonné zařízení s vyšší diskovou kapacitou primárně určené pro sběr, zobrazení, analýzy a dlouhodobého uložení síťových statistik z NetFlow dat exportovaných z aktivních prvků (s podporou NetFlow v5,v9 nebo IPFIX) nebo NetFlow senzorů s podporou HW akcelerace.

#### 3.3.1 Obecné požadavky

- možnost sběru NetFlow dat s neomezeného počtu aktivních prvků (s podporou NetFlow v5,v9 nebo IPFIX) a NetFlow senzorů,
- podpora verze NetFlow protokolu – programové vybavení kolektoru musí umožnit sběr a vyhodnocení NetFlow dat ve verzi 5 a 9 nebo IPFIX,
- datová bezpečnost – ukládání dat na RAID pole (Redundant Array of Independent Disks). V případě výpadku jednoho disku je systém stále v praceschopném stavu a nedojde ke ztrátě uložených NetFlow dat. Poškozený disk lze za běhu systému vyměnit,
- kapacita datového úložiště – systém je schopen sbírat a ukládat dlouhodobě data z několika NetFlow zdrojů,
- požadovaná minimální disková kapacita datového úložiště při RAID 6: 12 TB,
- rozšiřitelnost o SW moduly pro rozšíření funkcionalit senzoru (např. NBA-behaviorální analýza, nástroj pro reportování),
- konfigurační a monitorovací centrum (pro detailní analýzu NetFlow dat ve formě grafů, tabulek, výpisů komunikací atd.) prostřednictvím WEB rozhraní,
- rozšíření funkcionality o SW moduly (pluginy), jako např. SW moduly pro analýzu chování sítě (NBA-Network Behavior Analysis),
- licencování per zařízení bez omezení typu počet zdrojů dat, množství monitorovaných toků nebo počet uživatelů systému.

Další technické parametry jsou uvedeny v specifikačním listě.

### 3.4 SW moduly pro NetFlow kolektor

Pro NetFlow kolektory jsou vyžadovány SW moduly (pluginy) pro rozšíření funkcionality z oblasti síťové bezpečnosti týkající se detekce anomálií (ADS) a analýzy chování sítě (NBA/NBAD).

#### 3.4.1 Parametry - SW rozšiřující modul FlowMon ADS

FlowMon ADS je moderní systém detekce anomálií a nežádoucího chování na síti, který je založený na permanentním vyhodnocování a analýze NetFlow dat. Hlavním přínosem

pluginu je odhalení provozních problémů a zvýšení vnější i vnitřní bezpečnosti datové sítě. Hlavní výhodou proti IDS systémům je orientace na celkové chování zařízení v síti, což umožňuje reagovat na dosud neznámé nebo specifické hrozby, pro které není dostupná signatura.

Další technické parametry jsou uvedeny v specifikačním listě.

### 3.4.2 SW rozšiřující modul Cognitive Analyst

Cognitive Analyst je systém zaměřený na ochranu sítě proti síťovým útokům za použití analýzy chování sítě (Network Behavior Analysis – NBA). Cílem systému je rozšíření současně dostupných bezpečnostních řešení o detekci moderních útoků jako jsou APT a zero-day útoky, polymorfní malware, útoky na míru a další hrozby, které není možné odhalit tradičními přístupy na bázi rozpoznávání vzorů. Systém disponuje unikátním adaptačním mechanismem a díky tomu se neustále v čase optimalizuje. Je založen na využití umělé inteligence a speciálních detekčních algoritmů, které zajišťují nízký počet falešných poplachů.

Další technické parametry jsou uvedeny v specifikačním listě.

## 3.5 NetFlow senzor

NetFlow senzory musí být výkonné autonomní monitorovací zařízení pro všechny typy sítí od 10 Mb/s do 40 Gb/s určené pro sledování komunikace na počítačové síti a vytváření NetFlow statistik.

### 3.5.1 Obecné požadavky

- monitoring provozu na počítačové síti v reálném čase,
- vytváření statistik ve formátech NetFlow v5,v9,
- zpracování dat 10 Gb/s bez ztráty paketů,
- konfigurační a monitorovací centrum (pro detailní analýzu NetFlow dat ve formě grafů, tabulek, výpisů komunikací atd.) prostřednictvím WEB rozhraní,
- vestavěný kolektor pro zobrazení a analýzu NetFlow dat,
- kompatibilita s NetFlow kolektory ostatních výrobců,
- neviditelnost na L2 a L3 vrstvě,
- rozšiřitelnost o SW moduly pro rozšíření funkcionalit senzoru (např. detekce NATů v síti, logování přístupů na webové servery, atd.),
- podpora současného exportu NetFlow statistik minimálně na 5 cílů současně,
- podpora filtrování dat na sondě podle IP adres a VLAN,
- podpora pro IPv4, IPv6, VLAN a MPLS,
- snadná instalace do stávající síťové infrastruktury pomocí TAPu.

Další technické parametry jsou uvedeny v specifikačním listě.

## 3.6 IPS monitoring

Zařízení *Intrusion Prevention Systems* (IPS, tj. systémy pro prevenci průniku), také známé jako *Intrusion Detection and Prevention Systems* (IDPS, tj. systémy pro detekci a prevenci průniku), musí mít schopnost shromažďovat důkazy o aktivitě útočníka, likvidovat přístup útočníka do sítě, a překonfigurovat síť tak, aby odolala technice útočnickova průniku. Systém IPS musí umět zastavit útoky u zdroje hrozby a proaktivně chránit proti budoucím



hrozbám a zranitelným místům a přitom zůstat pro síť transparentní. S pokročilou in-line prevencí proti průnikům musí být zařízení schopno upozornit na útok, zničit problematické pakety, ukončit relaci pro útoky na bázi TCP a UDP a dynamicky zřídit firewall. Konkrétněji, IPS může provádět takové akce jako vyvolání poplachu, filtrování škodlivých paketů, násilné resetování spojení a/nebo blokování provozu z podezřelé IP adresy, blokování útočníků, ke zmírnění útoků DoS (Denial of Service), k zabránění krádeží informací a k zajištění bezpečnosti VoIP (Voice over IP) komunikace s využitím obsáhlé knihovny zranitelností a signatur.

### 3.6.1 Obecné požadavky

- *Analýza v reálném čase* – pouze v případě, že systém pracuje v reálném čase, je možné zachytit veškeré nežádoucí pakety a blokovat podezřelý provoz.
- *Spolehlivost a dostupnost* – je důležité pokusit se minimalizovat selhání systému, v opačném případě zůstane síť nechráněná a význam zařízení v síti je minimální. Systém také musí zůstat v činnosti i při aktualizaci databáze signatur a po jejím úspěšném dokončení by neměl být vyžadován restart.
- *Pružnost* – pokud již dojde k výpadku systému, je nutné provoz přesměrovat na další aktivní prvek, který by měl být schopen zajistit aspoň částečnou ochranu.
- *Malé zpoždění* – systém IPS by měl pracovat dostatečně rychle, aby zvládal analyzovat veškerý provoz v reálném čase. Zpoždění IPS by mělo přibližně odpovídat zpoždění, které nastává na směrovačích či přepínačích.
- *Vysoký výkon* – rychlost zařízení by měla být dostatečná, aby bylo možné s rezervou kontrolovat veškerý provoz na síti i při značném vytížení linky.
- *Přesnost detekce* – Systém prevence by měl generovat co nejmenší počet false positive poplachů. K tomu dochází např. v důsledku neaktualizované databáze signatur. Chybějící signatury by měly být doplňovány s dostatečnou rychlostí a bez nutnosti restartovat senzor, případně celé zařízení.
- *Různorodá kontrola* – systém by měl být schopen rozeznat, zdali se podezřelý provoz týká již konkrétního útoku, porušení pravidel nebo chyby na úrovni uživatele.
- *Schopnost upozornění* – v případě detekce nebezpečného provozu musí být zařízení schopno včas a důkladně informovat pověřenou osobu (výpis do konzole, uložení záznamu do databáze atd.)

Pro zabezpečení požadavku jsou požadovány:

A – Sondy s propustností 500 Mbps na přístupové body – 10/100/1000Mb  
(viz specifikační list)

B – Sondy s propustností 1 Gbps na přístupové body – 10/100/1000Mb  
(viz specifikační list)

C – Sondy páteřní – 10Gb  
(viz specifikační list)