Popis technického riešenia

1. Predmet ponuky a hlavné črty navrhovaného technického riešenia

Predmetom ponuky je poskytovanie elektronických komunikačných služieb privátnej dátovej siete (ďalej len „VPN“) pre vzájomnú internú komunikáciu Úradu a regionálnych úradov a špeciálnych stavebných úradov a iných súvisiacich organizácií s možnosťou flexibilného nárastu potrebných kapacít (ďalej len „Úrad“) a poskytovanie komplexných služieb, pod ktorými sa rozumie zriadenie, prevádzkovanie, monitorovanie, správu a prípadný servis použitých koncových zariadení a komponentov.

Spoločnosť Slovanet ponúka unikátne technické riešenie vyvinuté pre Úrad s vyhradením sieťových kapacít len pre Úrad s tým, že VPN vytvorená pre Úrad je separovaná od ostatných používateľov siete.

Predkladané technické riešenie umožňuje poskytovať komplexný rámec IP/MPLS služieb s požadovanou šírkou pásma, zabezpečením, zohľadňuje všetky požiadavky na kvalitu služby a bezpečnostné parametre definované v špecifikácii výberového konania (súťažných podkladoch a odpovediach na otázky uchádzačov).

V sieti Slovanet sú zabezpečované komplexné monitorovacie a manažmentové funkcie, tieto umožňujú poskytnúť Úradu požadovaný reporting a efektívnu súčinnosť pri odstraňovaní porúch.

Vyjadrenie uchádzača k požiadavkám verejného obstarávateľa (splnenie jednotlivých požiadaviek opisu predmetu zákazky):

Východisková situácia

Slovanet pri dizajne technického riešenia vychádzal z popisu východiskovej situácie, ktorej porozumel a chápe zámery a potreby Úradu.

Stanovisko uchádzača:
Zaznamenané a v plnom rozsahu akceptované

Identifikácia základných potrieb

- ✓ vybudovanie a prevádzkovanie služieb privátnej dátovej siete pre vzájomnú internú komunikáciu Úradu a regionálnych úradov a špeciálnych stavebných úradov a iných súvisiacich organizácií s možnosťou flexibilného nárastu potrebných kapacít;
- ✓ vybudovanie a prevádzkovanie zabezpečeného centrálneho prestupu do siete Internet;
- ✓ integrácia prepojenia do siete Govnet (už zrealizované);
- ✓ vybudovanie a prevádzkovanie centrálneho zabezpečeného prístupu do privátnej siete pre interných a externých užívateľov;
- ✓ vybudovanie a prevádzkovanie LAN sietí na pracoviskách Úradu a regionálnych úradov;
- ✓ vybudovanie a prevádzkovanie WiFi sietí (pre internú aj externú potrebu) na pracoviskách Úradu a regionálnych úradov;
- ✓ vybudovanie a prevádzkovanie samostatného prístupu do siete Internet pre externých užívateľov WiFi sietí s logicky oddelenou prevádzkou od internej komunikačnej prevádzky;
- ✓ vybudovanie a prevádzkovanie podpornej infraštruktúry (dátové stojany / rozvádzače a záložné zdroje napájania UPS) na pracoviskách Úradu a regionálnych úradov;

- ✓ poskytovanie služieb multimediálnej komunikácie medzi jednotlivými pracoviskami;
- ✓ príprava na integráciu záložného dátového centra do privátnej dátovej siete;
- ✓ príprava na integráciu bezpečnostných a „office friendly“ riešení (kamerové systémy, interaktívne tabule, manažment fyzického vstupu do objektu, dochádzkový systém, a pod.) do LAN sietí na pracoviskách Úradu a regionálnych úradov;
- ✓ monitorovanie prevádzky a služieb privátnej dátovej siete;
- ✓ poskytovanie služieb bežnej prevádzkovej podpory a technickej podpory na vyžiadanie pri rozšírení služieb a/alebo zmene konfigurácie služieb.

Stanovisko Slovanet:
Zaznamenané a v plnom rozsahu akceptované
Ponuka uchádzača v plnom rozsahu zohľadňuje požiadavku Úradu na špecifikáciu jednotlivých základných potrieb a parametrov služby privátnej siete.
Navrhované riešenie pre pripojenie Lokality/Pracoviska je spracované s dôrazom na vysokú dostupnosť a redundanciu a v závislosti podľa lokality a požadovaného SLA sú primárne a záložné pripojenia realizované nezávislými fyzickými trasami s využitím optickej, metalickej alebo rádiovej (resp. bezdrôtovej) infraštruktúry v licencovanom pásme. Komunikačný profil pre primárne trasy je navrhnutý na 100% garantovanej kapacity, bez agregácie.

Základné požiadavky

Slovanet v plnom rozsahu plní požiadavku Úradu na poskytnutie „komplexnej služby“ a v riešení nie sú použité žiadne komponenty, ktoré by predstavovali zjavné alebo známe skryté bezpečnostné riziká pre VPN sieť. Zároveň sú všetky koncové zariadenia, prostredníctvom ktorých budú služby poskytované nové, t.j. ktoré nebolo nikdy a nikde nainštalované, okrem vybalenia zariadenia a jeho prvotnej konfigurácie.

Navrhované technické riešenie bolo z hľadiska spoľahlivosti a bezpečnosti auditované (preverené) nezávislou certifikovanou autoritou s CISA bezpečnostným certifikátom (Certified Information Systems Auditor) a vyhovuje bezpečnostným štandardom na bezpečnosť virtuálnych privátnych sietí.

Stanovisko Slovanet:
Zaznamenané a v plnom rozsahu akceptované

Podrobná špecifikácia predmetu zákazky

Služby sieťovej konektivity

Dátovú komunikačnú infraštruktúru Úradu a partnerských organizácií bude tvoriť dátová virtuálna privátna sieť vrátane jej komponentov a infraštruktúry na úrovni WAN aj LAN vo všetkých lokalitách, resp. pracoviskách. Dátové pripojenie bude určené na vzájomnú elektronickú komunikáciu s ostatnými pracoviskami navzájom a bude zabezpečovať pripojenie na externé siete Internet a GOVNET.

Stanovisko Slovanet:
Zaznamenané a v plnom rozsahu akceptované
Bližšie informácie o navrhovanom riešení sú predložené v nasledujúcich kapitolách.

Bezpečnostné služby

Privátna dátová sieť poskytne bezpečnú komunikáciu. Pripojenie sa požaduje šifrované a prostredníctvom šifrovacích protokolov sa požaduje selektívne definovať bezpečnostné parametre, definovať spôsob utajenia prenosu, spôsob verifikácie odosielateľa a spôsob algoritmického zabezpečenia celistvosti prenášaných dát. Požaduje sa IPSEC protokol medzi

aktívnymi WAN prvkami, v konfigurácií SiteToSite. Pripojenie pre vybraných koncových používateľov do privátnej dátovej siete bude možné aj z Internetu cez IPSEC VPN klienta. Funkcionalita sieťovej bezpečnosti je požadovaná aj s ochranou voči organizovaným útokom typu DDoS. DDoS ochrana je požadovaná na elimináciu nelegitímneho dátového toku, keď je sieťová prevádzka postihnutá útokom typu DDoS a požadované je presmerovať, alebo inak efektívne a s veľkou účinnosťou odfiltrovať útok.

Stanovisko Slovanet:
Zaznamenané a v plnom rozsahu akceptované
Bližšie informácie o navrhovanom riešení sú predložené v nasledujúcich kapitolách.

Služby na úrovni lokálnych sietí

Súčasťou poskytovanej privátnej siete na úrovni lokálnej siete bude prenájom a prevádzka aktívnych prvkov LAN a WiFi infraštruktúry v jednotlivých lokalitách podľa požiadaviek Úradu.

Stanovisko Slovanet:
Zaznamenané a v plnom rozsahu akceptované
Bližšie informácie o navrhovanom riešení sú predložené v nasledujúcich kapitolách.

Služby správy, administrácie, monitoringu a prevádzkovej podpory

Slovanet poskytuje nepretržitý 24 hodinový/365 dňový monitoring privátnej dátovej siete (vrátane koncových zariadení) a služieb s možnosťou okamžitého prehľadu o stave privátnej dátovej siete a služieb poskytovaných privátnou dátovou sieťou. Riešenie poruchových stavov musí byť v súčinnosti so zodpovedajúcimi organizačnými zložkami Úradu, resp. ním poverenej tretej strany. Súčasťou poskytovaných komunikačných služieb musí byť správa a údržba dodaných a prevzatých koncových zariadení.

Súčasťou prevádzkovej podpory privátnej dátovej siete bude aj aktivácia doplnkových služieb a poskytovanie služieb expertnej technickej podpory na vyžiadanie.

Stanovisko Slovanet:
Zaznamenané a v plnom rozsahu akceptované
Bližšie informácie o navrhovanom riešení sú predložené v nasledujúcich kapitolách.

2. Základný popis filozofie navrhovaného technického riešenia

Pre vybudovanie požadovanej VPN bude použitá IP/MPLS sieťová infraštruktúra Slovanetu, ktorá je vybudovaná redundantne a zabezpečene na báze overenej Cisco technológie. Navrhovaná VPN umožňuje vzájomnú elektronickú komunikáciu s ostatnými pracoviskami navzájom a bude zabezpečovať pripojenie na externé siete Internet a GOVNET. Základná sieťová štruktúra je zobrazená na obrázku č. 1.

Bezpečné vysoko dostupné pripojenie všetkých lokalít (koncových bodov) siete VPN je realizované tak, že každá lokalita siete VPN je pripojená do IP/MPLS siete minimálne dvoma fyzicky navzájom nezávislými pripojeniami s výnimkou lokality Typ 5, kde Úrad požadoval iba primárne pripojenie. V prípade požiadavky Úradu je však možno toto pripojenie pre lokality Typu 5 rozšíriť aj o záložné pripojenie, nakoľko navrhovaný hardvér umožňuje realizáciu záložného pripojenia. Navrhované CPE zariadenia a konštrukcia prístupových okruhov umožňujú navýšiť kapacity pripojenia minimálne na požadované kapacity.

2.1 Logické sieťové riešenie, logická schéma VPN siete

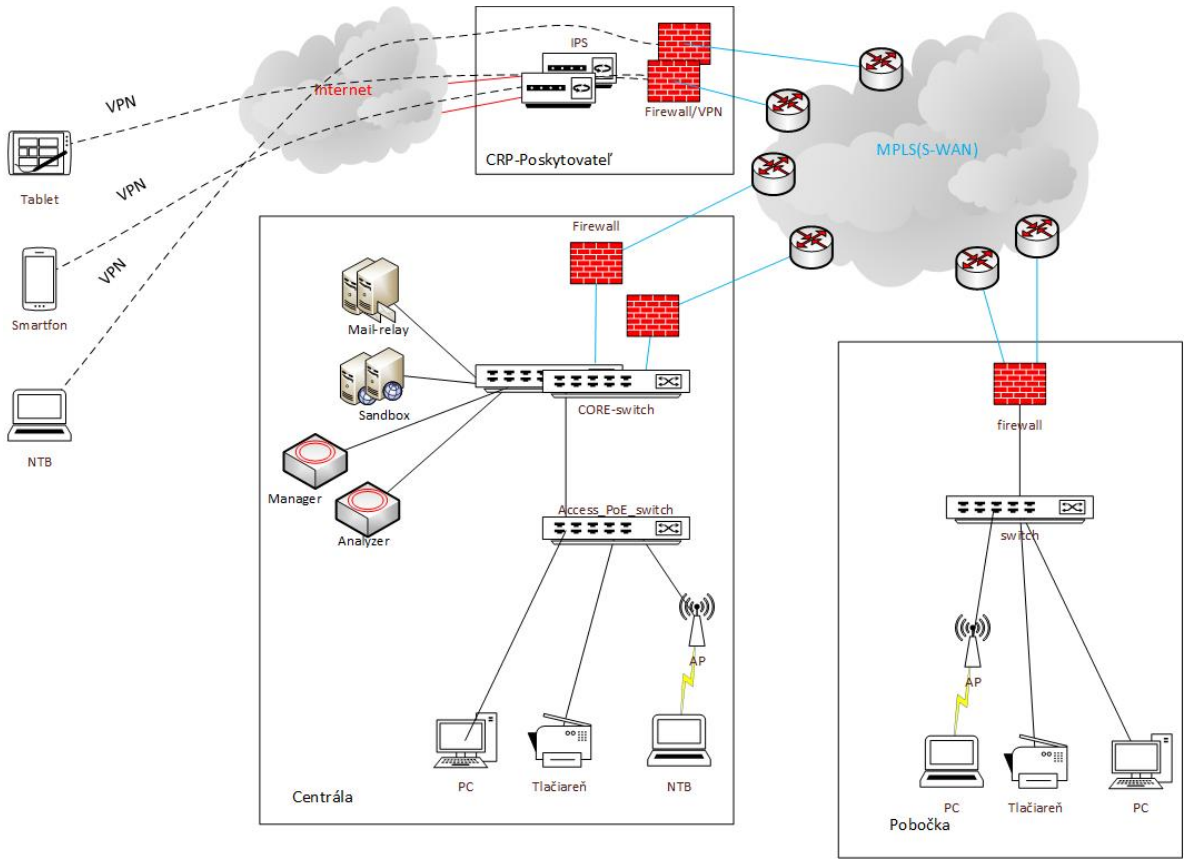
Cieľom navrhovaného riešenia je poskytnúť Úradu virtuálnu privátnu dátovú komunikačnú sieť (VPN) ako centralizované, homogénne sieťové riešenie realizované prostredníctvom IP/MPLS siete.

VPN sieť umožňuje prenos informácií cez sieťovú infraštruktúru poskytovateľa služieb (Slovanetu) spôsobom, ktorý podstatne zvyšuje mieru bezpečnosti a spoľahlivosti prenosu, poskytuje kvalitatívne garancie pomocou definovania kvalitatívnych parametrov QoS. Prostredníctvom adresácie a manažmentu IP/MPLS siete bude vytvorená oddelená privátna sieť, do ktorej bude mať prístup iba definovaná skupina užívateľov. Technológia IP/MPLS umožní uspokojiť odlišné nároky rozličných aplikácií.

Navrhovaná VPN poskytuje zákazníkovi konektivitu všetkých uzlov vytvorenú v topológii full – mesh (komunikácia any-to-any) a vytvára škálovateľné prostredie pre zmeny a rozširovanie VPN siete podľa budúcich požiadaviek.

Transport dát bude zabezpečený v minimálne 2 kvalitatívnych triedach (mission critical data a best effort traffic), typ dát a ich zaradenie do príslušnej triedy bude realizované na základe požiadavky Úradu.

Základná logická topológia VPN je na obrázku č. 1:



Obrázok č. 1: Logická schéma celkovej VPN

2.2 Fyzické sieťové riešenie

VPN bude postavená na moderných, kvalitných a spoľahlivých technológiách renomovaných výrobcov, prípadne na prenajatých dedikovaných kapacitách predných slovenských telekomunikačných operátorov.

Primárne pripojenie jednotlivých koncových bodov bude realizované výhradne jednou z nasledovných technológií:
- ✓ pripojenie prostredníctvom optického prenosového média;
- ✓ pripojenie prostredníctvom metalického prenosového média;
- ✓ rádiové pripojenie v licencovanom pásme.

Prístupová kapacita primárneho pripojenia bude plne symetrická a bude zodpovedať definovaným kapacitným požiadavkám pre daný typ koncového bodu (uvedené v tabuľke č. 1). Navýšenie prístupovej kapacity na minimálnu požadovanú úroveň bude zrealizované bez potreby výmeny prístupovej technológie s minimálnym dopadom na dostupnosť služby.

Záložné pripojenie jednotlivých lokalít bude realizované výhradne jednou z nasledovných technológií:
- ✓ pripojenie prostredníctvom optického prenosového média
- ✓ pripojenie prostredníctvom metalického prenosového média
- ✓ rádiové pripojenie v licencovanom pásme
- ✓ asymetrické pripojenie technológiou xDSL (aplikovateľné len pre Typ 4)
- ✓ bezdrôtové pripojenie technológiou 4G/LTE/5G (aplikovateľné len pre Typ 4).

Prístupová kapacita záložného pripojenia bude plne symetrická (s výnimkou pripojenia xDSL a 4G/LTE/5G) a bude zodpovedať definovaným kapacitným požiadavkám pre daný typ koncového bodu (uvedené v tabuľke č. 1).

Každý použitý typ prístupu poskytuje rýchlosť v požadovanom rozsahu a má vyhradenú kapacitu v sieti Slovanet.

Typ pripojenia	Základná kapacita primárneho pripojenia	Navýšená kapacita primárneho pripojenia	Kapacita záložného pripojenia	Typ SLA
Typ 1	500 Mbit/s	1GBit/s	500 Mbit/s	SLA 1
Typ 2	200 Mbit/s	500 Mbit/s	200 Mbit/s	SLA 1
Typ 3	100 Mbit/s	200 Mbit/s	100 Mbit/s	SLA 2
Typ 4	20 Mbit/s	50 Mbit/s	20 Mbit/s	SLA 2
Typ 5	10 Mbit/s	20 Mbit/s	n/a	SLA 3

Tabuľka č. 1

2.2.1 Prístupová sieť - popis použitých technológii

Optická infraštruktúra
Pri tomto riešení používa Slovanet na prepojenie medzi PE smerovačom a CE smerovačom optickú infraštruktúru, na ktorej bude prevádzkovaný Gigabit Ethernet (ďalej GE) ukončený na CE smerovači.
Uvedené riešenie predstavuje maximálnu možnú rezervu pre požadovanú prenosovú kapacitu a istotu z hľadiska splnenia požiadaviek Úradu na navyšovanie prenosovej kapacity.

Licencované rádio bod – bod
Pre tieto typy riešení používa Slovanet kvalitné a spoľahlivé rádiové systémy pracujúce vo vyhradených frekvenčných pásmach od 7GHz do 38GHz, kde je garantované nerušenie inými systémami. Vo VPN budú použité v konfigurácii, ako rádiový prenosový systém s prenosovou kapacitou až 1 Gbit/s.

Licencované rádio bod – multibod
Pre tieto typy riešení v oblastiach s väčšou hustotou požiadaviek na služby používa Slovanet najmodernejšie FWA rádiové systémy pracujúce v licencovanom pásme 3,5GHz a 10,5 GHz. Uvedené systémy umožňujú dedikovať a garantovať požadovanú prenosovú kapacitu, ktorá je logicky oddelená od ostatnej prevádzky.

Ethernet prepojenie
V objektoch, kde má Slovanet kolokovaný uzol svojej prístupovej siete je pre realizáciu pripojenia CE smerovača do IP/MPLS siete Slovanet využitý lokálny Ethernet metalický alebo optický káblový prepoj.

Digitálne okruhy
Pre pripojenie niektorých pracovísk môžu použité aj digitálne okruhy partnerov Slovanetu. Uvedené riešenie je použité pre vybudovanie nezávislej trasy s použitím nezávislého prenosového média a zvýšenie bezpečnosti prístupu na maximálnu mieru.

2.2.2 IP/MPLS sieť

IP/MPLS sieť Slovanet je postavená výlučne na smerovačoch a prepínačoch firmy Cisco. Hlavná chrbticová sieť Slovanetu je postavená v topológii dvojitého národného ringu medzi krajskými mestami s kapacitou n x 10Gbit, čím je zabezpečená vysoká dostupnosť a flexibilita siete. Okresné mestá tvoria regionálnu úroveň siete Slovanet, uzly regionálnej úrovne sú pripojené do jednotlivých miest v rámci národnej úrovne s kapacitou až n x 1 Gbit/s. Všetky uzly siete Slovanet sú zálohované voči výpadku el. energie samostatnými zdrojmi UPS.

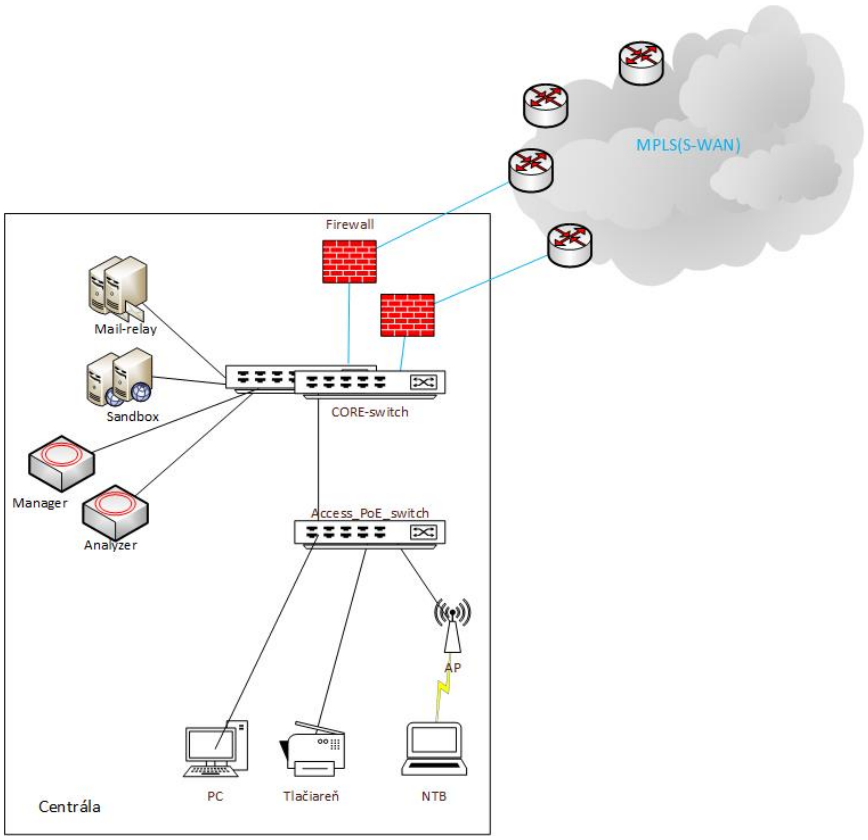
2.2.3 Technické riešenie pre koncový bod Typ 1 (centrála, Bratislava)

Primárne pripojenie koncového bodu Typ 1 na uzol poskytovateľa služby bude realizované cez optickú prístupovú linku. Prístupová kapacita primárneho pripojenia bude symetrická s kapacitou 1Gbit/s.

Sekundárne pripojenie koncového bodu Typ 1 na uzol poskytovateľa služby bude realizované cez nezávislú fyzickú trasu prostredníctvom optickej prístupovej linky, alebo prostredníctvom licencovaného rádia. Prístupová kapacita sekundárneho pripojenia bude symetrická s kapacitou 1Gbit/s.

Primárne aj sekundárne pripojenie koncového bodu Typ 1 bude dostupné súčasne a minimálna prístupová kapacita pripojenia bude 2 x 1Gbit/s. V prípade výpadku jedného z pripojení sa prevádzka automaticky presmeruje na druhé pripojenie.

Základné zapojenie lokality Typ 1 je na obrázku č. 2:



Obrázok č. 2: Schéma zapojenia koncového bodu Typ 1

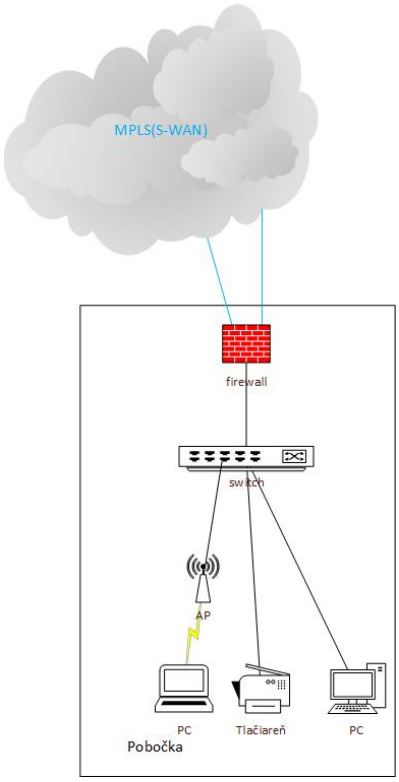
2.2.3 Riešenie pre koncový bod Typ 2, Typ 3, Typ 4 a Typ 5

Primárne pripojenie koncového bodu Typ 2, Typ 3, Typ 4 a Typ 5 na uzol poskytovateľa služby bude realizované jednou z možností definovaných v bode 2.2. Prístupová kapacita primárneho pripojenia bude symetrická a bude spĺňať minimálnu požiadavku na kapacitu linky pre danú lokalitu podľa „Tabuľky č. 1“

Primárne pripojenie umožňuje navýšenie prístupovej kapacity minimálne na hodnotu podľa Tabuľky č. 1 bez potreby zmeny hardvéru, výlučne zmenou konfigurácie prístupovej linky s minimálnym prerušením prevádzky v rámci tolerovanej doby nedostupnosti služby.

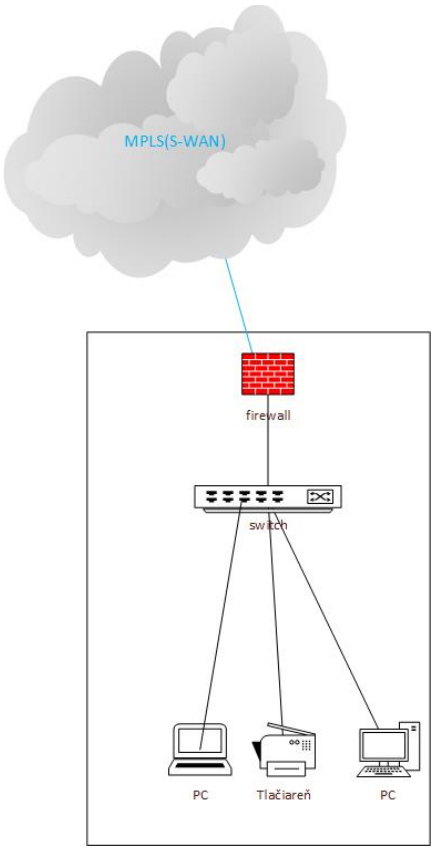
Sekundárne pripojenie koncového bodu Typ 2, Typ 3, Typ 4 na uzol poskytovateľa služby bude realizované cez nezávislú fyzickú trasu jednou z možností definovaných v bode 2.2. Prístupová kapacita sekundárneho pripojenia bude symetrická a bude spĺňať minimálnu požiadavku na kapacitu linky pre danú lokalitu podľa „Tabuľky č. 1“.

Základné pripojenie lokality Typ 2, Typ 3 a Typ 4 je na obrázku č. 3:



Obrázok č. 3: Schéma zapojenia koncového bodu Typ 2, Typ 3 a Typ 4

Základné pripojenie lokality Typ 5 je na obrázku č. 4:



Obrázok č. 4: Schéma zapojenia koncového bodu Typ 5

2.3 Centralizovaný bezpečný prestup do siete Internet

Centralizovaný prestup do siete Internet a smerovanie v privátnej dátovej sieti bude realizovaný v priestoroch dátových centier Poskytovateľa tak, aby bola zabezpečená vysoká dostupnosť služby. Prenosová kapacita bude v súlade s požiadavkami na prenosové kapacity jednotlivých lokalít, prepojených v rámci siete IP MPLS, vrátane požiadaviek na kapacitu pripojenia do siete Internet.

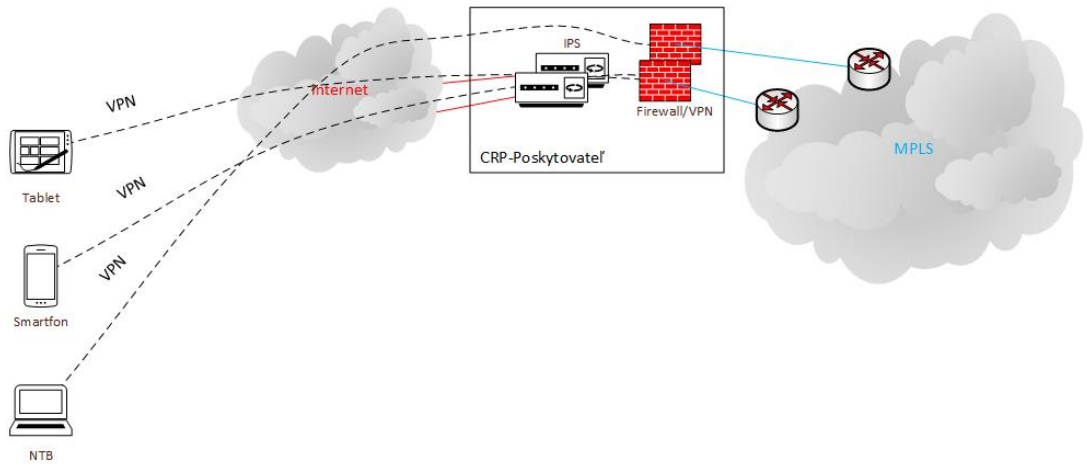
Služba bezpečného prístupu do siete Internet bude ukončená na zariadení typu Next Generation Firewall (NGFW). Pripojený aktívny prvok centralizovaného prístupu Internet bude podporovať protokol BGP a prenosové rýchlosti min. 1Gbps.

Smerovanie prevádzky do siete Internet z privátnej dátovej siete bude realizované prostredníctvom zariadení NGFW s dvoma nezávislými trasami, každá s prenosovou kapacitou 1Gbit/s symetricky.

Štandardná služba centralizovaného Internet pripojenia obsahuje:

- ✓ vysokokapacitné pripojenie a redundantné pripojenie (redundancia je navrhovaná aj pre pripojenie, aj pre aktívne prvky);
- ✓ poskytovanie záložného DNS (menného) servera v redundantnej konfigurácií;
- ✓ službu registrátora doménového mena;
- ✓ službu poskytnutia verejného IP adresného rozsahu (IPV4) v počte 14 pevných verejných IP adries.

Schéma pripojenia do siete Internet je na obrázku č. 5:



Obrázok č. 5 – Schéma pripojenia do siete internet

2.4 Vzdialený VPN prístup do privátnej dátovej siete

Pre vzdialený VPN prístup bude realizovaná technológia, umožňujúca bezpečný vzdialený prístup užívateľov verejného obstarávateľa do jeho privátnej dátovej siete. Služba bude poskytovaná ako bezpečné pripojenie do privátnej dátovej siete pre zamestnanca pracujúceho mimo stáleho pracovisko a/alebo pracovníkov partnerských organizácií s využitím ľubovoľného prístupu do siete Internet. Služba vzdialeného prístupu bude vysoko dostupná, plne manažovaná a zahŕňa vybudovanie a prevádzkovanie zariadenia typu VPN koncentrátor. Redundantný aktívny prvok bezpečného prístupu do VPN bude poskytovať vzdialený šifrovaný

prístup z koncového zariadenia používateľa (PC, notebook) pripojeného v ľubovoľnom bode siete Internet do privátnej dátovej siete verejného obstarávateľa.

Služba vzdialeného VPN prístupu do privátnej dátovej siete bude umožňovať paralelné pripojenie min. 200 užívateľov s možnosťou rozšírenia až na 1000 užívateľov bez potreby výmeny hardvéru.

2.5 Integrácia pripojenia do siete GOVNET

Technický návrh zabezpečuje integráciu služieb existujúceho dátového prepojenia so sieťou GOVNET v súlade s pravidlami stanovenými správcom siete GOVNET. Ide o prevádzkovanie zabezpečeného lokálneho prepojenia služieb privátnej dátovej siete s infraštruktúrou siete GOVNET. Bude zabezpečený samostatný fyzický port na prestupovom aktívnom WAN prvku v danej lokalite. Prístup do siete GOVNET je už v súčasnosti zriadený a poskytovaný.

Budú dodržané všetky podmienky pripojenia v zmysle prevádzkových predpisov NASES.

Miestom pripojenia do siete GOVNET je centrála privátnej dátovej siete (Tomášikova 14366/64A, 831 04 Bratislava).

3. Bezpečnostné služby

3.1 Šifrovaná komunikácia medzi uzlami privátnej dátovej siete

Privátna dátová sieť poskytne bezpečnú komunikáciu. Pripojenie bude šifrované a prostredníctvom šifrovacích protokolov sa budú selektívne definovať bezpečnostné parametre, definovať spôsob utajenia prenosu, spôsob verifikácie odosielateľa a spôsob algoritmického zabezpečenia celistvosti prenášaných dát. Ďalej sa budú selektívne definovať bezpečnostné parametre v súlade s aktuálnou bezpečnostnou politikou a príslušnej legislatívy, najmä v zmysle Zákona o Kybernetickej bezpečnosti a príslušných vyhlášok.
Navrhovaný je IPSEC protokol medzi aktívnymi WAN prvkami, v konfigurácií SiteToSite. Pripojenie pre vybraných koncových užívateľov do VPN bude možné aj z Internetu cez VPN klienta.

3.2 Next generation firewall (NGFW)

Technický návrh zahŕňa nasadenia a správu technológie Next Generation Firewall (NGFW) za účelom granulárneho riadenia dátovej komunikácie medzi privátnou dátovou sieťou verejného obstarávateľa, sieťou Internet a sieťami externých dodávateľov a partnerov verejného obstarávateľa. Účelom nasadenia technológie Next Generation Firewall je dosiahnutie najvyššieho možného stupňa ochrany vonkajšieho perimetra siete verejného obstarávateľa a ochranu jeho privátnych sietí pred neoprávneným prístupom. Služba bude plne manažovaná Poskytovateľom a prevádzkovaná v dátovom centre Poskytovateľa v režime vysokej dostupnosti.

Služba Next Generation Firewall bude umožňovať nasledovné funkcionality:

Schopnosť rozpoznania aplikácií – podporovať schopnosť rozpoznať a následne umožniť, zakázať alebo požadovaným spôsobom limitovať dátovú komunikáciu, prináležiacu konkrétnej aplikácii a bez ohľadu na použitý komunikačný protokol a port, cez ktorý aplikácia komunikuje;
Schopnosť rozpoznania identity užívateľov – podporovať schopnosť rozpoznania identity užívateľov za účelom granulárnej kontroly prístupu ku konkrétnym aplikáciám na základe

užívateľa, skupiny užívateľov resp. zariadení, z ktorých je realizovaný prístup k systémom verejného obstarávateľa;
Centralizovaný manažment, administrácia, logovania a reporting – podporovať možnosť centralizovaného manažmentu prostredníctvom web rozhrania;
Stavová inšpekcia paketov - podporovať možnosť stavovej inšpekcie dát v reálnom čase min. v rozsahu 2-7 vrstvy OSI modelu;
Hĺbková inšpekcia paketov (Deep packet inspection - DPI) – podporovať možnosť hĺbkovej inšpekcie za účelom identifikovania a následného blokovania prípadných chýb, anomálií a známych typov útokov v dátovej komunikácii;
Ochrana proti prieniku (Intrusion Detection/Prevention System - IDS/IPS) – podporovať integrovanú ochranu proti prieniku do siete verejného obstarávateľa s možnosťou automatického zablokovania alebo notifikácie o prebiehajúcej neželanej resp. abnormálnej dátovej komunikácii;
Možnosť inšpekcie šifrovanej komunikácie – podporovať možnosť nahliadať do obojsmerne prebiehajúcej šifrovanej dátovej komunikácie min. pre protokol SSL;
Možnosť integrácie s inými bezpečnostnými riešeniami – podporovať možnosť integrácie min. so systémom SIEM, bezpečnostným reportingovým nástrojom a službou viacfaktorovej autentifikácie;
Vstavaná antivírová a antibot ochrana – podporovať zabudovaný mechanizmus ochrany proti vírusom a botom so schopnosťou identifikácie infikovaných súborov min. pre protokoly HTTP, HTTPS, FTP, POP3, SMTP a SMB;

Minimálne navrhované výkonové parametre pre službu Next Generation Firewall:
Redundancia – plná redundancia zariadení;
Priepustnosť firewallu – priepustnosť 1,6 Gb/s v prípade IPv4/IPv6 UDP paketov s veľkosťou 1518 bitov;
Priepustnosť IPSec VPN – priepustnosť 1 Gb/s pri paketoch s veľkosťou 512 bitov pri použití šifrovania AES256-SHA256;
Priepustnosť SSL inšpekcie – priepustnosť 1 Gb/s pre HTTPS spojenia;
Priepustnosť SSL VPN – priepustnosť 1 Gb/s (pri TLS v1.2 s AES256-SHA šifrovaní vrátane podpory TLS v1.3)

3.3 Data Loss Prevention (DLP) - systém na prevenciu pred únikom citlivých dát

Technický návrh zahŕňa nasadenie a správu technológie Data Loss Prevention (DLP) - systému na zabránenie únikom citlivých dát z interného prostredia verejného obstarávateľa pre 2000 počet koncových bodov. Pre Verejného obstarávateľa bude zabezpečený prístup ku manažment konzole DLP systému za účelom vytvárania, modifikácie a rušenia bezpečnostných politík, získania prehľadu o incidentoch a celkovom stave systému v reálnom čase a za účelom reportingu. V prípade potreby bude k dispozícii možnosť prevzatia manažmentu celého riešenia do svojej vlastnej správy.

Služba Data Loss Prevention (DLP) podporuje nasledovné funkcionality:
Bezpečnostný audit dát – podporovať auditovanie historických dát, vrátane dát z externých zariadení, webových uploadov, emailov, instant messagingu, tlače a cloudových úložísk;
Podpora auditovania pre Office 365 – podporovať auditovanie operácii so súbormi a odchádzajúcich emailov prostredníctvom služby MS Office 365;
Podpora bezpečnostných noriem a regulácií – podpora pre bezpečnostné normy a regulácie, min. v rozsahu GDPR;
Klasifikácia inšpektovaného obsahu – klasifikovať senzitívne súbory a emaily pomocou preddefinovaných vzorov a pravidiel;
Detekcia podozrivých aktivít – detekcia a notifikácia podozrivých aktivít v reálnom čase;
Ochrana siete a emailov – podporovať ochranu pre emaily, webové uploady, instant messaging a zdieľané sieťové disky;

Ochrana zariadení a tlače – podporovať ochranu dát ukladaných na externé úložné zariadenia a taktiež ochranu pred neželaným vytlačením dát na tlačiarňach všetkých typov;
Ochrana vzdialeného prístupu – schopnosť zabrániť únikom dát cez vzdialený prístup k pracovnej ploche;
Pokročilá klasifikácia dát – detegovať a označovať senzitívne dáta na základe pôvodu alebo typu súboru prostredníctvom uložených metadát;
Vytváranie kópií podozrivých dát – schopnosť vytvárať šifrované kópie podozrivých dát z incidentov za účelom forenznej analýzy;
Správa riešenia – podporovať správu prostredníctvom web rozhrania v plnom rozsahu;
Kontrola pracovnej plochy – podporovať ochranu pracovnej plochy s možnosťou zabrániť únikom dát vytváraním kópií obrazovky;
Podpora pre BitLocker – podporovať šifrovanie BitLocker;
Ochrana synchronizácie dát na cloudové úložiská – podporovať ochranu dát, ktoré sú synchronizované na externé cloudové úložiská typu OneDrive, GoogleDrive, DropBox a pod.;
Ochrana pre Office 365 – podporovať ochranu proti neželanému zdieľaniu dokumentov Office 365 a SharePoint prostredníctvom cloudovej služby;
Podpora pre integráciu s doménou – podporovať integráciu s Active Directory;
Integrácia s NGFW – podporovať integráciu s ponúkaným Next Generation Firewallom za účelom automatizácie vybraných operácií.

3.4 Vzdialený VPN prístup používateľov

Technický návrh zahŕňa nasadenie a správu technológie, umožňujúcej bezpečný vzdialený prístup používateľov verejného obstarávateľa do jeho privátnej siete.

Služba vzdialeného VPN prístupu podporuje nasledovné funkcionality:

Bezpečnosť – podporovať vzdialený prístup pomocou protokolov min. IPSec VPN / L2TP VPN;
Viacfaktorová autentifikácia – okrem štandardného prihlasovania prostredníctvom prihlasovacieho mena a hesla musí podporovať aj viacfaktorovú autentifikáciu prostredníctvom softvérového tokenu, generujúceho jednorazové číselne kódy, dostupného pre všetky bežne používané OS a mobilné platformy;
Správa VPN používateľov – umožňovať správu VPN používateľov (min. v rozsahu vytvárania, rušenia a dočasného zablokovania účtu, priradenia tokenu používateľovi, možnosti definovania pravidiel a politík, vymedzujúcich prístup vzdialených používateľov na konkrétne zariadenie resp. služby vo vnútornej sieti verejného obstarávateľa) prostredníctvom web rozhrania;
Overovanie používateľov – podporovať overovanie používateľov prostredníctvom samostatného autentizačného servera, bezpečne oddeleného od vnútornej infraštruktúry verejného obstarávateľa aj od Internetu;
Autorizácia používateľov – podporovať možnosť autorizácie vzdialených používateľov s funkcionalitou reportingu o udalostiach, týkajúcich sa prihlasovania sa používateľov do VPN a využívania vzdialeného pripojenia;
Logovanie prístupov – podporovať centralizované logovanie vzdialených VPN prístupov používateľov za účelom zisťovania problémov a bezpečnostných incidentov;
Kompatibilita – VPN klient musí byť dostupný pre všetky bežne používané OS a mobilné platformy.

4. Služby na úrovni lokálnych sietí

4.1 LAN prepínače

Technický návrh zahŕňa nasadenie a správu technológie typu LAN prepínač umožňujúcej pripojenie koncových zariadení typu PC/NTB, VoP SIP telefón, WiFi AP prípadne iných typov

s využitím funkcionality napájania týchto koncových zariadení prostredníctvom PoE, resp. PoE+.

V závislosti od komunikačných potrieb sú navrhované nasledovné typy LAN prepínačov:
Typ A: 8-portové aktívne prvky (prepínače): min. 8 down-link portov 10/100/1000 RJ45
Typ B: 24-portové aktívne prvky (prepínače): min. 24 down-link portov 10/100/1000 RJ45
Typ C: 48-portové aktívne prvky (prepínače): min. 48 down-link portov 10/100/1000 RJ45
Typ D: 24-portové aktívne prvky (prepínače): min. 24 down-link portov SFP+ (10G) – non-PoE

Up-link porty:
Typ A: min. 2 SFP porty/sloty 1Gbps použiteľné ako pre optickú tak aj pre metalickú kabeláž
Typ B: min. 2 SFP+ porty/sloty 10Gbps použiteľné ako pre optickú tak aj pre metalickú kabeláž
Typ C: min. 4 SFP+ porty/sloty 10Gbps použiteľné ako pre optickú tak aj pre metalickú kabeláž
Typ D: min. 4 SFP+ porty/sloty 10Gbps pre optickú kabeláž

L2 funkcionalita:
- podpora IEEE 802.3x Flow Control,
- podpora jumbo (min. 9000B) rámcov,
- podpora monitorovania a záznamu o dátových tokoch v hardvéri,
- podpora IEEE 802.3ad (LACP),
- podpora IEEE 802.3az (Energy Efficient Ethernet),
- podpora IEEE 802.1q, hlasových aj dynamických VLAN,
- podpora IEEE 802.1d (Spanning Tree Protocol),
- podpora IEEE 802.1s MST,
- podpora IEEE 802.1w RSTP,
- podpora IEEE 802.1ab LLDP,
- ochrana STP Protokolu pred zmenou koreňového prepínača, filtrovanie BPDU,
- ochrana pri vzniku jednosmerných liniek,
- podpora lokálneho aj vzdialeného zrkadlenia dátových tokov.

Bezpečnosť:
- riadenie bezpečnostných funkcií pomocou IPv4 aj IPv6 prístupových filtrov,
- podpora IPv6 first hop security - min. funkcia RA guard, DHCPv6 guard, IPv6 Source Guard,
- podpora RADIUS CoA,
- podpora Dynamic ARP Inspection, DHCP Snooping, IP Source Guard,
- podpora IEEE 802.1x s dynamickým priradením VLAN, Podpora IEEE 802.1x s dynamickým priradením ACL,
- podpora IEEE 802.1x s MAB,
- podpora IEEE 802.1x pre dátovú aj hlasovú VLAN súčasne na jednom fyzickom porte,
- podpora webovej autentifikácie pre non-802.1x klientov,
- podpora IEEE 802.1x Guest VLAN, Auth-fail VLAN, Auth-bypass VLAN,
- podpora Wake-on-LAN spolu s 802.1x,
- ochrana riadiacej jednotky pred DoS útokmi,
- podpora IEEE 802.1ae macsec 128 (neplatí pre 8 port. zariadenie).

Manažment zariadení:
- samostatný konzolový port a/alebo samostatný 10/100 Ethernet network manažment port,
- podpora SSHv2, HTTPS,
- podpora SNMPv3 (s autentifikáciou a šifrovaním).

Riadenie kvality služieb QoS:
- riadenie kvality poskytovaných služieb (QoS) pre prenos dát hlasu a videa, prioritný queueing, traffic shaping, traffic policing, DSCP remarking,
- klasifikácia / Marking / Policing / Queueing,
- klasifikácia podľa 802.1p CoS / ToS / DSCP / MAC / L3 ACL / L4 ACL.

4.2 WiFi AP a WiFi kontrolér

Technický návrh zahŕňa nasadenie a správu technológie typu WiFi access point (WiFi AP) v spojení so zariadeniami typu WiFi kontrolér (centrálny riadiaci prvok) na riadenie bezdrôtových prístupových sietí.

Na WiFi kontrolér budú definované všetky sieťové a bezpečnostné parametre. Systém bude mať funcionalitu „captive portal“ resp. „hot spot“ s automatickým odpájaním užívateľov. Tento riadiaci prvok bude mať minimálne 2Gpbs priepustnosť, podporu pre pripojenie až do 256 WiFi AP.

Funkcionality WiFi kontroléra:
Podpora RF manažment signálu s aktívnou identifikáciou a zmierňovaním rušenia signálu.
Podpora bezdrôtových štandardov: IEEE 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11k, 802.11n, 802.11r, 802.11v, 802.11w, 802.11ac, 802.1Q, 802.1X.
Podpora bezpečnostných štandardov: WPA2™ AES, WPA3™ AES s 802.1x alebo preshared key, Web Captive Portal, MAC blocklist & allowlist: EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST.

Funkcionality WiFi AP:
- dual-band802.11a/g/n/ac/ax
- podpora 802.11ac Wave 2
- certifikácia Wifi Alliance Wifi6 a WPA3
- inteligentné riadenie prevádzkového režimu 2.4GHz, 5GHz, 6GHz,
- podpora 802.3at PoE,
- podpora multigigabit-ethernet 2.5Gbps IEEE802.3bz
- min. počet LAN portov 1x 10/100/1000Base-T
- analýza 7 aplikačnej vrstvy s možnosťou prioritizácie a blokovania jednotlivých aplikácií
- podpora asistovaného roamingu 802.11k, 802.11r, 802.11v

4.3 Záložný zdroj napájania UPS

Technický návrh zahŕňa nasadenie a správu technológie typu UPS slúžiaceho pre zálohovanie napájania koncových zariadení typu smerovač, LAN prepínač a WiFi AP.

V závislosti od komunikačných potrieb a potrieb na distribuovanú alokáciu prvkov LAN siete sú navrhované nasledovné typy UPS zariadení:
Typ A: záložné napájanie koncového bodu privátnej komunikačnej siete Typ 1 (WAN smerovač, 4 x LAN prepínač Typ C, 4 x WiFi AP) minimálne pod dobu 60 minút;
Typ B: záložné napájanie koncového bodu privátnej komunikačnej siete Typ 2 a Typ 3 (WAN smerovač, 1 x LAN prepínač Typ C, 2 x WiFi AP) minimálne pod dobu 60 minút;
Typ C: záložné napájanie koncového bodu privátnej komunikačnej siete Typ 4 (WAN smerovač, 1 x LAN prepínač Typ B, 1 x WiFi AP) minimálne pod dobu 60 minút;
Typ D: záložné napájanie distribuovaného uzla LAN siete (1 x LAN prepínač Typ C, 2 x WiFi AP) minimálne pod dobu 30 minút;

4.4 Technologický stojan (rack)

Technický návrh zahŕňa nasadenie a správu technológie typu technologický stojan (rack) slúžiaceho pre umiestnenie a primárne napájanie koncových zariadení typu smerovač, LAN prepínač a UPS.

Aktívne prvky budú umiestnené do racku (oceľový rám so štandardným 19‘‘ uchytením), ktorý bude obsahovať centrálnu napájaciu lištu, z ktorej budú primárne napájané aktívne zariadenia. Rack bude uzatvorený a uzamykateľný.

V závislosti od komunikačných potrieb a potrieb na distribuovanú alokáciu prvkov LAN siete sú navrhované nasledovné typy technologických stojanov:
Typ A: min. 42 U
Typ B: min. 20 U

5. Služby správy, administrácie, monitoringu a prevádzkovej podpory

5.1 Služby správy, administrácie, monitoringu

Technický návrh zahŕňa nepretržitý 24 hodinový/365 dňový monitoring privátnej dátovej siete (vrátane koncových zariadení) a služieb s možnosťou okamžitého prehľadu o stave privátnej dátovej siete a služieb poskytovaných privátnou dátovou sieťou. Poskytovateľ služby zabezpečuje správu a administráciu privátnej dátovej siete a zároveň všetkých aktívnych koncových zariadení, ktoré sú poskytované ako súčasť služby (smerovače, LAN prepínače, WiFi AP a kontroler, UPS).

Služba centralizovaného monitoringu bude vysoko dostupná a bude spĺňať nasledovné funkcionality:
Alerting – podpora automatického vyhodnocovania chybových stavov a následná možnosť alertingu, hlásenia incidentov a prevádzkových problémov;
Reporting – podpora automatického reportingu aktuálnych dát v reálnom čase a tiež historických dát s min. granularitou deň/týždeň/mesiac/rok;
Prístup – pre technický personál verejného obstarávateľa bude zabezpečený prístupu k dashboardu monitorovacieho nástroja min. v móde read only, t.j. na sledovanie štatistík systému v reálnom čase a archívnych dát bez možnosti zmeny konfigurácie systému;
Informácia o plnení SLA – monitorovací nástroj bude mať možnosť automaticky vyhodnocovať nastavené parametre SLA a následne spracovať report o plnení SLA parametrov.

5.2 Služby prevádzkovej podpory

Technický návrh zahŕňa poskytnutie služby nepretržitej prevádzkovej podpory a odstraňovania prípadných poruchových stavov. Poskytovateľ disponuje centrom prevádzkovej a technickej podpory s nepretržitým režimom 24 hodín/365 dní. Toto kontaktné miesto môže používateľ použiť v prípade akýchkoľvek problémov alebo otázok súvisiacich s poskytovanou službou v prípade poruchy.

Pre potreby klarifikácie technických otázok súvisiacich s poskytovaním služby a pri riešení minoritných nezávažných porúch neohrozujúcich garantované SLA Poskytovateľ disponuje centrom podpory „HELP DESK“ počas pracovnej doby verejného obstarávateľa v režime min. 8 hodín / 5 pracovných dní.

Súčasťou prevádzkovej podpory privátnej dátovej siete aj aktivácia doplnkových služieb uvedených nižšie a poskytovanie služieb expertnej technickej podpory pri rozšírení a/alebo zmene konfigurácie privátnej dátovej siete na vyžiadanie verejným obstarávateľom.

6. Doplnkové služby

Verejný obstarávateľ môže požadovať poskytovanie doplnkových služieb, ktoré by boli poskytované ako rozšírenie existujúcich základných služieb privátnej dátovej siete o nové funkcionality, resp. by boli poskytované formou expertnej technickej podpory. Poskytovateľ poskytuje nasledujúci rozsah doplnkových služieb:

- ✓ Zriadenie novej alebo presťahovanie existujúcej lokality Typ 2, Typ 3, alebo Typ 4;
- ✓ Navýšenie kapacity pripojenia pre primárny prístup pre lokalitu Typ 1
- ✓ Navýšenia kapacity pripojenia pre záložný prístup pre lokalitu Typ 1
- ✓ Navýšenie kapacity pripojenia pre primárny prístup pre lokality Typ 2 až Typ 5;
- ✓ Zriadenie a prevádzkovanie nového zariadenia LAN prepínač a jeho začlenenie do existujúcej siete;
- ✓ Zriadenie a prevádzkovanie nového WiFi AP a jeho začlenenie do existujúcej siete pod príslušný WiFi kontrolér;
- ✓ Poskytovanie služieb expertnej technickej podpory.

7. Prevádzkovanie siete a poskytovanie služby VPN

7.1 Prevádzkovanie siete

Prevádzkovanie siete Slovanet, a.s. je realizované prostredníctvom Centra monitorovania siete a technických tímov, ktoré sú alokované v nasledujúcich mestách: Bratislava, Trenčín, Žilina, Zlaté Moravce, Banská Bystrica, Poprad a Košice.

Centrum monitorovania siete 24 hodín denne zabezpečuje dohľad nad všetkými zariadeniami a prenosovými časťami. Kontrolné mechanizmy siete dokážu do určitej miery samostatne rozpoznávať poruchy a netypické situácie a následne informovať technickú podporu signálom o stupni závažnosti podľa typu poruchy. V prípade potreby okamžitého zásahu je o probléme informovaný odborný technický tím, ktorý je pripravený okamžite vzniknutú situáciu riešiť.
Duálny princíp technickej podpory zaručuje, že nikdy nenastane situácia, aby nebol o každom zákazníkovi informovaný aspoň jeden pracovník, ktorý je členom aktuálneho technického tímu.

Náplňou práce technických tímov je preventívna údržba siete, administrácia a konfigurácia siete, výstavba sieťovej infraštruktúry, inštalácia a konfigurácia sieťových prvkov v zákazníckych priestoroch, inštalácia a konfigurácia koncových telekomunikačných zariadení, odstraňovanie poruchových stavov v sieti a na zákazníckych sieťových uzloch, odstraňovanie porúch koncových telekomunikačných zariadení. Alokácia tímov na celom území Slovenska umožňuje rýchly prístup na miesto poruchy a znižuje tak čas potrebný na odstránenie poruchy.

Prípadné poruchy súvisiace s prevádzkou VPN, oznamuje poverený pracovník zákazníka telefonicky alebo písomne (e-mailom alebo faxom) na kontakty:

Centrum monitorovania siete a služba hotline Slovanet
tel. číslo: 02 / 208 28 120,
fax. číslo: 02 / 208 28 222,
e-mail adresa: nmc@slovanet.net.

Ohlásenie poruchy musí obsahovať opis poruchy, čas vzniku a identifikáciu volajúceho s kontaktnými údajmi pre informácie o riešení poruchy.

7.2 Poskytovanie služby VPN

Poskytovanie služby VPN je spojené s administráciou siete Slovanet, a administráciou sieťových prvkov umiestnených v priestoroch zákazníka.

V terminológii virtuálnych privátnych sietí realizovaných cez IP/MPLS sieť delíme zariadenia podľa ich umiestnenia a vykonávanej funkcie.

Zákaznícke komunikačné zariadenia komunikujúce protokolom IP a podieľajúce sa na WAN sieti vytvorenej ako IP/MPLS VPN, umiestnené v priestoroch zákazníka (Customer Premises), nazývame hraničné smerovače a budeme ich označovať CE (Customer Edge).
IP smerovače poskytovateľa služby, ktoré vykonávajú IP/MPLS značkovanie a prepínanie a zároveň slúžia na pripájanie zákazníckych smerovačov CE, s ktorými sú spojené na IP vrstve, nazývame PE (Provider Edge).

IP smerovače poskytovateľa služby, ktoré vykonávajú IP/MPLS značkovanie, prepínanie a neslúžia na pripájanie zákazníkov a tvoria chrbticovú sieť IP/MPLS, nazývame P (Provider Router).

Medzi CE smerovačom a PE smerovačom je nakonfigurovaný protokol BGPv4, prostredníctvom ktorého prebieha výmena zákazníckych smerovacích informácií v sieti IP/MPLS VPN.
CE smerovače vykonávajú:

- ✓ triedenie paketov do jednotlivých kvalitatívnych tried,
- ✓ selektívne šifrovanie,
- ✓ IP smerovanie do siete IP/MPLS VPN.

Triedenie paketov na CE je nevyhnutné pri paketoch, ktoré sú následne šifrované protokolom IPSec, nakoľko po zašifrovaní už nie je možné určiť príslušnosť jednotlivých paketov k aplikáciám. Triedenie paketov do jednotlivých tried komunikačných profilov prebieha na PE smerovačoch, ktoré sa podieľajú aj na výmene smerovacích informácií v rámci siete IP/MPLS VPN protokolom MP-IBGP. Výmena IP smerovacích tabuliek medzi PE a P smerovačmi je IGP protokolom IS-IS s TLV rozšíreniami. Distribúcia značiek vo vnútri siete Slovanet medzi PE a P smerovačmi je protokolmi LDP a RSVP-TE v závislosti na platforme susediacich smerovačov (LSR).

NGFW na jednotlivých lokalitách Úradu sú pripojené do IP/MPLS siete Poskytovateľa prístupovými linkami. Na sieťovej úrovni komunikujú s PE smerovačmi protokolom IP.

IP adresy v celej IP/MPLS VPN sieti sú z privátneho IP adresného priestoru, podľa odporúčania RFC 1918 a tento priestor nekoliduje s inými IP/MPLS VPN sieťami Poskytovateľa.

Záložné spojenia sa budú aktivovať automaticky mechanizmom tzv. „floating static“. Ethernetové rozhranie voči LAN sieti jednotlivých lokalít Úradu bude nakonfigurované ako „access interface“, pričom na základe upresnenej požiadavky je možné implementovať/nakonfigurovať aj rýchlostné limity na jednotlivé služby a ACL.

Prípadné zmeny SW konfigurácie súvisiace s prevádzkou VPN, oznamuje poverený pracovník zákazníka písomne (e-mailom alebo faxom) na adrese: techsupport@slovanet.net.

Ohlásenie žiadosti o zmenu SW konfigurácie musí obsahovať lokalitu, opis zmeny a identifikáciu žiadateľa s kontaktnými údajmi pre informáciu o riešení zmeny konfigurácie.

7.3 Monitorovanie siete VPN

Monitorovacie funkcie pre sieť VPN budú realizované prostredníctvom Monitoring servera, na ktorom budú nainštalované príslušné monitorovacie nástroje. Monitoring server bude umiestený v uzle Poskytovateľa. Uvedený server bude v správe Slovanet, a.s. s autorizovaným prístupom príslušných zložiek Úradu.

Pre účely požadovanej správy siete VPN zabezpečovanej Slovanetom bude zriadené pripojenie Centra technickej podpory Slovanetu k Monitoring serveru v lokalite zákazníka. Uvedené pripojenie bude realizované vytvorením samostatnej VLAN pre monitoring (VLAN monitoring). Bezpečné pripojenie k LAN sieti Úradu a vytvorenie DMZ na strane Úradu zabezpečí implementácia Firewall-u.
Popísaný spôsob monitorovania siete VPN umožní Slovanetu bezpečným spôsobom splniť požiadavky Úradu na správu, reporting a monitorovanie siete VPN .

7.4 Monitorovacie nástroje použité pre monitorovanie siete VPN

Pre spracovanie získaných monitoringových dát zo siete VPN budú použité nasledujúce monitorovacie aplikácie:

- ✓ Nagios
- ✓ Cacti
- ✓ Smokeping
- ✓ SPECTRUM (u poskytovateľa)

Monitorovací nástroj Nagios

Nagios slúži pre monitorovanie počítačových sietí a systémov, kontroluje tzv. hosts (zariadenia – servery, routre a pod.) a services (služby na daných zariadeniach, ako ping, telnet, ssh a pod.), ktoré sú špecifikované používateľom. Pri zmene stavu monitorovaného zariadenia alebo služby, systém umožňuje notifikovať o tejto zmene.

Základné možností systému Nagios sú:

- ✓ Monitorovanie sieťových služieb (SMTP, POP3, HTTP, NNTP, PING atď.)
- ✓ Monitorovanie systémových zdrojov (záťaž procesora, počet prihlásených používateľov)
- ✓ Jednoduchý design plugin-ov umožňujúci vytváranie vlastných service checks
- ✓ Paralelné spúšťanie kontrol
- ✓ Možnosť implementácie hierarchie siete pomocou definovania parent host – rodičovského zariadenia, čím sa dajú určiť a rozlíšiť zariadenia ktoré sú down alebo unreachable
- ✓ Notifikácia definovaného kontaktu (napr. správca Mail serveru) pre zariadenie alebo službu pri zmene ich stavu (e-mailom, sms-kou, pagerom, alebo používateľom definovaným spôsobom)
- ✓ Možnosť definovať event handlers , čo môžu byť napr. skripty, ktoré sú spúšťané v nejakom stave zariadenia alebo služby pre aktívne riešenie problému.
- ✓ Automatická rotácia log súborov
- ✓ Podpora redundantného monitoringu
- ✓ Upraviteľné web rozhranie – prezentačná vrstva

Viac informácií o systéme Nagios je možné nájsť na http://www.nagios.org .

Monitorovací nástroj Cacti

Cacti je úplný frontend k RRDTool nástroju, ktorý ukladá všetky potrebné informácie pre vytváranie grafov a napĺňa ich údajmi v MySQL databáze. Cacti je celé naprogramované v

PHP, okrem možnosti spravovania grafov, zdrojov dát a Round Robin archívov umožňuje zbieranie dát samozrejme s SNMP podporou.

Zbieranie dát môže byť realizované aj prostredníctvom externých skriptov a tak je možné naplniť akékoľvek dáta do Cacti následne do MySQL/RRD.

Akonáhle sú zadefinované zdroje dát, RRDTool vytvorí grafy. Cacti umožňuje vytváranie komplexných grafov použitím štandardných RRDTool typov grafov a konsolidačných funkcií. Cacti umožňuje nielen vytvárať ale aj mnohými spôsobmi zobrazovať a prezentovať vytvorené grafy. Okrem pohľadov typu „listview“ a „preview“ umožňuje aj zobrazenie v stromovej štruktúre.

Užívateľská administrácia, ktorú poskytuje Cacti, umožňuje pridávať používateľov a prideľovať im práva na prezeranie a editovanie určených častí Cacti.

Cacti je škálovateľné pre použitie s veľkým počtom zdrojov dát a grafov, použitím šablón.

Monitorovací nástroj Smokeping

SmokePing je nástroj na meranie latencie a stratovosti v sieti. Umožňuje merať, zaznamenávať, zobrazovať latenciu a stratovosť v časovom rade. Smokeping používa RRDTool nástroj pre ukladanie dlhodobých výsledkov meraní a tiež pre vykresľovanie grafov v časovom rozlíšení až do 1 minúty.

Smokeping používa systém externých pluginov pre ľahkú rozšíriteľnosť.

Smokeping používa smart alarm systém, na rozdiel od jednoduchých alarmov definovaných medznými hodnotami, smokeping umožňuje definovania vzorov latencie a stratovosti a ich zasielanie na email.

Skriptovacie nástroje slúžia na zálohovanie konfigurácií aktívnych prvkov zákazníka. Konfigurácie sú automaticky zálohované po každej zmene, alebo na pokyn administrátora, čo umožňuje mať aktuálny stav v ľubovoľnom čase a v prípade havárie je možné tieto nahradiť v pôvodnom stave.

Monitorovací nástroj SPECTRUM

Systém SPECTRUM Network Fault Manager spoločnosti Computer Associates zabezpečuje monitorovanie a manažment udalostí, chybových stavov, dostupnosti, využitia a výkonu sledovaných zariadení, sieťových prvkov a definovaných funkcií. Je to hlavný nástroj monitorovania telekomunikačnej infraštruktúry spoločnosti a jej zákazníkov.

Implementovaním vybranej sady nástrojov:

- ✓ Data Manager with Report Gateway Toolkit;
- ✓ MPLS VPN Manager;
- ✓ QoS Manager;
- ✓ Report Manager;
- ✓ Service Manager;
- ✓ Service Performance Manager;

zo širokého portfólia SPECTRUM nástrojov, umožňuje operátorom siete podstatne zrýchliť nájdenie príčin porúch, úplnej alebo čiastočnej nefunkčnosti alebo zmene sledovaných parametrov a okamžite iniciovať ich odstránenie. Tieto činnosti podporujú integrované unikátne vlastnosti SPECTRA, ako hľadanie prvotnej príčiny pri komplexnejších poruchách (Root Cause Management), vzťahy medzi udalosťami a stavmi (Event Correlation).

Zároveň umožňuje nastaviť a plne automatizovať report manažment.

Popis výmeny informácií pri riešení poruchových stavov a požiadaviek na zmenu konfigurácie VPN siete:

Súčasťou dohľadového centra je Helpdesk, ktorý prijíma reklamácie a požiadavky zákazníkov a zabezpečuje ich riešenie. Prípadné poruchy súvisiace s prevádzkou služby, oznamuje poverený pracovník zákazníka telefonicky alebo písomne (e-mailom alebo faxom) na adrese:

Centrum monitorovania siete a služba hotline
tel. číslo: 02 / 208 28 120
fax. číslo: 02/208 28 627,
e-mail adresa: operator@slovanet.net.

Ohlásenie poruchy musí obsahovať opis poruchy, čas vzniku a identifikáciu volajúceho s kontaktnými údajmi pre informácie o riešení poruchy.

Po obdržaní požiadavky na odstránenie poruchy pracovník dohľadového centra zrealizuje základné zisťovania stavu siete a služby. V prípade potreby spätne kontaktuje zákazníka s požiadavkou na ďalšie doplňujúce údaje potrebné pre klarifikáciu príčiny vzniku poruchy. Po identifikácií príčiny poruchového stavu zabezpečí v spolupráci s údržbovými zložkami najskôr jej odstránenie na diaľku. V prípade, že je možné poruchu odstrániť na diaľku bez potreby súčinnosti zákazníka je porucha odstránená a zákazník je informovaný o jej odstránení a požiadaný o preverenie a potvrdenie funkčnosti služby. V prípade, že je pri odstraňovaní poruchy na diaľku potrebná súčinnosť zákazníka, pracovník dohľadového centra kontaktuje kontaktnú osobu zákazníka s požiadavkou na poskytnutie súčinnosti a dohodnú ďalší postup pri odstraňovaní poruchy. Obdobne po odstránení poruchy je zákazník informovaný o jej odstránení a požiadaný o preverenie a potvrdenie funkčnosti služby. V prípade, že je pri odstránení poruchy nutný výjazd na lokalitu zákazníka, tak pracovník dohľadového centra dohodne s kontaktnou osobou zákazníka súčinnosť požadovanú od zákazníka a kontakt na zodpovednú osobu zákazníka v dotknutej lokalite, kde bude realizovaný údržbový zásah. Následne údržbový pracovník Slovanet už napriamo komunikuje s určenou osobou od zákazníka a dohodne si poskytnutie potrebnej súčinnosti a prístupu na miesto realizácie údržbového zásahu. Po odstránení poruchy je zákazník informovaný o jej odstránení a požiadaný o preverenie a potvrdenie funkčnosti služby.

Po obdržaní požiadavky na zmenu konfigurácie siete pracovník dohľadového centra v spolupráci s príslušným obchodníkom prideleným k zákazníkovi overí, či bola požiadavka na zmenu konfigurácie vystavená autorizovanou osobou zákazníka, a či je v zmluve nastavené oprávnenie na požadovaný rozsah konfiguračnej zmeny. V prípade vystavenia požiadavky neautorizovanou osobou je zákazník (autorizovaná kontaktná osoba) kontaktovaný s požiadavkou na autorizované potvrdenie objednávky na zmenu konfigurácie. Po overení autorizovanosti požiadavky je spustený proces realizácie zmenovej požiadavky. V prípade potreby pracovník Slovanetu zodpovedný za zmenu konfiguračného nastavenia spätne kontaktuje zákazníka s požiadavkou na ďalšie doplňujúce údaje potrebné pre klarifikáciu nastavenia nových parametrov služby. V prípade, že je možné zmenu konfigurácie realizovať na diaľku bez potreby súčinnosti zákazníka je konfigurácia zrealizovaná v dohodnutý termín a zákazník je informovaný o jej realizovaní a požiadaný o preverenie a potvrdenie funkčnosti zmenenej služby. V prípade, že je pri zmene konfigurácie na diaľku potrebná súčinnosť zákazníka, pracovník zodpovedný za konfiguráciu kontaktuje kontaktnú osobu zákazníka s požiadavkou na poskytnutie súčinnosti a dohodnú ďalší postup pri zmene konfigurácie. Obdobne je po zrealizovaní zmeny konfigurácie zákazník informovaný o jej realizovaní a požiadaný o preverenie a potvrdenie funkčnosti novej služby. V prípade, že je pri konfiguračnej zmene nutný výjazd na lokalitu zákazníka, tak pracovník zodpovedný za konfiguráciu dohodne s kontaktnou osobou zákazníka súčinnosť požadovanú od zákazníka

a kontakt na zodpovednú osobu zákazníka v dotknutej lokalite, kde bude realizovaný konfiguračný zásah. Následne pracovník Slovanet už napriamo komunikuje s určenou osobou od zákazníka a dohodne si poskytnutie potrebnej súčinnosti a prístupu na miesto realizácie konfiguračného zásahu. Po zrealizovaní konfiguračnej zmeny je zákazník informovaný o jej odstránení a požiadaný o preverenie a potvrdenie funkčnosti novej služby.

8 Bezpečnosť riešenia VPN

8.1 Koncepcia bezpečnosti a bezpečnostné štandardy

Slovanet pri dizajne a prevádzkovaní siete uplatňuje princípy manažovanej bezpečnosti, ktoré sú definované štandardom ISO/IEC 17799:2005 „Information Technology - Code of practise for Information Security Management“.

Vo svojej bezpečnostnej politike sa Slovanet zameriava na bezpečnosť informácií prenášaných komunikačnou sieťou, ktoré definuje ako zachovanie:

a) **dôvernosti** – zaistenie toho, aby informácia bola dostupná iba osobám s oprávneným prístupom;
b) **integrity** – zabezpečenie správnosti a kompletnosti informácií plus metódy jej spracovania;
c) **dostupnosti** – zaistenie toho, aby informácie a s nimi zviazané aktivity boli prístupné autorizovaným užívateľom podľa ich potreby.

Súčasťou návrhu dizajnu siete, resp. zákazníkovej informačnej a komunikačnej infraštruktúry je dôkladné zváženie potenciálnych hrozieb, analýza a vyhodnotenie bezpečnostných rizík z nich vyplývajúcich, definovanie opatrení na elimináciu rizík a ich následná realizácia.
Implementované bezpečnostné koncepty a modely sú v súlade so štandardom ISO/IEC TR 13335-1 „Information technology – Guidelines for the management of IT security, Part 1: Concepts and models for IT security“.

Riadenie a plánovanie bezpečnosti komunikačnej a informačnej infraštruktúry vychádza zo štandardu ISO/IEC TR 13335-2 „Information technology – Guidelines for the management of IT security, Part 2: Managing and planning IT security“.

Použité bezpečnostné techniky sú odvodené od princípov definovaných v štandarde ISO/IEC TR 13335-3 „Information technology – Guidelines for the management of IT security, Part 3: Techniques for the management of IT security“.

8.2 Zabezpečenie fyzickej bezpečnosti a bezpečnosti prostredia

Všetky uzly v sieti Slovanet sú umiestnené v zabezpečených uzamknutých zónach s kontrolou a evidenciou prístupu, pričom prístup k predmetnej sieťovej infraštruktúre majú len určení vyškolení pracovníci.

Sieťová infraštruktúra je inštalovaná v klimatizovaných priestoroch s ochranou voči prieniku prachu a drobných nečistôt, so zálohou voči výpadku elektrickej energie samostatnými zdrojmi UPS. Uzly v Bratislave majú napájanie zálohované vlastným dieselagregátom. Uzly mimo územia Bratislavy majú pre svoju potrebu pripravené pohotovostné dieselagregáty, ktoré sa nachádzajú v lokálnych skladoch v pobočkách Slovanetu. V prenajatých priestoroch je táto záloha plne realizovaná prenajímateľom.

Sieťová kabeláž je chránená proti poškodeniu, resp. neoprávnenému prístupu inštaláciou do chráničiek uložených v zemi, alebo v prípade vnútorných rozvodov v zabudovaných

kolektoroch. Metalické káblové rozvody sú proti zásahu bleskom chránené prepäťovou ochranou a zemnením.

8.3 Sieťová bezpečnosť na 1. a 2. vrstve

Slovanet, a.s. pri návrhu a implementácií zákazníckych VPN sietí využíva vysokú bezpečnostnú úroveň všetkých sieťových komponentov na 1. a 2. vrstve OSI modelu, ktorá je dosiahnutá fyzickým a logickým oddelením prevádzky s použitím transportu:

- ✓ na dedikovaných optických vláknach,
- ✓ na prenajatých metalických okruhoch,
- ✓ cez licencované rádiové spoje,
- ✓ cez metalické DSL prístupy,
- ✓ cez separátne ethernet VLAN,
- ✓ cez separátne dedikované digitálne okruhy na SDH platforme.

Tento princíp umožňuje vytvoriť vyhradené sieťové zdroje a transportné kapacity, ktoré sú určené iba na komunikáciu predmetnej VPN a zároveň svojou podstatou eliminuje riziko chybnej konfigurácie v sieti, nakoľko konfigurácia VPN je takto vztiahnutá na vyhradené fyzické porty a všetka logická prevádzka pretekajúca cez príslušný port je súčasťou iba jedinej VPN siete.

Z hľadiska bezpečnosti voči výpadku je prevádzka VPN siete na transportnej úrovni naviac chránená mechanizmami rýchleho prepnutia (do 50 ms) na záložný smer (SDH, Ethernet over SDH, Ethernet over fiber, WDM).

8.4 Sieťová bezpečnosť na 3. vrstve

Komunikácia medzi CE a PE smerovačmi je proti nežiadúcemu prístupu zabezpečená primárne na nižších úrovniach siete vyhradeným použitím prístupových technológií, pričom prevádzka z CE smerovača je smerovaná cez vyhradený port na PE smerovači. Bezpečnosť vnútri kostrovej IP/MPLS siete je daná vytvorením separátneho adresného priestoru pre VPN a zároveň oddeleným smerovaním a priradením špecifického „návestia“, ktoré nie je dostupné, a preto ani čitateľné mimo Slovanet IP/MPLS siete.

Rozsah a typ informácii prenášaných medzi jednotlivými pobočkami VPN je možné presne zadefinovať v sieti IP/MPLS prostredníctvom implementácie prístupových filtrov (Access list), ktoré znemožňujú neautorizovaný prístup zo špecifických adries, resp. skupín adries.

Internetová prevádzka je v IP/MPLS sieti je striktne oddelená od prevádzky VPN sietí. Internetová prevádzka je konfigurovaná a agregovaná v separátnej bezpečnostnej zóne, pre ktorú sú vyhradené separátne prístupové a agregačné zariadenia. Internetová prevádzka je smerovaná mimo adresného priestoru VPN klientskych sietí.

8.5 Bezpečnosť prístupu ku zdrojom siete VPN

Bezpečný administrátorský prístup na smerovače je možný len z dedikovaného servera, v bezpečnostnej zóne v sieti vyhradenej pre manažment a administráciu, logicky a vo veľkej miere aj fyzicky oddelenej od produkčnej siete. Prístup administrátora vyžaduje identifikáciu a autentizáciu na AAA serveri, pričom činnosť administrátora je zaznamenávaná zápismi o vykonaných aktivitách (accounting). Týmto je zabezpečené opatrenie voči neautorizovanej konfigurácií VPN, resp. je evidovaná prípadná nesprávna konfigurácia a na základe vyhodnotenia zápisov o činnosti administrátora je možné chybnú konfiguráciu identifikovať a napraviť. Slovanet používa AAA server Takacs+. Aby sa zabránilo prípadnej mimovoľnej

chybnej konfigurácií sú používané konfiguračné postupy a automatizované nástroje, ktoré zabezpečujú:

- ✓ Integritu prideľovania adresných priestorov, ktoré eliminujú konfiguráciu VPN, ktorej adresný rozsah sa prekrýva s adresným rozsahom inej VPN;
- ✓ Správnosť a kompletnosť smerovania, kde každá zákaznícka VPN má pridelené svoje unikátne návestie;
- ✓ Zaznamenávanie činnosti administrátorov;
- ✓ Zaznamenávanie histórie zmien v sieti (procesný systém Slovanet, a.s. zabezpečuje, že každá zmena konfigurácie je ukladaná na centrálny server s priebežným zálohovaním dát, resp. záloha konfiguračného nastavenia sa sťahuje pravidelne s periódov 1 týždeň, čo eliminuje riziká nesprávnej konfigurácie po prípadnom výpadku).

Zamedzenie prípadným DoS útokom na VPN zákazníka je realizované procesom korektnej konfigurácie, filtrácie smerovania a detekcie neštandardných stavov v sieti.

8.6 Špecifické aspekty riešenia bezpečnosti VPN

Bezpečný prístup na koncové zariadenia VPN

Bezpečný prístup na NGFW v sieti VPN je realizovaný cez demilitarizovanú zónu (DMZ), ktorá je logicky a fyzicky oddelená od produkčnej prevádzky prostredníctvom separátnej VLAN pre administráciu, ktorá je do VPN siete pripojená cez dva nezávislé ethernetové porty na dvoch centrálnych smerovačoch pracujúcich v „hot stand-by“ režime, čím je eliminované možné ohrozenie straty dostupnosti. Prístup administrátora vyžaduje identifikáciu a autentizáciu na AAA serveri, pričom činnosť administrátora je zaznamenávaná zápismi o vykonaných aktivitách (accounting). Autentizácia je navrhovaná ako dvojúrovňová: 1. úroveň = prihlásenie sa do DMZ zóny; 2. úroveň = oprávnenie vykonať konfiguračný zásah.

Bezpečné oddelenie VPN a ochrana prenášaných údajov

VPN je navrhnutá na samostatnej infraštruktúre 1. a 2. vrstvy modelu OSI, kde je prepojenie centrály realizované prostredníctvom dvoch nezávislých prístupových technológií cez dva CE smerovače pracujúce v „hot stand-by“ režime. Primárne prepojenie pobočiek v krajských mestách je navrhované cez dedikovanú transportnú SDH sieť. Záložné prepojenie krajských pobočiek a primárne pripojenie okresných pobočiek je navrhnuté cez logicky oddelenú časť IP/MPLS siete určenú jedinečným návestím cez separátne porty na PE smerovačoch. Záložné pripojenie pobočiek v okresných mestách je navrhnuté cez DSL sieť. Na prenos dát z DSL prístupov je v sieti zmluvného partnera používaná IP/MPLS sieť, z ktorej dáta do IP/MPLS siete Slovanet prestupujú na úrovni L2.

Uvedené opatrenia minimalizujú a prakticky eliminujú vplyv nesprávnej konfigurácie, ktorá sa takto stáva veľmi transparentnou a prehľadnou. Procesné postupy a využitie konfiguračných nástrojov Cisco platformy (ako napr. IP Solution Center) garantujú maximálnu ochranu prenášaných údajov. Tým, že je VPN navrhovaná ako fyzicky a logicky oddelená od ostatnej časti siete sa v maximálnej miere eliminuje riziko neautorizovanej činnosti, ktorá by prichádzala z vonkajšieho prostredia. Riziko neautorizovanej činnosti zvnútra VPN siete je eliminované dvojúrovňovou autentizáciou a logickým oddelením produkčnej a manažmentovej siete.

9 Služba VPN a ochrana prevádzky VPN siete na úrovni IP/MPLS

Služba VPN zahrňuje pripojenie pracovísk Úradu prostredníctvom hraničných NGFW umiestnených v priestoroch zákazníka a vyhradenou alokáciou sieťových zdrojov IP MPLS siete. Navrhovaná VPN poskytuje zákazníkovi konektivitu všetkých uzlov vytvorenú v topológii full – mesh (komunikácia any-to-any) a vytvára škálovateľné prostredie pre zmeny a rozširovanie VPN siete podľa budúcich požiadaviek.

VPN sieť je spôsob prenosu informácie cez sieťovú infraštruktúru poskytovateľa služieb (Slovanetu) s plne transparentnou architektúrou bez vplyvu na protokoly vyšších vrstiev, ktorá podstatne zvyšuje mieru bezpečnosti a spoľahlivosti prenosu, poskytuje kvalitatívne garancie pomocou definovania kvalitatívnych parametrov QoS (QoS - oneskorenie a garancia pásma).

Pridelením MPLS značky (MPLS label) pre VPN sieť je možné vytvoriť oddelenú bezpečnú privátnu sieť v rámci IP/MPLS siete Slovanet, do ktorej bude mať prístup iba definovaná skupina užívateľov.

Pripojenie každého NGFW umiestneného v zákazníckej lokalite ku PE smerovaču siete IP/MPLS je zabezpečené prostredníctvom samostatnej garantovanej prístupovej linky s rozhraním FE/GE. NGFW na jednotlivých lokalitách Úradu sú pripojené do IP/MPLS siete.

Medzi NGFW a PE smerovačom je nakonfigurovaný protokol BGPv4, prostredníctvom ktorého prebieha výmena zákazníckych smerovacích informácií v sieti IP/MPLS VPN.
CE smerovače vykonávajú:

- ✓ triedenie paketov do jednotlivých kvalitatívnych tried,
- ✓ selektívne šifrovanie,
- ✓ IP smerovanie do siete IP/MPLS VPN.

Slovanet prevádzkuje IP MPLS sieť na smerovačoch a prepínačoch firmy Cisco Systems. Kostrové MPLS smerovače (P) a prístupové MPLS smerovače (PE), kde sa pripájajú zákazníci, sú smerovače firmy Cisco Systems Service Provider series.

Sieť Slovanet podporuje aj „dial up“ spôsoby prístupu do VPN, a to tak z fixnej siete, ako aj z mobilných sietí, prostredníctvom prístupových brán, ktoré sú oddelené od ostatnej časti siete v špeciálnej bezpečnej DMZ zóne.

10. Garancia kvality poskytovaných služieb (SLA)

Garantovaná kvalita poskytovaných služieb (ďalej tiež „SLA“, t.j. Service Level Agreement) je definovaná skupinou merateľných hodnôt, ktoré majú podstatný vplyv na prevádzku a kvalitu poskytovaných verejných telekomunikačných služieb. Tieto hodnoty vyjadrujú minimálnu úroveň, ktorú sa Poskytovateľ zaväzuje verejnému obstarávateľovi poskytnúť ako záruku za dodržanie medzných hodnôt dohodnutej skupiny parametrov. Zárukou je dohodnutá finančná náhrada, na ktorú má užívateľ nárok v prípade, že medzné parametre služby nie sú v danom období dodržané.

Prípojný bod služby (ďalej tiež „PBS“) je fyzické rozhranie charakterizované funkčnými, mechanickými, elektrickými a protokolovými vlastnosťami, ktoré umožňuje pripojenie koncového zariadenia verejného obstarávateľa.

Porucha je taký stav, ktorý znemožňuje riadne používanie služby v dohodnutom rozsahu a kvalite. Za poruchu sa nepovažuje dočasné prerušenie poskytovania služby počas plánovanej

a odsúhlasenej údržby. Akákoľvek údržba, ktorá nebola naplánovaná a odsúhlasená verejným obstarávateľom a ktorá spôsobí nedostupnosť služby, bude považovaná za poruchu. Pokiaľ porucha presahuje z jedného do nasledujúceho kalendárneho mesiaca, považuje sa iba za jednu poruchu a započítava sa do kalendárneho mesiaca, v ktorom vznikla.

Doba opravy (TTR) - je garantovaná doba opravy poruchy vyjadrená v minútach alebo hodinách a počíta sa ako doba medzi nahlásením poruchy (telefonicky, e-mailom, prostredníctvom Helpdesku poskytovateľa) účastníkom operátorovi servisného strediska a okamihom obnovenia prevádzky, potvrdeným účastníkom.

Dostupnosť služby (ďalej tiež „SA“, t.j. Service Availability) je garantovaná dostupnosť služby vyjadrená ako podiel času, počas ktorého môže verejný obstarávateľ používať službu v dohodnutom rozsahu a kvalite, k dĺžke celého sledovaného obdobia. Sledované obdobie je kalendárny mesiac (vyjadrený v minútach) a výsledná hodnota dostupnosti služby sa vyjadruje v percentách so zaokrúhlením na dve desatinné miesta smerom nahor.

SA bude počítaná podľa nasledovného vzorca:

$$SA\ [\%] = \frac{(\Sigma \text{ minút/mesiac} -- \Sigma \text{ minút nedostupnosti/mesiac})}{\Sigma \text{ minút/mesiac}} \times 100\%$$

Doba nedostupnosti služby (vyjadrená v minútach) je doba, počas ktorej nemohla byť služba používaná v dohodnutej kvalite.

Dĺžka sledovaného obdobia: 1 mesiac.

Počet dní v mesiaci	Počet minút v mesiaci
28	40320
29	41760
30	43200
31	44640

Kategórie SLA a garantované parametre:

Pre poskytovanie služieb privátnej dátovej siete sú definované nasledovné kategórie SLA a k nim prislúchajúce garantované parametre:

Kategória SLA	Dostupnosť služby SA (v %)	Doba opravy TTR (v hod.)
SLA 1	99,9 %	Do 4 hodín
SLA 2	99,5 %	Do 8 hodín
SLA 3	99,0 %	Do 8 hodín NBD

Poznámka: NBD (Next Business day) znamená nasledujúci pracovný deň.

11. Certifikácia odbornej spôsobilosti z pohľadu bezpečnosti

Riešenie Slovanet, a.s. pre VPN bolo z pohľadu bezpečnosti auditované a schválené nezávislou certifikovanou autoritou s CISA certifikátom.

Prehlásenie CISA audítora a jeho CISA certifikát sú priložené ako samostatné dokumenty do ponuky.

12. Návrh časového realizačného harmonogramu

Slovanet pristupuje k realizácii siete a služieb pre významných klientov formou projektového manažmentu, kde špeciálne vyčleňuje svoje zdroje, ktoré sú alokované výhradne pre realizáciu projektu. Projektový manažér organizuje všetky technické aktivity súvisiace s realizáciu a dohladuje jej hladký priebeh v súlade s časovým realizačným harmonogramom. Je hlavnou kontaktnou osobou voči klientovi pre potrebu súčinnosti klienta pri realizácii diela.

Časový realizačný harmonogram je odvodený od termínu podpisu zmluvy a trvanie jednotlivých aktivít je definované v kalendárnych dňoch.

Začiatok realizácie je termín nadobudnutia platnosti zmluvy a ukončenie realizácie je definované termínom pripravenosti na poskytovanie služby.

Termín spustenia služieb je maximálne do 60 dní od nadobudnutia účinnosti zmluvy za podmienky dodržania základných ustanovení pre súčinnosť špecifikovaných v rámcovej dohode. Maximálna garantovaná doba implementácie služieb ukončená míľnikom pripravenosti na akceptáciu (RfA) je v súlade s návrhom na plnenie kritérií stanovená na 56 kalendárnych dní.

Časový realizačný harmonogram je vo forme grafu predložený ako samostatný dokument ponuky

13. Zaškolenie administrátorov

Definovaní administrátori Úrad budú zaškolení do jednotlivých častí riešenie, aby mohli:

- ✓ Kontrolovať aktuálne nastavenia služby (read-only prístup)
- ✓ V prípade vybraných častí (definovať používateľov vzdialeného VPN prístupu, manažment konzola DLP, úprava „captive portalu“ wifi siete) meniť nastavenia (read-write prístup)
- ✓ Pristupovať na monitorovacie nástroje
- ✓ Pristupovať na vyhodnocovacie a reportingové nástroje

Zaškolenie bude pre maximálny počet 10 osôb v rozsahu 8 hodín v jednom dni, alebo môžu byť rozdelené na 2x 4hod.

Náklady na zaškolenie sú súčasťou ceny za zriadenie privátnej dátovej siete.

14. Produktové listy navrhovaných CPE zariadení

Produktové listy navrhovaných CPE zariadení využitých v navrhovanom riešení sú predložené ako samostatné dokumenty do ponuky.