NAFTA a.s., Votrubova 1, 821 09 Bratislava

Súťažné podklady

Názov súťaže (ďalej len „súťaž“):

„Duálne pripojenie do internetu – perimeter“

OBSAH

A. POKYNY PRE NAVRHOVATEĽOV

A.1 VŠEOBECNÉ POKYNY

A.1.1 Identifikácia vyhlasovateľa súťaže:

Názov organizácie:	NAFTA a.s.
IČO:	36 286 192
IČ DPH:	SK2022146599
Sídlo spoločnosti:	Votrubova 1, 821 09 Bratislava
Zapísaná:	Obchodný register Okresného súdu Bratislava1, oddelenie Sa, vložka číslo 4837/B
Krajina:	Slovenská republika

	Obchodné záležitosti	Technické záležitosti
Kontaktná osoba:	Ing. Mária Hudecová	Ing. Anton Piovarči
Telefón:	+421 2 4024 2579	+421 2 4024 2552
Fax:	+421 2 4024 2516	
E-mail:	VK-14002-dual.pripojenie@nafta.sk	
v kópii:	maria.hudecova@nafta.sk	anton.piovarci@nafta.sk
Internetová stránka:	www.nafta.sk	

A.1.2 Predmet súťaže:

Predmetom súťaže je dodanie služby:

„Duálne pripojenie do internetu – perimeter“ podľa realizačného projektu vypracovaného spoločnosťou NAFTA a.s., uvedeného v **Prílohe č. 1**

A.1.3 Typ zmluvného vzťahu

Zmluva o Dielo resp. Objednávka v zmysle návrhu vyhlasovateľ.

A.1.4 Miesto a termín dodania

Miestom dodania: NAFTA a.s
- lokalita Michalovce
- Centrálny areál PZZP (ďalej „CA“)
- Bratislava / Lozorno – výber podľa dostupnosti internetového pripojenia

Predpokladaný termín dodania: **október / november 2014.**

A.1.5 Hodnotenie návrhov

Hodnotiť sa budú iba návrhy navrhovateľov predložené spôsobom a v termíne v zmysle vyhlásenia súťaže.

Vyhlasovateľ si vyhradzuje právo po predložení návrhov obmedziť počet navrhovateľov a takto určených navrhovateľov vyzvať na individuálne rokovania o podmienkach zmluvy.

Vyhlasovateľ si vyhradzuje právo rokovať s navrhovateľom o návrhu v niekoľkých po sebe nasledujúcich etapách s možnosťou vyzvať navrhovateľov na predloženie aktualizovanej cenovej ponuky po každej etape rokovaní.

A.1.6 Vysvetľovanie a dorozumievanie

Akékoľvek dorozumievanie a poskytovanie informácií medzi vyhlasovateľom a navrhovateľmi sa bude uskutočňovať elektronicky. Adresa pre elektronickú komunikáciu je uvedená v bode A.1.1.

A.2 POKYNY PRE VYPRACOVANIE NÁVRHU

A.2.1 Obsah návrhu

Predložený návrh musí obsahovať doklady v tomto poradí:

1. Názov a presnú adresu navrhovateľa, IČO a kontaktné údaje štatutárneho orgánu navrhovateľa v súlade s výpisom Obchodného registra, resp. osoby oprávnenej konať v mene navrhovateľa v záväzkových vzťahoch pre ďalšie rokovanie o zmluvných podmienkach.
2. Krycí list (**Príloha č.3)** s prehlásením súhrnnej maximálnej ceny, s uvedením termínov realizácie a záručnej lehoty.
3. Vyhlásenie navrhovateľa, že súhlasí s podmienkami súťaže určenými vyhlasovateľom, podpísané štatutárnym orgánom navrhovateľa, resp. osobou oprávnenou konať v mene navrhovateľa.
4. Vyhlásenie navrhovateľa o pravdivosti a úplnosti všetkých dokladov, dokumentov a údajov uvedených v návrhu, podpísané štatutárnym orgánom navrhovateľa, resp. osobou oprávnenou konať v mene navrhovateľa.
5. Garancie ekonomickej a technickej spôsobilosti k predmetu súťaže.
6. Referencie na rovnaký alebo podobný predmet súťaže, uskutočnené za posledné 3 roky, ktoré realizoval navrhovateľ ako dodávateľ.
7. Navrhovateľom parafované Všeobecné obchodné podmienky (www.nafta.sk), ktoré sú neoddeliteľnou súčasťou súťažných podkladov, na znak súhlasu.

A.2.2 Vyhotovenie návrhu

Navrhovateľ môže predložiť len jeden návrh na celý predmet súťaže resp. jeho ucelenú časť.

Návrh musí byť vyhotovený v slovenskom, resp. českom jazyku.

Návrh musí byť čitateľný, vyhotovený v písomne a to písacím strojom, tlačiarňou počítača, perom s nezmazateľným atramentom a pod.

Návrh musí byť podpísaný štatutárnym orgánom navrhovateľa v súlade s výpisom Obchodného registra, resp. osobou oprávnenou k tomuto úkonu. Originál dokumentu preukazujúci oprávnenie osoby podpísať návrh musí byť v takomto prípade súčasťou návrhu.

A.2.3 Platnosť návrhu

Platnosť návrhu musí byť minimálne do **28.02.2015**.

A.2.4 Variantné riešenie

Neumožňuje sa predloženie variantného riešenia.

A.3 PREDKLADANIE NÁVRHOV

A.3.1 Označenie obalov s návrhmi

Navrhovatelia predkladajú návrhy v elektronickej podobe na e-mailu adresu: VK-14002-dual.pripojenie@nafta.sk v kópii maria.hudecova@nafta.sk . Ponuka musí byť zreteľne

označená názvom súťaže **„VK14002_Duálne pripojenie“** s uvedením sídla navrhovateľa (odosielateľa).

A.3.2 Miesto a termín predkladania návrhov

Otázky k súťažným podmienkam je potrebné doručiť na adresu v zmysle bodu A.3.1 **do 11.9.2014 do 10:00h.**

Návrhy je potrebné doručiť na adresu v zmysle bodu A.3.1 **do 17.9.2014 do 10:00h.**

B. PODMIENKY ÚČASTI

B.1 EKONOMICKÁ A FINANČNÁ SPÔSOBILOSŤ

Ekonomickú a finančnú spôsobilosť preukazuje navrhovateľ predložením nasledovných podkladov a uvedením nasledovných informácií:

1. Doklad o oprávnení podnikať pre predmetný rozsah prác nie starší než 3 mesiace ku dňu predkladania cenového návrhu.
2. Prehlásenie o obrate navrhovateľa za posledné 3 roky v oblasti zhodnej alebo podobnej ako je predmet súťaže.
3. Vyhlásenie štatutárneho zástupcu navrhovateľa, že na majetok navrhovateľa nebol ku dňu vyhlásenia súťaže vyhlásený konkurz, nie je v likvidácii a nemá v evidencii daňové nedoplatky.

B.2 TECHNICKÁ SPÔSOBILOSŤ

Technickú spôsobilosť preukazuje navrhovateľ predložením nasledovných podkladov a uvedením nasledovných informácií:

1. Počet zamestnancov navrhovateľa, profesijnú štruktúru zamestnancov s uvedením prípadných lokalít resp. pobočiek .
2. Čestné prehlásenie, že navrhovateľ má k dispozícii strojové a technické vybavenie potrebné na plnenie predmetu súťaže.

C. OPIS PREDMETU SÚŤAŽE

Predmet súťaže je bližšie špecifikovaný **Prílohe č. 1,** ktorá tvorí neoddeliteľnú súčasť týchto súťažných podkladov.

D. NÁVRH CENY, FAKTURÁCIA, ZÁRUKA

D.1 SPÔSOB URČENIA CENY

1. Cena za predmet súťaže musí byť stanovená v zmysle zákona NR SR č.18/1996 Z. z. o cenách v znení neskorších predpisov.
2. Navrhovateľom uvádzané ceny budú v EUR.
3. Navrhovateľ navrhne cenu predmetu súťaže v tomto zložení:
    a) navrhovaná zmluvná cena bez DPH,
    b) sadzba DPH a výška DPH
    c) navrhovaná zmluvná cena vrátane DPH.
4. Ak navrhovateľ nie je platcom DPH, uvedie navrhovanú zmluvnú cenu celkom. Na skutočnosť, že nie je platiteľom DPH, upozorní (uvedie ju) v návrhu.

5. Cena za predmet súťaže je maximálna pre zadefinovaný predmet súťaže s pevnými a nemennými jednotkovými cenami.
6. Ceny navrhované navrhovateľom musia vyjadrovať cenovú úroveň v čase, v ktorom bol podaný návrh vyhlasovateľovi súťaže.
7. Do Ceny musí navrhovateľ zahrnúť všetky a akékoľvek náklady, ktoré mu vzniknú v súvislosti s dodaním predmetu súťaže, vrátane **6 mesačnej podpory** po prevzatí Diela. (napr. cenu za HW a SW, licencie, inštaláciu, konfiguráciu, zaškolenie, projekt vyhotovenia, dokumentáciu, dopravu a to v plnom rozsahu požadovaných funkcionalít a pri zabezpečení súčasnej funkčnosti)

   Od post implementačnej podpory očakávame spoluprácu pri „dolaďovaní" systému tak, aby boli realizované všetky funkčnosti, ktoré máme v súčasnosti implementované.

   V prípade kritických funkčnosti budeme požadovať odozvu rádovo v hodinách. V ostatných prípadoch podľa dohody. Detaily budú predmetom rokovania z víťazným uchádzačom..
8. Cena uvedená v návrhu kryje všetky náklady spojené s predmetom súťaže musí obsahovať celkovú cenu za predmet súťaže, vrátane nákladov pre splnenie predmetu súťaže a všetkých ostatných nákladov navrhovateľa.
9. Cena musí zohľadňovať i náklady navrhovateľa na zaškolenie zamestnancov vyhlasovateľa (minimálne dvoch) v súvislosti so základnou obsluhou, údržbou, bezpečnosťou pri obsluhe, prevádzkovým nastavením a pod.
10. Cena musí zahŕňať náklady na projekt vyhotovenia.
11. Komisia na vyhodnotenie návrhov môže požiadať navrhovateľa o objasnenie a zdôvodnenie primeranosti navrhnutej ceny.

D.2 FAKTURÁCIA

Vyhlasovateľ neposkytuje preddavky.

Práce budú vyfakturované na základe faktúry, podľa skutočne vykonaných a odsúhlasených prác vo forme zisťovacieho protokolu a na základe podpísaného odovzdávacieho protokolu po ukončení všetkých prác a skúšok a po odovzdaní kompletnej dokumentácie.

Splatnosť faktúry **60 dní od doručenia** je podrobne popísaná v Prílohe č. 2.

Fakturácia:

90% z Ceny za Dielo na základe preberacieho protokolu po zhotovení Diela

10% z Ceny za Dielo na základe preberacieho protokolu po postimplementačnej podpore.

D.3 ZÁRUKA

Záručná doba na dielo sa stanovuje na **4 rokov** odo dňa prevzatia diela vyhlasovateľom.

Podrobná špecifikácia záručných podmienok a spôsob vybavovania reklamácií budú predmetom zmluvy.

E. DOPLŇUJÚCE PODMIENKY A USTANOVENIA

1. Súťažné podklady poskytuje vyhlasovateľ bezplatne, zostávajú však majetkom vyhlasovateľa.
2. Vyhlasovateľ si vyhradzuje právo meniť podmienky súťaže, prípadne súťaž kedykoľvek zrušiť. O týchto skutočnostiach bude navrhovateľov informovať.
3. Navrhovateľ nemá nárok na náhradu nákladov spojených s účasťou v súťaži.
4. V rámci vyhodnotenia návrhov si vyhlasovateľ vyhradzuje právo požiadať navrhovateľov o vysvetlenie návrhu, resp. overiť si niektoré údaje a skutočnosti uvedené v návrhu.
5. Uzavretím súťaže a oznámením výsledku súťaže nevzniká zmluvný vzťah.
6. Návrhy sa nevracajú navrhovateľom, ale zostávajú archivované u vyhlasovateľa ako súčasť dokumentácie súťaže.

7. Všetky dokumenty a listiny, ktoré navrhovateľ predloží vyhlasovateľovi, musia byť podpísané navrhovateľom, štatutárnym orgánom navrhovateľa alebo členom štatutárneho orgánu navrhovateľa alebo jeho zástupcom, ktorý je oprávnený konať v mene navrhovateľa v záväzkových vzťahoch. Oprávnenie tejto osoby musí byť v súlade s predloženými dokladmi o oprávnení podnikať, resp. splnomocnením.
8. Vyhlasovateľ si vyhradzuje právo na obstaranie jednotlivých komponentov od iných dodávateľov po vzájomnej dohode s navrhovateľom
9. Vyhlasovateľ si vyhradzuje právo z predloženého návrhu prijať aj čiastkové plnenie predloženého návrhu.
10. Vyhlasovateľ je oprávnený vybrať si návrh, ktorý mu najviac vyhovuje, pričom nie je povinný oznamovať dôvody svojho rozhodnutia. Takisto je oprávnený odmietnuť všetky predložené návrhy.
11. Súťažné podklady sú predmetom obchodného tajomstva bez časového obmedzenia.

F. ZOZNAM PRÍLOH

Príloha č. 1 – Špecifikácia predmetu súťaže

Príloha č. 2 - Všeobecné obchodné podmienky (ďalej „VOP“)

Príloha č. 3 - Krycí list

Príloha č. 1 – Špecifikácia predmetu súťaže

Duálne pripojenie do internetu - Perimeter

1. ÚČEL DOKUMENTU

Tento dokument je vypracovaný ako súčasť návrhu projektu " Duálne pripojenie do internetu / Update perimetra siete (pripojenie siete Nafta a.s. do internetu)“ a je podkladom pre vypracovanie ponuky na dodávku perimetra.

2. POPIS SÚČASNÉHO STAVU PERIMETRA SIETE

a) Celá sieť fy Nafta a.s. je pripojená k internetu jedným relatívne pomalým pripojením (12Mb/s) na ISP
   - existuje aj druhé pripojenie, ktoré bolo zriadené pre potreby FTP servera. Momentálne nie je k dispozícii HW a konfiguračné (dohoda s ISP) riešenie na vzájomný backup týchto pripojení

b) MPLS sieťou medzi pobočkami a LAN sieťou centrály – aktuálne reálne využité (po presťahovaní Gbelov) už len v Michalovciach.

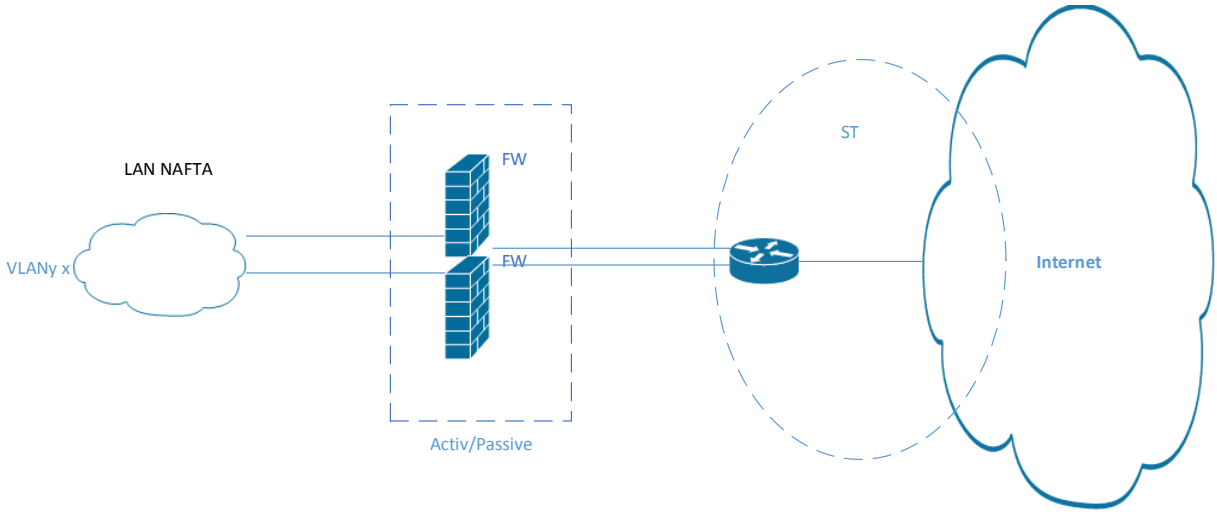
c) Pomocou firewall clustra (riešenie vysokej dostupnosti – ďalej len HA) na linuxe

d) kontrola webovej komunikácie je prostredníctvom prechodu cez proxy server (dva proxy servery za sebou, tmg od MS a linuxový squid)

e) linuxovým poštovým serverom na ktorom prebieha kontrola antispamu a antiviru

f) DNS serverom poskytujúcim záznamy smerom von

g) VPN koncentrátorom zabezpečujúcim prístup interných aj externých pracovníkov a firiem do siete Nafta a.s.. Používame OpenVPN (koncentrátor i klienti)



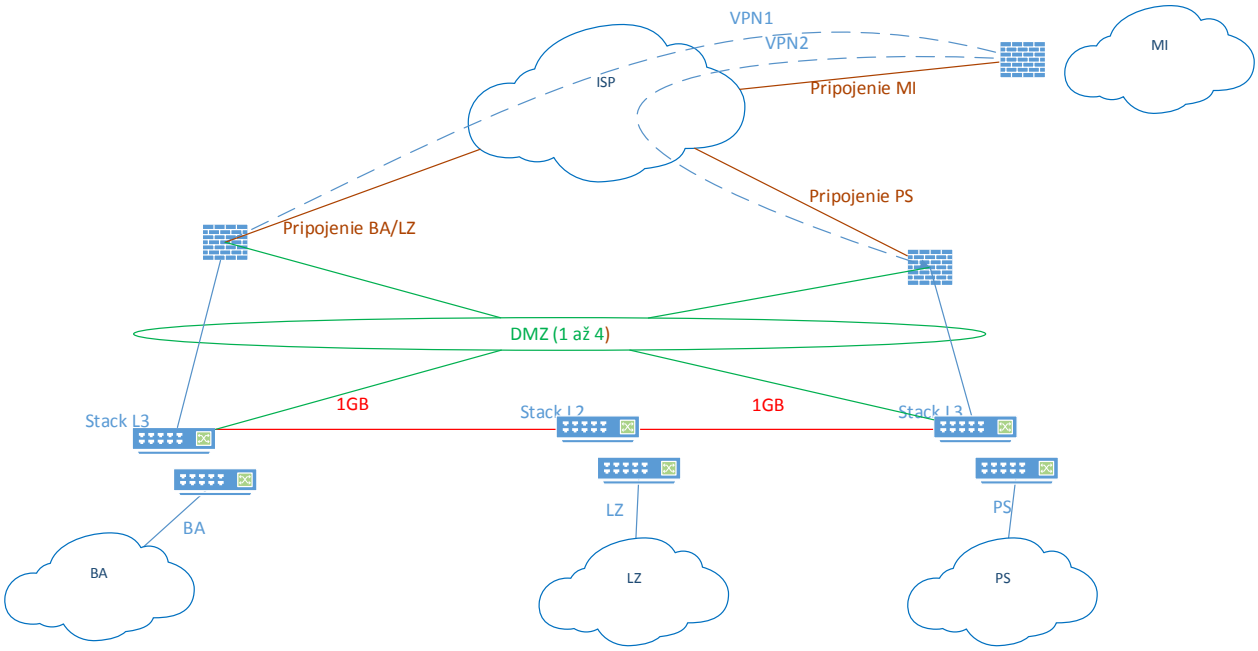
Obrázok č.1 Existujúci stav perimetra v lokalite PS

V súčasnej sieti sme identifikovali nasledovné bezpečnostné riziká:

1) sieť momentálne nedisponuje redundantným pripojením do internetu a redundantnými zariadeniami na perimetri siete
2) nedostatočná ochrana proti DoS útokom
3) nie sú použité ochrany a funkcie next-generation firewallov, kontrola na vyšších vrstvách komunikácie (až po kontrolu na aplikačnej úrovni)

4) nedostatočná ochrana proti hrozbám prostredníctvom sieťových spojení do a z internetu (kontrola vírusov, spyware, v kryptovaných aj nekryptovaných spojení)
5) nie je aktivovaná kontrola prechádzajúcej komunikácie VPN
6) nedostatok ochrany voči úniku informácii (DLP)
7) nedisponuje aplikačnou kontrolou služieb v DMZ sieti
8) problematicky realizovateľné disaster recovery plány
9) Nemožnosť zvýšiť výrazným spôsobom rýchlosť existujúceho metalického pripojenia do internetu.

Schématický náčrt riešenia vonkajšieho perimetra



V náčrte riešenia nie sú realizované komponenty od DMZ vyššie.

3. Perimeter – popis požiadaviek na výkon a funkcionalitu firewallov

3.1 Podrobný opis požiadaviek riešenia na perimeter v BA/Lozorne a PS (spolu 2ks)

Firewall musí byt dodaný ako dva HW appliance (jeden na každej lokalite) (preferujeme túto variantu) alebo virtuálne riešenie pod VMWare.

Riešenie (HW & SW) musí byť postavené na jednom výrobcovi vrátane všetkých databáz (ako napr. antivírus, IPS, filtrácia webu a pod.).

Licencovanie pre firewall nesmie byť založené na počte chránených zariadení alebo na počte chránených užívateľov, preferujeme tzv. per box licenčný model. V prípade, že takéto licencovanie nie je povolené, treba rátať minimálne s 500 používateľmi a s možnosťou ďalšieho rozšírenia. Treba uviesť aj ceny rozšírenia licencií.

Počet fyzických sieťových rozhraní firewallu: min. 10x 10/100/1000 GigE, z toho minimálne 2x 1Gbps SFP

Výkon a priepustnosti firewallu.

Požiadavka na uvedené výkony/priepustnosti je pri plnej funkčnosti firewallu (t.j. nakonfigurovaní a spustení všetkých požadovaných služieb):

1) firewallu min. 300 Mbps full-duplex
2) systému riadenia aplikácii min. 300 Mbps
3) systému riadenia FW + AV +IPS + Aplikačná kontrola min. 200Mbit full-duplex
4) Firewall musí byť schopný obslúžiť min. 120000 súčasných spojení, musí zvládnuť aspoň 15000 nových spojení za sekundu
5) IPSEC protokolu min. 100Mbps
6) Minimálny počet IPSEC tunelov 600
7) Počet súčasných SSL VPN používateľov min. 400

Ďalšie požiadavky na riešenie perimetra:

1) Firewall musí umožňovať zabezpečený vzdialený prístup (secure remote access) pomocou SSL VPN.
2) Firewall musí mať podporu pre 802.1q, minimálny počet VLAN 300, podpora číslovania by bola vhodná pre VLAN-y v rozsahu 1-4094, prípadne uvedte.
3) Firewall musí mať podporu agregácie portov pomocou štandardu 802.3ad
4) Ukladanie logov bude dočasne (do vybudovania syslog servera) riešené interne vo FW. Deklarujte veľkosť interného pamäťového priestoru pre ukladanie logov.
5) Podpora cluster-u v režime Active-active a active-pasive. Podpora pre interface monitoring a synchronizáciu spojení medzi jednotlivými nodmi cluster-u.
6) uvítali by sme keby bol management firewall platformy fyzicky oddelený, v tom prípade musí používať samostatný CPU, RAM, NIC. Táto požiadavka nie je KO kritérium.
7) Firewall musí podporovať dynamický routing, minimálne RIP, OSPF, BGP, PIM a IGMP.
8) Uvítali by sme, keby riešenie podporovalo virtuálne routovacie tabuľky eventuálne inú technológiu ktorou by sa dalo ovplyvniť routovanie (smerovanie) dát na základe splnenia alebo nesplnenia definovaných pravidiel. Táto požiadavka nie je KO kritérium.
9) Systém musí podporovať policy based forwarding.
10) Policy based forwarding by mal byť založený na používateľoch alebo skupinách používateľov a na aplikáciách.
11) Firewall musí mať stavovú synchronizáciu TCP, UDP a NAT spojení
12) Systém musí podporovať rôzne módy pre sieťové rozhrania: L2 (transparent), L3 a promiskuitný mód
13) Firewall musí byť schopný autentifikovať používateľov. Požadujeme podporu LDAP, RADIUS a Kerberos.
14) Autentifikácia používateľov pomocou Microsoft AD musí byť možná aj bez klienta na koncových zariadeniach.
15) Autentifikácia používateľov pomocou Microsoft AD bez nutnosti inštalácie klienta na doménové kontroléry. Agent pre komunikáciu s AD musí byt zabudovaný priamo v systéme firewallu.
16) Systém musí mať podporu min. pre 3 rôzne Microsoft AD domény súčasne.
17) Uvítame rozšíriteľnosť riešenia o agenta pre identifikáciu používateľov pre OS Microsoft Windows, Mac OS X, Android a iOS. Táto požiadavka nie je KO kritérium.

18) Riešenie musí obsahovať spôsob identifikácie používateľov na Microsoft a Citrix terminál serveroch (buď pomocou agentov alebo bez agentov). Táto požiadavka nie je KO kritérium. Doplniť o detailný popis funkcionality.
19) Systém musí podporovať autentifikáciu používateľov pomocou sekvencií alebo iným spôsobom. Požadujeme možnosť definovať minimálne 3 typy autentifikácii v rámci jedného autentifikačného profilu, napr. LDAP, Rádius, lokálna DB. V prípade iného riešenia viacnásobného overenia používateľa žiadame detailný popis.
20) Firewall musí mať integrovaný systém ochrany proti sieťovým útokom (IPS). Databázu signatúr IPS preferujeme ukladať priamo na zariadení. Aplikácia IPS profilu na prechádzajúcu komunikáciu musí byť na úrovni firewall policy.V prípade inej overenej implementácii IPS do FW žiadame detailný popis.
21) Firewall musí mať integrovaný systém detekcie a riadenia aplikácii. Systém musí byť schopný zisťovať aplikácie pomocou signatúr, t.j. nezávisle na použitom porte/protokole. Taktiež musí umožňovať vytvorenie vlastných signatúr pre aplikácie. Žiadame detailný popis spôsobu vytvárania vlastných signatúr. Aplikácie musia byť identifikované priamo vo firewalle (firewall si môže stiahnúť zo stránok výrobcu signatúry, ale nesmie posielať aplikácie na otestovanie) a musia byť jedným z rozhodovacích kritérií v rámci firewall policy.
22) Systém by mal umožňovať riadenie aplikácii tak, že vie blokovať všetky aplikácie okrem tých, ktoré sú explicitne povolené v rámci politík. Táto požiadavka nie je KO kritériom, ale preferujeme jej splnenie.
23) Systém musí byť schopný de kryptovať SSL pre outbound aj inbound traffic a ďalej musí byť schopný zablokovať exploity (IPS), vírusy a škodlivý kód (AntiVirus a AntiSpyware) v rámci SSL komunikácie. Systém musí umožňovať vytvorenie výnimiek z SSL dekryptovania minimálne na základe URL kategórie.
24) Systém musí umožňovať blokovanie súborov na základe typu a obsahu. Systém musí tiež obsahovať aspoň základnú ochranu proti úniku citlivých dát (DLP). Žiadame o detailný popis implementovanej technológie pre DLP.
25) Systém musí umožňovať kontrolu prechádzajúcej komunikácie na prítomnosť vírusov a škodlivého kódu. Databáza signatúr musí byt uložená priamo na zariadení. AV musí byť schopný kontrolovať minimálne nasledovné protokoly: SMTP, POP3, IMAP, HTTP, HTTPS, FTP.
26) Systém musí byť schopný zabrániť zero-day útokom na základe typu a obsahu komunikácie ako aj na základe aplikácie a používateľa. Požadujeme pokročilú detekciu pomocou lokálneho alebo externého sandbox systému. Tento systém musí byť od rovnakého vendora ako FW appliance a musí poskytovať updaty signatúr pre AV, Webfiltering, DNS, C&C.
27) Systém musí byť schopný blokovať komunikáciu na adresy riadiacich centier botnetov.
28) Firewall musí mať integrovanú ochranu proti botnetom - reputácia IP adries, DNS a URL záznamov.
29) Firewall musí umožňovať riadenie prístupu na web stránky podľa kategórii a užívateľských identít. Žiadame uviesť počet kategórii a kategórie URL databázy ktoré sú poskytované výrobcom firewallu (bez používateľsky definovaných kategórií) ak takáto databáza existuje...
30) Riešenie musí poskytovať možnosť obmedzenia šírky pásma na základe src alebo dst IP, protokolu, user identity, aplikácie a času (od – do, dni v týždni, dni v týždni + čas, atď.)
31) QoS systém musí poskytovať možnosť nastavenia aspoň 7 rôznych traffic classes

32) Firewall musí poskytovať ochranu pred DoS útokmi aspoň na úrovni limitovania počtu súčasných spojení per source alebo destination IP, user identity a aplikáciu.
33) Uvítali by sme keby riešenie umožňovalo konfiguráciu bezpečnostných politík z jedného miesta, napr, z centrálneho mgmt serveru. Pravidlá z centrálneho managementu môžu byť definované ako nadradené alebo podradené k lokálnym firewall pravidlám. Ak takáto možnosť vo vašom riešení existuje, prosíme o detailný popis.
34) Riešenie musí umožňovať vzdialené pripojenie k zariadeniu pomocou SSH a/alebo HTTPS protokolov.
35) Riešenie musí podporovať debugovanie problémových scenárov na úrovni L2 - L7. Musí tiež obsahovať riešenie alebo spôsob, ktorým bude produkovať výstup v pcap formáte.
36) Podpora pravidelného automatického zálohovania konfigurácie.
37) Systém musí vedieť publikovať MS Exchange cez owa.

3.2 Podrobný opis požiadaviek riešenia na perimeter v MI (1ks)

Firewall musí byt dodaný ako HW appliance.

Riešenie (HW & SW) musí byť postavené na jednom výrobcovi vrátane všetkých databáz (ako napr. antivírus, IPS, filtrácia webu a pod.).

Licencovanie pre firewall nesmie byť založené na počte chránených zariadení alebo na počte chránených užívateľov, preferujeme tzv. per box licenčný model. V prípade, že takéto licencovanie nie je povolené, treba rátať minimálne s 50 používateľmi a s možnosťou ďalšieho rozšírenia. Treba uviesť aj ceny rozšírenia licencií.

Počet fyzických sieťových rozhraní firewallu (v prípade appliance): min. 4x 10/100/1000 GigE.

Výkon a priepustnosti firewallu.

Požiadavka na uvedené výkony/priepustnosti je pri plnej funkčnosti firewallu (t.j. nakonfigurovaní a spustení všetkých požadovaných služieb):

1) firewallu min. 100 Mbps full-duplex
2) systému riadenia aplikácii min. 50 Mbps
3) Firewall musí byť schopný obslúžiť min. 64000 súčasných spojení, musí zvládnuť aspoň 3000 nových spojení za sekundu
4) IPSEC protokolu min. 50 Mbps
5) Minimálny počet IPSEC tunelov 50
6) Počet súčasných SSL VPN používateľov min. 50.

Ďalšie požiadavky na riešenie perimetra:

1) Firewall musí umožňovať secure remote access pomocou SSL VPN.
2) Firewall musí mať podporu pre 802.1q, minimálny počet VLAN 100, podpora číslovania by bola vhodná pre VLAN-y v rozsahu 1-4094, prípadne uvedte.
3) Ukladanie logov bude dočasne (do vybudovania syslog servera) riešené interne vo FW. Deklarujte veľkosť interného pamäťového priestoru pre ukladanie logov.
4) Firewall musí podporovať dynamický routing, minimálne RIP, OSPF, BGP, PIM a IGMP.
5) Systém musí podporovať policy based forwarding. Policy based forwarding by mal byť založený na používateľoch alebo skupinách používateľov a na aplikáciách.
6) Firewall musí mať stavovú synchronizáciu TCP, UDP a NAT spojení

7) Systém musí podporovať rôzne módy pre sieťové rozhrania: L2 (transparent), L3 a promiskuitný mód.
8) Firewall musí byť schopný autentifikovať používateľov. Požadujeme podporu LDAP, RADIUS a Kerberos.
9) Autentifikácia používateľov pomocou Microsoft AD musí byt možná aj bez klienta na koncových zariadeniach.
10) Autentifikácia používateľov pomocou Microsoft AD bez nutnosti inštalácie klienta na doménové kontroléry. Agent pre komunikáciu s AD musí byť zabudovaný priamo v systéme firewallu.
11) Systém musí mať podporu min. pre 3 rôzne Microsoft AD domény súčasne.
12) Riešenie musí obsahovať spôsob identifikácie používateľov na Microsoft a Citrix terminál serveroch (buď pomocou agentov alebo bez agentov). Táto požiadavka nie je KO kritérium. Doplniť o detailný popis funkcionality.
13) Systém musí podporovať autentifikáciu používateľov pomocou sekvencií alebo iným spôsobom. Požadujeme možnosť definovať minimálne 3 typy autentifikácii v rámci jedného autentifikačného profilu, napr. LDAP, Rádius, lokálna DB. V prípade iného riešenia viacnásobného overenia používateľa žiadame detailný popis.
14) Firewall musí mať integrovaný systém detekcie a riadenia aplikácii. Systém musí byť schopný zisťovať aplikácie pomocou signatúr, t.j. nezávisle na použitom porte/protokole. Taktiež musí umožňovať vytvorenie vlastných signatúr pre aplikácie. Žiadame detailný popis spôsobu vytvárania vlastných signatúr. Aplikácie musia byť identifikované priamo vo firewalle (firewall si môže stiahnúť zo stránok výrobcu signatúry, ale nesmie posielať aplikácie na otestovanie) a musia byť jedným z rozhodovacích kritérií v rámci firewall policy.
15) Systém by mal umožňovať riadenie aplikácii tak, že vie blokovať všetky aplikácie okrem tých, ktoré sú explicitne povolené v rámci politík. Táto požiadavka nie je KO kritériom, ale preferujeme jej splnenie.
16) Systém musí umožňovať blokovanie súborov na základe typu a obsahu. Systém musí tiež obsahovať aspoň základnú ochranu proti úniku citlivých dát (DLP). Žiadame o detailný popis implementovanej technológie pre DLP.
17) Riešenie musí poskytovať možnosť obmedzenia šírky pásma na základe src alebo dst IP, protokolu, user identity, aplikácie a času (od – do, dni v týždni, dni v týždni + čas, atď.)
18) QoS systém musí poskytovať možnosť nastavenia aspoň 7 rôznych traffic classes
19) Firewall musí poskytovať ochranu pred DoS útokmi aspoň na úrovni limitovania počtu súčasných spojení per source alebo destination IP, user identity a aplikáciu.
20) Uvítali by sme keby riešenie umožňovalo konfiguráciu bezpečnostných politík z jedného miesta, napr, z centrálneho mgmt serveru. Pravidlá z centrálneho managementu môžu byť definované ako nadradené alebo podradené k lokálnym firewall pravidlám. Ak takáto možnosť vo vašom riešení existuje, prosíme o detailný popis.
21) Riešenie musí umožňovať vzdialené pripojenie k zariadeniu pomocou SSH a/alebo HTTPS protokolov.
22) Riešenie musí podporovať debugovanie problémových scenárov na úrovni L2 - L7. Musí tiež obsahovať riešenie alebo spôsob, ktorým bude produkovať výstup v pcap formáte.
23) Podpora pravidelného automatického zálohovania konfigurácie.

3.3 Podrobný opis požiadaviek riešenia interného firewallu (1ks)

Firewall musí byt dodaný ako HW appliance.

Riešenie (HW & SW) musí byť postavené na jednom výrobcovi vrátane všetkých databáz (ako napr. antivírus, IPS, filtrácia webu a pod.).

Licencovanie pre firewall nesmie byť založené na počte chránených zariadení alebo na počte chránených užívateľov, preferujeme tzv. per box licenčný model. V prípade, že takéto licencovanie nie je povolené, treba rátať minimálne s 50 používateľmi a s možnosťou ďalšieho rozšírenia. Treba uviesť aj ceny rozšírenia licencií.

Počet fyzických sieťových rozhraní firewallu (v prípade appliance): min. 4x 10/100/1000 GigE.

Výkon a priepustnosti firewallu.

Požiadavka na uvedené výkony/priepustnosti je pri plnej funkčnosti firewallu (t.j. nakonfigurovaní a spustení všetkých požadovaných služieb):

1) firewallu min. 100 Mbps full-duplex
2) systému riadenia aplikácii min. 50 Mbps
3) Firewall musí byť schopný obslúžiť min. 64000 súčasných spojení, musí zvládnuť aspoň 3000 nových spojení za sekundu
4) IPSEC protokolu min. 50 Mbps
5) Minimálny počet IPSEC tunelov 50
6) Počet súčasných SSL VPN používateľov min. 50.

Ďalšie požiadavky na riešenie perimetra:

1) Firewall musí umožňovať secure remote access pomocou SSL VPN.
2) Firewall musí mať podporu pre 802.1q, minimálny počet VLAN 100, podpora číslovania by bola vhodná pre VLAN-y v rozsahu 1-4094, prípadne uvedte.
3) Ukladanie logov bude dočasne (do vybudovania syslog servera) riešené interne vo FW. Deklarujte veľkosť interného pamäťového priestoru pre ukladanie logov.
4) Firewall musí podporovať dynamický routing, minimálne RIP, OSPF, BGP, PIM a IGMP.
5) Systém musí podporovať policy based forwarding. Policy based forwarding by mal byť založený na používateľoch alebo skupinách používateľov a na aplikáciách.
6) Firewall musí mať stavovú synchronizáciu TCP, UDP a NAT spojení
7) Systém musí podporovať rôzne módy pre sieťové rozhrania: L2 (transparent), L3 a promiskuitný mód.
8) Firewall musí byť schopný autentifikovať používateľov. Požadujeme podporu LDAP, RADIUS a Kerberos.
9) Autentifikácia používateľov pomocou Microsoft AD musí byt možná aj bez klienta na koncových zariadeniach.
10) Autentifikácia používateľov pomocou Microsoft AD bez nutnosti inštalácie klienta na doménové kontroléry. Agent pre komunikáciu s AD musí byť zabudovaný priamo v systéme firewallu.
11) Systém musí mať podporu min. pre 3 rôzne Microsoft AD domény súčasne.
12) Riešenie musí obsahovať spôsob identifikácie používateľov na Microsoft a Citrix terminál serveroch (buď pomocou agentov alebo bez agentov). Táto požiadavka nie je KO kritérium. Doplniť o detailný popis funkcionality.
13) Systém musí podporovať autentifikáciu používateľov pomocou sekvencií alebo iným spôsobom. Požadujeme možnosť definovať minimálne 3 typy autentifikácii v rámci

jedného autentifikačného profilu, napr. LDAP, Rádius, lokálna DB. V prípade iného riešenia viacnásobného overenia používateľa žiadame detailný popis.

14) Firewall musí mať integrovaný systém detekcie a riadenia aplikácii. Systém musí byť schopný zisťovať aplikácie pomocou signatúr, t.j. nezávisle na použitom porte/protokole. Taktiež musí umožňovať vytvorenie vlastných signatúr pre aplikácie. Žiadame detailný popis spôsobu vytvárania vlastných signatúr. Aplikácie musia byť identifikované priamo vo firewalle (firewall si môže stiahnúť zo stránok výrobcu signatúry, ale nesmie posielať aplikácie na otestovanie) a musia byť jedným z rozhodovacích kritérií v rámci firewall policy.
15) Systém by mal umožňovať riadenie aplikácii tak, že vie blokovať všetky aplikácie okrem tých, ktoré sú explicitne povolené v rámci politík. Táto požiadavka nie je KO kritériom, ale preferujeme jej splnenie.
16) Systém musí umožňovať blokovanie súborov na základe typu a obsahu. Systém musí tiež obsahovať aspoň základnú ochranu proti úniku citlivých dát (DLP). Žiadame o detailný popis implementovanej technológie pre DLP.
17) Riešenie musí poskytovať možnosť obmedzenia šírky pásma na základe src alebo dst IP, protokolu, user identity, aplikácie a času (od – do, dni v týždni, dni v týždni + čas, atď.)
18) QoS systém musí poskytovať možnosť nastavenia aspoň 7 rôznych traffic classes
19) Firewall musí poskytovať ochranu pred DoS útokmi aspoň na úrovni limitovania počtu súčasných spojení per source alebo destination IP, user identity a aplikáciu.
20) Uvítali by sme keby riešenie umožňovalo konfiguráciu bezpečnostných politík z jedného miesta, napr. z centrálneho mgmt serveru. Pravidlá z centrálneho managementu môžu byť definované ako nadradené alebo podradené k lokálnym firewall pravidlám. Ak takáto možnosť vo vašom riešení existuje, prosíme o detailný popis.
21) Riešenie musí umožňovať vzdialené pripojenie k zariadeniu pomocou SSH a/alebo HTTPS protokolov.
22) Riešenie musí podporovať debugovanie problémových scenárov na úrovni L2 - L7. Musí tiež obsahovať riešenie alebo spôsob, ktorým bude produkovať výstup v pcap formáte.
23) Podpora pravidelného automatického zálohovania konfigurácie.

4. Proxy a mail ochrana

4.1 Podrobný opis požiadaviek riešenia antispam

Antispam musí byt dodaný ako HW appliance (preferujeme túto variantu) alebo virtuálne riešenie pod VMWare. Riešenie musí byť postavené na jednom vendorovi vrátane všetkých databáz (ako napr. antivirus, antispam a pod.). HW musí byť dostatočne výkonný na to aby zvládol kontrolovať SMTP komunikáciu pre min. 700 používateľov (aktuálne cca 500 až 600 používateľov).

Licencovanie môže byť založené na počte chránených užívateľov, v takom prípade požadujeme licenciu pre min. 650 užívateľov. S ponukou rozšírenia licencií o ďalších užívateľov (ceny licencii pre ďalších užívateľov).

V prípade HW apliance:

Počet fyzických sieťových rozhraní: min. 2x 10/100/1000 GigE.

1) Zariadenie musí mať redundantne napájanie, možnosť konfigurácie diskového subsystému do RAID-u s redundanciou jedného alebo dvoch diskov.
2) Interný storage musí mať kapacitu minimálne 500GB.
3) Podpora HA v režime Active-Passive.
4) Riešenie musí poskytovať možnosť ukladať logy interne aj na syslog server
5) Systém musí podporovať rôzne módy: SMTP proxy a MTA (Mail Transfer Agent) musí byť schopný autentifikovať používateľov. Požadujeme podporu min. LDAP.
6) Systém musí umožňovať blokovanie súborov na základe typu a obsahu. Systém musí tiež obsahovať aspoň základnú ochranu proti úniku citlivých dát (DLP). Žiadame o detailný popis implementovanej technológie pre DLP.
7) Zariadenie musí mať podporu pre per user karantény. Používatelia musia mať možnosť náhľadu do svojej karantény. Administrátori resp. group administrátori musia mať možnosť nahliadať do karantén všetkých používateľov resp. všetkých používateľov v rámci spravovanej skupiny.
8) Zariadenie musí umožňovať integráciu s MS Outlook klientom za účelom jednoduchého označovania prichádzajúcej pošty pomocou junk/good tlačidiel.
9) Riešenie musí umožňovať používateľom správu svojich black/white listov.
10) Musí byť schopná zabrániť DHA (Directory Harvest Attacks) a DoS útokom. Systém musí byť schopný pozdŕžať podozrivé spojenia (tarpitting), úplne zablokovať odosielateľa v prípade prekročenia thresholdov (napr. počet spojení per IP address) resp. obmedziť odosielateľa (throttling)
11) Riešenie musí obsahovať systém Bounce Address Tag Validation na ochranu pred NDR útokmi.
12) Súčasťou Antispam ochrany musia byť technológie, ktoré pokrývajú funkčnosťou nasledujúce technológie: Greylisting s podporou whitelistov, IP reputation service, SPF/Sender ID, DKIM, Language based filtering, RBL/DNSBL, Phishing/Fraud detection
13) Súčasťou Antivírus ochrany musí byť detekcia zero-day malware-u. AV musí byť schopný odrezať nebezpečné prílohy.
14) Zariadenie musí byť schopné identifikovať a zablokovať šírenie spamu z 'trusted' siete minimálne pomocou limitov na počet odchádzajúcich emailov. V prípade prepojenia na LDAP požadujeme, aby boli administrátorom ihneď reportované odchádzajúce správy z chránených domén, ktoré sú odosielané z neexistujúcich adries.
15) Zariadenie musí obsahovať auditovací nastroj, ktorý bude schopný vyhľadávať informácie v logoch podľa: odosielateľa, príjemcu, subjektu, msg ID, dátumu, typu hrozby (spam, vírus, phishing, clean ...), lokácie (delivered, rejected, junk folder, queued, deleted, bouced, approval box ...). musí tiež umožniť preposlať alebo stiahnuť takto vyhľadané správy.
16) Riešenie by ma implementovaný Approval box alebo obdobnú technológiu na kontrolu a schvaľovanie odosielanej pošty, do ktorého môže byť na základe pravidiel uložená odchádzajúca správa. Správy z Approval boxu sú odoslané príjemcovi až po ich schválení príslušným pracovníkom. Pre approval box požadujeme možnosť nastaviť default akciu v prípade, že príslušný pracovník neapprovne správu do zadaného času. Akcie pre approval box: None, approve & deliver, delete, bouce back to sender. Ak vaše riešenie poskytne iný spôsob schvalovania odosielanej pošty, tak ho žiadame detailne popísať.
17) Zariadenie musí umožňovať externú enkrypciu a dekrypciu správ na základe politík.
18) Musí byť schopne archivovať prechádzajúcu smtp komunikáciu na základe politík.

19) Zariadenie musí obsahovať reportovací nástroj, pomocou ktorého je možné generovať reporty v PDF formáte.
20) Riešenie musí umožňovať vzdialené pripojenie k zariadeniu pomocou SSH a/alebo HTTPS protokolov. Taktiež požadujeme aby bolo možné sledovať performance zariadenia pomocou SNMP protokolu.
21) Podpora pravidelného automatického zálohovania konfigurácie.

4.2 Podrobný opis požiadaviek riešenia proxy:

Proxy musí spĺňať minimálne:

1) Antivírusová kontrola — zariadenie kontroluje celú webovú komunikáciu a blokuje jednotlivé webové objekty, ktoré sú infikované alebo inak nebezpečné.
2) URL filtering — Filtrovanie jednotlivých URL je zabezpečované na základe lokálne uloženej databázy, ktorá sa pravidelne aktualizuje.
3) Autorizácia používateľov — zariadenie umožňuje vytvárať lokálne databázy používateľov, avšak samozrejmosťou je aj podpora LDAP.
4) Data Leakage Prevention — schopnosť zariadenia kontrolovať webovú prevádzku vrátane obsahu požiadaviek či odpovedí umožňuje použiť zariadenie aj ako jednoduché DLP riešenie a chrániť tak spoločnosť pred únikom dôležitých dát/údajov do internetu.

V prípade, že firewall(-y) podľa bodu 3.1 vedia zabezpečiť aj funkčnosť proxy, akceptujeme nerealizovať dodávku proxy vo Vašom riešení. V tomto prípade implicitne uveďte v popise firewallu podľa bodu 3.1 funkčnosti ktoré zabezpečujú aj funkcie proxy servera.

5. Ostatné pokyny:

Celé riešenie sa bude realizovať po zriadení nových internetových pripojení. Nafta, a.s. pripraví a zabezpečí infraštruktúru pre DMZ-ky.

Celé riešenie perimetra sa otestuje mimo siete LAN. Nafta a.s. až do posledných testov bude fungovať na existujúcom riešení.

Testy budú prebiehať s vybranými používateľmi, s kópiami virtuálnych serverov, ktoré budú umiestnené v DMZ-ke.

Po akceptácii testov sa preklopí celá prevádzka na novú infraštruktúru.

V cene riešenia musí dodávateľ akceptovať minimálne jeden návrat k existujúcemu systému (v prípade neúspešného preklopenia na novú infraštruktúru).

Príloha č. 2 - Všeobecné obchodné podmienky – odberateľ (ďalej „VOP“)

http://www.nafta.sk/sites/default/files/uploaded-files/vop_nove_2014_jun_nafta_odberatel.pdf

Príloha č. 3

KRYCÍ LIST zo dňa .....

Názov: „Duálne pripojenie do internetu - Perimeter“

A. Navrhovateľ:

Názov: .....

Adresa: .....

IČO: .....

DIČ: .....

Poverený zástupca navrhovateľa: .....

tel. ..... fax. .....

B. Po preštudovaní súťažných podkladov navrhujeme vykonanie predmetu súťaže:

1. podľa položiek :

P. Č	Položka	množstvo	MJ	Jed. cena	Celkom v Eur bez DPH
1	Náklady na HW a SW pre perimeter				
2	Náklady na inštaláciu a konfiguráciu zariadení				
3	Náklady na 6 mesačnú podpora				
4	Náklady na eventuálne dobudovanie infraštruktúry				
5	Školenie				
6	Dokumentácia, Projekt vyhotovenia				
Cena za perimeter bez DPH (súčet 1-6)					
7	Náklady na proxy a mail ochranu				
8	Náklady na inštaláciu a konfiguráciu zariadení				
9	Náklady na 6 mesačnú podpora				
10	Náklady na eventuálne dobudovanie infraštruktúry				
11	Školenie				
12	Dokumentácia, Projekt vyhotovenia				
Cena za proxy a mail ochranu bez DPH (súčet 7-12)					

Cena celkom bez DPH (súčet 1-12)	
DPH 20%	
Cena celkom s DPH v Eur	

2. v termíne:

Začatie prác: **15.10.2014**

Ukončenie prác: **október / november 2014**

Platnosť tohto návrhu je stanovená do: **28.02.2015**

.....

Pečiatka, meno, priezvisko a podpis zástupcu navrhovateľa