



Č. j. UHUL/6910/2020/ISaT

Podmínky veřejné zakázky malého rozsahu dle § 27 zákona č. 134/2016 Sb.

Název veřejné zakázky:

Dodávka VPN řešení

1. Informace o zadavateli:

Zadavatel: ČR – Ústav pro hospodářskou úpravu lesů Brandýs nad Labem
organizační složka státu zřízená MZe ČR

Adresa: Nábřežní 1326, 250 01 Brandýs nad Labem

IČ: 00020681

DIČ: neplátce DPH

Osoba oprávněná
za zadavatele jednat: Ing. Jaromír Vašíček, CSc., ředitel ÚHÚL

Administrace zakázky: Rudolfa Šnajdrová,
Telefon: 321 021 120
E-mail: snajdrova.rudolfa@uhul.cz

2. Předmět veřejné zakázky:

Název dodávky	CPV	Měrná jednotka	Množství
Dodávka VPN řešení	72267100-0	Viz specifikace	Viz specifikace
Předpokládaná celková hodnota v Kč bez DPH:		275 000,-	

Předpokládaná hodnota je zároveň i hodnotou maximální pro plnění.

3. Základní technická specifikace

Viz příloha č. 3

Zadavatel si vyhrazuje právo v průběhu posuzování a hodnocení nabídek provést laboratorní testy řešení nabízených jednotlivými účastníky z důvodu ověření deklarovaných technických parametrů.

Z důvodu laboratorních testů si zadavatel vyhrazuje právo na dodání libovolného zařízení ze specifikace účastníka k laboratorním testům do 10-ti pracovních dnů od doručení požadavku zadavatele.

Předmětem laboratorních testů je prověření deklarovaných technických parametrů účastníkem nabízeného plnění a prověření zda navrhované řešení splňuje požadavky uvedené v „Technické specifikaci“.

Nesplnění testu (požadovaného parametru či funkčnosti) je chápáno jako nesplnění požadavků zadavatele, které povede k vyřazení nabídky účastníka a jeho následnému vyloučení z účasti v zadávacím řízení.

4. Doba a místo plnění:

Termín plnění: do 20 dnů od účinnosti smlouvy / na 3 roky

Termín fakturace: do 18. 12.2020

Místo plnění: Praha, Žižkovská věž

5. Způsob zpracování a podání nabídky:

- Nabídka bude podána přes elektronické tržiště Gemin.
- Nabídka bude podána v elektronické podobě prostřednictvím elektronického nástroje.
- Zadavatel nebude akceptovat nabídky podané jiným způsobem (poštou, osobně, emailem).
- Nabídka bude obsahovat:
 - Návrh smlouvy digitálně podepsaný
 - vyhotovení smlouvy ve formátu. doc /Microsoft Word/,
 - doklady v prosté kopii, jimiž dodavatel prokazuje splnění kvalifikace,
 - vyplněný Krycí list Příloha č. 1
 - vyplněné Čestné prohlášení Příloha č. 2
 - vyplněný cenový přehled, Příloha č. 4

- Přehled o splnění závazných technických a funkčních požadavků viz příloha č.3 bod 6. „Závazné technické a funkční požadavky“- doplnit
- Popis nabízeného řešení ve formě dokumentu se specifikací nabízeného řešení, produktovou dokumentací, a to k jednotlivým nabízeným HW a SW komponentům.

Dokumenty s produktovou dokumentací mohou být doloženy v českém nebo v anglickém jazyce.

- Předloží-li dodavatel zadavateli výpis ze seznamu kvalifikovaných dodavatelů, tento výpis nahrazuje doklad prokazující

- a) základní způsobilost, čestné prohlášení, příloha č. 2,
- b) profesní způsobilost v tom rozsahu, v jakém údaje ve výpisu ze seznamu kvalifikovaných dodavatelů prokazují splnění kritérií profesní způsobilosti.

Zadavatel přijme výpis ze seznamu kvalifikovaných dodavatelů, pokud k poslednímu dni, ke kterému má být prokázána základní způsobilost nebo profesní způsobilost, není výpis ze seznamu kvalifikovaných dodavatelů starší než 3 měsíce.

- Nabídka nebude obsahovat přepisy a opravy, které by mohli zadavatele uvést v omyl.
- Nabídka bude zpracována v jazyce českém.
- Variantní řešení se nepřipouští.
- Zadavatel požaduje plnění v celém rozsahu nabídky.

6. Lhůta pro podání nabídek:

Počátek běhu lhůty pro podání nabídek:
23. 11. 2020

Konec běhu lhůty pro podání nabídek:
2. 12. 2020 v 9: 00 hodin

7. Otevírání obálek s nabídkami:

2. 12. 2020 v 9:00 hodin

8. Údaje pro podání nabídky:

Uchazeč předloží přehlednou nabídku v Kč v členění:

- Nabídková cena bez daně z přidané hodnoty (DPH)
- Samostatně DPH (podle platných předpisů)
- Nabídková cena včetně DPH

Nabídková cena v této skladbě bude uvedena na krycím listě nabídky a bude stanovena jako cena nejvýše přípustná.

9. Údaje o hodnotících kritériích:

Základním kritériem hodnocení je: Nejnižší nabídková celková cena

Váha: 100 %

V případě shodného výsledku rozhodne pořadí, ve kterém byly nabídky podány.

10. Zadavatel požaduje:

Na základě usnesení vlády ze dne 18. prosince 2013 č. 982 ke Zprávě o zavádění technologie DNSSEC a o plnění usnesení vlády ze dne 8. června 2009 č. 727, ke Zprávě o přechodu na internetový protokol verze 6 (IPv6) tyto body:

- podpora technologie DNSSEC všech relevantních požadovaných služeb
- podporu protokolu IPv6 v případě dodávky služeb, tak i zboží (hardware)

11. Základní způsobilost:

Čestné prohlášení účastníka, že je způsobilý být dodavatelem veřejné zakázky, tedy že splňuje základní způsobilost viz příloha č. 2.

12. Profesní způsobilost:

Dodavatel prokazuje splnění profesní způsobilosti ve vztahu k České republice předložením výpisu z obchodního rejstříku nebo jiné obdobné evidence, pokud jiný právní předpis zápis do takové evidence vyžaduje.

13. Ekonomická kvalifikace:

Prokázání ekonomické kvalifikace zadavatel nepožaduje.

14. Technická kvalifikace:

Prokázání technické kvalifikace zadavatel nepožaduje.

15. Doklady o kvalifikaci

Doklady prokazující základní způsobilost a profesní způsobilost musí prokazovat splnění požadovaného kritéria způsobilosti nejpozději v době 3 měsíců přede dnem zahájení zadávacího řízení.

16. Zadávací lhůta (se rozumí lhůta, po kterou účastníci zadávacího řízení nesmí ze zadávacího řízení odstoupit)

Délka zadávací lhůty: Zadávací lhůta začíná běžet dnem skončení lhůty pro podání nabídek a končí 30. 12. 2020

17. Zadavatel si vyhrazuje právo:

- a) ověřit deklarované skutečnosti z nabídek před ukončením hodnocení nabídek
- b) vyzvat uchazeče k vysvětlení nabídky před ukončením hodnocení nabídek
- c) všechny předložené nabídky odmítnout
- d) kdykoli zadávací řízení zrušit, a to z jakéhokoli důvodu nebo i bez uvedení důvodu

18. Seznam příloh k veřejné zakázce:

- Příloha č. 1 Krycí list
- Příloha č. 2 Čestné prohlášení
- Příloha č. 3 Technická specifikace
- Příloha č. 4 Cenový přehled

V Brandýse nad Labem, dne 23. 11. 2020

Ing. Jaromír Vašíček, CSc.
ředitel ÚHÚL



Ústav pro hospodářskou úpravu lesů
Brandýs nad Labem, organizační složka státu
Nábřeží 1326, Brandýs n. L.-Stará Boleslav
PSČ: 250 01, IČ: 000 20 681
www.uhul.cz Informace o lesích
Tel.: 321 021 111, pedatelna@uhul.cz

17/15

Krycí list nabídky č. j. ÚHÚL/6910/2020/ISaT**1. Veřejná zakázka**

Veřejná zakázka malého rozsahu dle § 27 zákona č.134/2016 Sb.

Název:

„Dodávka VPN řešení“**2. Základní identifikační údaje:****2.1. Zadavatel**

Název :	Ústav pro hospodářskou úpravu lesů Brandýs nad Labem
Sídlo:	Nábřeží 1326, 250 01 Brandýs nad Labem- Stará Boleslav
Tel.	321 021 111
E-mail	podatelna@uhul.cz
IČ :	00020681
Osoba oprávněná jednat jménem zadavatele:	Ing. Jaromír Vašíček, CSc., ředitel ÚHÚL
Kontaktní osoba:	Rudolfa ŠNAJDROVÁ
Tel./fax:	321 021 120
E-mail:	snajdrova.rudolfa@uhul.cz

2.2. Uchazeč:

Název:	
Sídlo/místo podnikání:	
Tel./fax:	
E-mail:	
IČ:	
DIČ:	
Spisová značka v obchodním rejstříku:	
Osoba oprávněná jednat za uchazeče:	
Kontaktní osoba uchazeče:	
Tel./fax:	
E-mail:	

3. Nabídková cena

Název dodávky	Cena bez DPH	Samostatně DPH	Cena včetně DPH
Cena celkem			

4. Měna, ve které je nabídková cena v bodu 3. uvedena**5. Oprávněná osoba za uchazeče jednat**

Podpis oprávněné osoby:	
Titul, jméno, příjmení:	
Funkce:	
Razítko:	

ČESTNÉ PROHLÁŠENÍ ZÁKLADNÍ ZPŮSOBILOSTI
--

Název zakázky	Dodávka VPN řešení
Č. j.	UHUL/6910/2020/ISaT

Identifikační údaje uchazeče	
Název uchazeče	
Sídlo	
IČ	
DIČ	
Bankovní spojení	
Osoba oprávněná jednat jménem či za dodavatele	

Prohlašuji tímto čestně, že nejsem dodavatel, který

- a) byl v zemi svého sídla v posledních 5 letech před zahájením zadávacího řízení pravomocně odsouzen pro trestný čin uvedený v příloze č. 3 k tomuto zákonu nebo obdobný trestný čin podle právního řádu země sídla dodavatele; k zahrazeným odsouzením se nepřihlíží,
- b) má v České republice nebo v zemi svého sídla v evidenci daní zachycen splatný daňový nedoplatek,
- c) má v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění,
- d) má v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti,
- e) je v likvidaci²⁴⁾, proti němuž bylo vydáno rozhodnutí o úpadku²⁵⁾, vůči němuž byla nařízena nucená správa podle jiného právního předpisu²⁶⁾ nebo v obdobné situaci podle právního řádu země sídla dodavatele.

Je-li dodavatelem právnická osoba, musí podmínku podle odstavce 1 písm. a) splňovat tato právnická osoba a zároveň každý člen statutárního orgánu. Je-li členem statutárního orgánu dodavatele právnická osoba, musí podmínku podle odstavce 1 písm. a) splňovat

- a) tato právnická osoba,
- b) každý člen statutárního orgánu této právnické osoby a
- c) osoba zastupující tuto právnickou osobu v statutárním orgánu dodavatele.

Účastní-li se zadávacího řízení pobočka závodu

- a) zahraniční právnické osoby, musí podmínku podle odstavce 1 písm. a) splňovat tato právnická osoba a vedoucí pobočky závodu,

- b) české právnické osoby, musí podmínku podle odstavce 1 písm. a) splňovat osoby uvedené v odstavci 2 a vedoucí pobočky závodu.

ČESTNÉ PROHLÁŠENÍ O STŘETU ZÁJMŮ

Prohlašuji tímto čestně, že nejsme obchodní společnost, na kterou dopadá zákaz účasti v zadávacím řízení ve smyslu § 4b zákona č. 159/2006 Sb., o střetu zájmů.

Datum	
Místo	
Jméno, příjmení a funkce oprávněné osoby	
Podpis	

Postup tohoto řízení není stanoven přímo zákonem č. 134/2016 Sb., o veřejných zakázkách ve znění pozdějších předpisů

TECHNICKÁ SPECIFIKACE

OBSAH

1. OBECNÁ FUNKČNÍ A TECHNICKÁ SPECIFIKACE.....	2
2. POPIS A POŽADOVANÉ PARAMETRY SLUŽBY	4
3. POŽADAVKY NA VYUŽÍVANÝ HW	5
4. POŽADAVKY NA PARAMETRY VPN	7
5. PŘÍSLUŠENSTVÍ.....	8
6. PŘÍLOHY	9
6.1. ZÁVAZNÉ TECHNICKÉ A FUNKČNÍ POŽADAVKY	9

1. OBECNÁ FUNKČNÍ A TECHNICKÁ SPECIFIKACE

Cílem je zajištění bezpečného připojení pro 250 uživatelů současně pomocí technologie VPN do interní sítě ústavu po dobu 3 let. Připojení bude realizováno formou služby. Služba bude poskytována prostřednictvím HW a SW vybavení umístěného v hostingovém centru Zadavatele a SW klientem instalovaným na koncových zařízeních připojovaných uživatelů.

Uchazeč zajistí zřízení služby, konfiguraci a provoz služby, včetně všech HW, SW prostředků a případných licencí. Dále Uchazeč zajistí realizaci případných změnových požadavků v rozsahu 2 MD/rok.

Cena za služby bude uhrazena jednorázově po zřízení služby. Změnové požadavky nad rámec stanoveného paušálu budou fakturovány dle skutečnosti. Cena za 1 MD za provedené vícepráce nesmí překročit cenu za 1 MD uvedených v paušálu.

Veškeré použité HW a SW vybavení použité pro poskytování služby přejde po uplynutí 3 let plně do vlastnictví Zadavatele.

Poskytovaná služba musí splňovat požadované parametry specifikované v kapitolách 2, 3 a 4. Zadavatel preferuje, aby všechna HW zařízení a SW využívaná Uchazečem pro zajištění služby byla z důvodu kompatibility a nárokům na management od jednoho výrobce.

Zadavatel požaduje záruku na HW a SW po celou dobu poskytování služby (minimálně 3 roky). Veškerá HW zařízení a SW využívaný Uchazečem pro zajištění služby v rámci tohoto výběrového řízení musí být určen pro český trh a koncového zákazníka Ústav pro hospodářskou úpravu lesů. Zadavatel požaduje pro zajištění služby využití originálního a nového zařízení, licencované ve jménu zákazníka tak, aby bylo možné eskalovat případné závady na technickou podporu výrobce.

U vybraných zařízení bude vítězný Uchazeč povinen doložit oficiální potvrzení zastoupení výrobce o určení používaného HW (seznamu sériových čísel zařízení) pro český trh a koncového zákazníka Ústav pro hospodářskou úpravu lesů, pokud o to Zadavatel požádá.

Uchazeč je povinen v rámci služby zajistit minimálně 3 letou podporu všech využívaných produktů, a to za následujících podmínek:

- Uchazeč poskytne v rámci služby Zadavateli po dobu trvání (3 roky) všechny relevantní SW releases a verze SW nabízené výrobcem tak, aby dodané řešení vyhovovalo zadání Zadavatele a fungovalo bez závad. Uchazeč se zároveň zavazuje informovat Zadavatele o nových SW verzích a funkcích, které mohou rozšiřovat poskytované řešení způsobem, který Zadavatel shledá ve shodě s potřebami dalšího rozvoje poskytovaného řešení. Uchazeč se dále zavazuje získat potřebné SW produkty legálním způsobem za podmínek stanovených výrobcem zařízení.
- Uchazeč je povinen řádným způsobem uzavřít dohodu o podpoře s výrobcem zařízení tak, aby v případě závady na dodaných zařízeních, kterou není Uchazeč schopen sám odstranit, bylo možné eskalovat závadu přímo k výrobcí zařízení. Zároveň je Uchazeč povinen zajistit Zadavateli přístup k dokumentaci výrobce zařízení a znalostní bázi, kterou výrobce v rámci své podpory poskytuje.
- Uchazeč je povinen zajistit opravu provozovaného řešení za podmínek specifikovaných Zadavatelem v režimu 24x7 po dobu 3 let. Odstranění závady do 24 hodin od nahlášení závady.
- Výše specifikovanou podporu a dostupnost náhradních dílů Zadavatel požaduje po dobu min. 3 let.
- Záruka na HW a SW 3 roky (od výrobce)
- Při reklamačním procesu zůstává vadné zboží u zákazníka

- Bezplatný přístup k novým verzím
- firmware po dobu 3 let
- Řešení složitějších technických problémů v češtině pomocí lokálního partnera výrobce využívaných technologií.
- Dodavatel zajistí seznámení zástupců objednatele a jejich proškolení pro práci s nástroji pro centrální správu, s funkcemi administrátorského přístupu k nástrojům jednotlivých funkcí, se zabezpečeným přístupem pro vzdálenou správu jednotlivých komponent (https, ssh), s grafickým rozhraním pro správu jednotlivých komponent řešení, s nástroji pro hromadné a dávkové konfigurace a s nástroji pro monitorování technických parametrů systému.

2. POPIS A POŽADOVANÉ PARAMETRY SLUŽBY

- Zajištění bezpečného připojení pro 250 uživatelů současně pomocí technologie VPN do interní sítě ústavu po dobu 3 let
- Poskytování služby v režimu: 24x7x365
- Délka trvání služby - 3 roky
- Reakce a odstranění závady: Potvrzení servisního zásahu do 1h od prokazatelného nahlášení na helpdesk Uchazeče a odstranění závady do 24 hodin od nahlášení.
- Realizace změnových požadavků Zadavatele v rozsahu 2MD / rok
- Realizace změnových požadavků Zadavatele do 24 hodin od prokazatelného nahlášení na helpdesk Uchazeče
- Služba bude poskytována prostřednictvím HW zařízení (VPN koncentrátor) umístěného v hostingu Zadavatele splňující parametry uvedené v kapitole 3.
- Služba bude poskytována prostřednictvím SW klienta instalovaného na koncové zařízení uživatelů pro současné připojení 250 uživatelů po dobu 3 let splňující parametry popsané v kapitole 4

3. POŽADAVKY NA VYUŽÍVANÝ HW

Pro zajištění služby bude využito 1 ks HW zařízení pro zakončení VPN tunelů od jednotlivých uživatelů – VPN koncentrátor. Tento VPN koncentrátor musí splňovat následující parametry:

Výkon a funkcionality VPN koncentrátoru:

- Formát zařízení - Appliance, 1RU
- Minimální počet 1Gb 10/100/1000 BaseT Ethernet pro management, standardně osazených - 1
- Minimální počet 1Gb SFP rozhraní portů pro data – 4
- Minimální počet 1Gb 10/100/1000 BaseT pro data – 8
- Počet současných VPN připojení – min. 250
- Možnost rozšíření současných VPN připojení na - min. 400
- Možnost rozšíření o funkce NextGen FW
- Možnost rozšíření o funkce NextGen IPS
- Podporovaný počet současně otevřených spojení NGFW s AVC - 400 K
- Rychlost vytváření nových spojení NGFW s AVC - 22K
- Propustnost stavového FW (top parametry) - 6 Gbps
- Propustnost NGIPS (top parametry) – 2,2 Gbps
- Propustnost aplikačního FW (next-gen FW) – (top parametry) – 2,2 Gbps
- Propustnost aplikačního FW + IPS (next-gen FW, IPS) - (top parametry) – 2,2 Gbps
- Hardwarové dešifrování TLS - 1,5 Gbps
- Propustnost IPSec VPN 1024B TCP – 1,2 Gbps
- Podpora L2 (transparentního) módu s podporou NAT a PAT
- Podpora L3 (routovaného) módu s podporou NAT a PAT
- Podpora stateful failover - active/standby
- Podpora min. 2 virtuálních bezpečnostních kontextů (virtuálních firewallů)
- Dynamické směrování - podpora alespoň RIP, OSPF, BGP
- Podpora IPv6 dynamického směrování – alespoň OSPFv3, BGP
- Podpora Policy based Routing
- Podpora kontroly paketů TCP provozu s ochranou před útoky, jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod.
- Podpora filtrace IPv4, IPv6
- Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD
- Podpora filtrace podle bezpečnostních skupinových rolí přiřazených na přístupových přepínačích
- Podpora inspekce IPv6 provozu
- Podpora NAT64 a DNS64
- Možnost integrace cloudových bezpečnostních bran s transparentním směrováním určitého provozu na tyto prvky a zde prováděnou inspekci na škodlivý kód případně pro řízení přístupu podle uživatelské identity, typu aplikace, apod.
- Funkce QoS až na úrovni jednotlivých toků (flow) s podporou LLQ
- Bezpečnostní pravidla mohou kromě adres a portů zohlednit i identitu uživatele
- Zohlednění kontextových informací o koncovém zařízení (typ, stav, spod.) a využití ve filtrech
- API rozhraní pro sdílení kontextových informací s dalšími systémy

- Možnost začlenit do SDN řešení – kontrolerem řízená infrastruktura (APIC)

4. POŽADAVKY NA PARAMETRY VPN

Nabízený VPN SW a HW musí splňovat následující vlastnosti:

- Plná kompatibilita se stávajícím VPN klientem nadřazené organizace (Ministerstvo zemědělství) – Cisco Anyconnect
- Podpora IPsec VPN
- IPsec VPN s podporou standardů: RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP), RFC 2409 - The Internet Key Exchange (IKE), RFC 2412 - OAKLEY Key Determination Protocol
- Podpora nového protokolu pro výměny klíčů IKEv2
- Podpora šifrovacích metod – minimálně: DES, 3DES, AES-128, AES-192, AES-256
- Podpora kontrolních mechanismů: MD5, SHA
- Podpora NextGen šifrovacích algoritmů: AES-GCM/GMAC-128, AES-GCM/GMAC-192, AES-GCM/GMAC-256
- Podpora komponentu Suite-B: SHA-2 mechanismu s metodami: SHA-256, SHA-384
- Podpora šifrovacích algoritmů eliptických křivek (součást Suite-B): ECDH, ECDSA
- Podpora SSL VPN
- Jednotný klient pro IPsec (IKEv2) i SSL VPN
- SSL VPN klient k dispozici pro všechny běžné desktopové OS: XP SP2+ 32-bit(x86) a 64-bit(x64), Vista (32-bit a 64-bit), Windows 7 (32-bit a 64-bit), Windows 10 (32-bit a 64-bit), MAC OS X(10.5, 10.6.x, 10.7.x, 10.8.x), Linux
- Distribuce VPN klient SW může poskytnout i jednotný 802.1X supplicant s autentizačními metodami: EAP-TLS, tunelovaný EAP-TLS, EAP-MSCHAPv2 nebo EAP-GTC, chráněný pomocí EAP-PEAP, EAP-FAST nebo EAP-TTLS
- VPN klient může být distribuovaný s 802.1X modulem řešící i efektivní machine/user autentizaci podle EAP-FAST (EAP Chaining)
- VPN klient má vlastní modul pro diagnózu a reporting pro řešení případných problémů
- SSL VPN klient je k dispozici pro moderní mobilní platformy na bázi Android a Apple iOS.
- Podpora TLS i DTLS pro SSL připojení
- Podpora současné autentizace koncové stanice i uživatele
- Podpora definice pravidel pro VPN přístup přímo prostředky FW a jejich automatická distribuce VPN připojeným klientům
- Jednotná správa VPN přístupů pro různé mobilní platformy a různé OS, včetně smart-phone a tabletů
- Možnost definovat specifická přístupová oprávnění (bezpečnostní politiky, ACL, atd.) podle identity nebo skupiny uživatele (např. v AD)
- Možnost dynamického přiřazení bezpečnostních politik (způsob a možnosti přístupu) podle aktuálního stavu koncové stanice: detekce instalovaných verzí bezpečnostního SW, detekce typu platformy a operačního systému
- Podpora autentizačních mechanismů: lokální databáze na FW, RADIUS, Lightweight Directory Access Protocol (LDAP)
- Podpora veřejných CA, včetně možnosti CA přímo na firewallu
- Možnost současné autentizace AAA a certifikátem

5. PŘÍSLUŠENSTVÍ

V rámci zakázky požadujeme dodávku originálního příslušenství výrobce, konkrétně rozhraní ke stávajícím aktivním prvkům Cisco Nexus. Požadované typy a počty jsou uvedeny v následující tabulce:

Počet	Typ	Určeno pro zařízení
4	GLC-T	Stávající zařízení Cisco Nexus

6. PŘÍLOHY

6.1. ZÁVAZNÉ TECHNICKÉ A FUNKČNÍ POŽADAVKY

Tabulky plnění závazných technických a funkčních požadavků zadavatele k vyplnění pro uchazeče.

Uchazeč vyplní tabulky v poli „hodnota nabízená uchazečem“ a v poli „odkaz na produktovou dokumentaci uchazeče“.

Pole ve sloupci „minimální požadovaná hodnota zadavatelem“ může obsahovat tyto údaje:

- **PODPORUJE** = je součástí zařízení; v takovém případě uchazeč splní požadavek zadavatele, pokud s ohledem na jeho nabídku uvede do sloupce „hodnota nabízená uchazečem“ údaj „PODPORUJE“
- **UMOŽŇUJE** = funkcionalitu lze v budoucnu aktivovat upgradem SW, licenčně nebo instalací dalšího HW přímo do zařízení; v takovém případě uchazeč splní požadavek zadavatele, pokud s ohledem na jeho nabídku uvede do sloupce „hodnota nabízená uchazečem“ údaj „UMOŽŇUJE“
- Jiný požadavek zadavatele na uvedení číselného údaje, rozmezí či podobně; v takovém případě uchazeč splní požadavek zadavatele, pokud s ohledem na jeho nabídku uvede do sloupce „hodnota nabízená uchazečem“ parametr dle požadavku zadavatele

Pole ve sloupci „odkaz na produktovou dokumentaci uchazeče“ uchazeč vyplní názvem či jinou jednoznačnou identifikací dokumentu, která takovou produktovou dokumentaci ve vztahu k tomu kterému parametru obsahuje (například produktový list, katalogový list, datasheet, část instalačního či jiného manuálu apod.).

Produktovou dokumentaci uchazeče (sadu dokumentů) souhrnně vloží pod doplněnou Tabulkou plnění závazných technických a funkčních požadavků zadavatele.

	Parametr/funkcionalita	minimální hodnota požadovaná zadavatelem	hodnota nabízená uchazečem	odkaz na produktovou dokumentaci uchazeče
VPN KONCENTRÁTOR				
1.	Formát zařízení - Appliance, 1RU	PODPORUJE		
2.	Minimální počet 1Gb 10/100/1000 BaseT Ethernet	1		

	pro management, standardně osazených			
3.	Minimální počet 1Gb SFP rozhraní portů pro data	4		
4.	Minimální počet 1Gb 10/100/1000 BaseT pro data	8		
5.	Počet současných VPN připojení	250		
6.	Možnost rozšíření současných VPN připojení na - min. 400	UMOŽŇUJE		
7.	Možnost rozšíření o funkce NextGen FW	UMOŽŇUJE		
8.	Možnost rozšíření o funkce NextGen IPS	UMOŽŇUJE		
9.	Podporovaný počet současně otevřených spojení NGFW s AVC	400 K		
10.	Rychlost vytváření nových spojení NGFW s AVC	22K		
11.	Propustnost stavového FW (top parametry)	6 Gbps		
12.	Propustnost NGIPS (top parametry)	2,2 Gbps		
13.	Propustnost aplikačního FW (next-gen FW) – (top parametry)	2,2 Gbps		
14.	Propustnost aplikačního FW + IPS (next-gen FW, IPS) - (top parametry)	2,2 Gbps		
15.	Hardwarové dešifrování TLS	1,5 Gbps		
16.	Propustnost IPSec VPN 1024B TCP	1,2 Gbps		
17.	Podpora L2 (transparentního) módu s podporou NAT a PAT	PODPORUJE		
18.	Podpora L3 (routovaného) módu s podporou NAT a PAT	PODPORUJE		

19.	Podpora stateful failover active/standby	PODPORUJE		
20.	Podpora min. 2 virtuálních bezpečnostních kontextů (virtuálních firewallů)	PODPORUJE		
21.	Dynamické směrování - podpora alespoň RIP, OSPF, BGP	PODPORUJE		
22.	Podpora IPv6 dynamického směrování – alespoň OSPFv3, BGP	PODPORUJE		
23.	Podpora Policy based Routing	PODPORUJE		
24.	Podpora kontroly paketů TCP provozu s ochranou před útoky jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod.	PODPORUJE		
25.	Podpora filtrace IPv4, IPv6	PODPORUJE		
26.	Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD	PODPORUJE		
27.	Podpora filtrace podle bezpečnostních skupinových rolí přiřazených na přístupových přepínačích	PODPORUJE		
28.	Podpora inspekce IPv6 provozu	PODPORUJE		
29.	Podpora NAT64 a DNS64	PODPORUJE		
30.	Možnost integrace cloudových bezpečnostních bran s transparentním směrováním určitého provozu na tyto prvky a zde prováděnou inspekci na škodlivý kód případně pro řízení přístupu podle uživatelské identity, typu aplikace, apod.	PODPORUJE		

31.	Funkce QoS až na úrovni jednotlivých toků (flow) s podporou LLQ	PODPORUJE		
32.	Bezpečnostní pravidla mohou kromě adres a portů zohlednit i identitu uživatele	PODPORUJE		
33.	Zohlednění kontextových informací o koncovém zařízení (typ, stav, spod.) a využití ve filtrech	PODPORUJE		
34.	API rozhraní pro sdílení kontextových informací s dalšími systémy	PODPORUJE		
35.	Možnost začlenit do SDN řešení – kontrolerem řízená infrastruktura (APIC)	PODPORUJE		
PARAMETRY VPN				
1.	Podpora IPSec VPN	PODPORUJE		
2.	IPsec VPN s podporou standardů: RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP), RFC 2409 - The Internet Key Exchange (IKE), RFC 2412 - OAKLEY Key Determination Protocol	PODPORUJE		
3.	Podpora nového protokolu pro výměny klíčů IKEv2	PODPORUJE		
4.	Podpora šifrovacích metod – minimálně: DES, 3DES, AES-128, AES-192, AES-256	PODPORUJE		
5.	Podpora kontrolních mechanismů: MD5, SHA	PODPORUJE		
6.	Podpora NextGen šifrovacích algoritmů: AES-GCM/GMAC-128, AES-GCM/GMAC-192, AES-GCM/GMAC-256	PODPORUJE		
7.	Podpora komponentu Suite-B: SHA-2 mechanismu s metodami: SHA-256, SHA-384	PODPORUJE		
8.	Podpora šifrovacích algoritmů elyptických křivek (součást Suite-B): ECDH, ECDSA	PODPORUJE		
9.	Podpora SSL VPN	PODPORUJE		
10.	Jednotný klient pro IPsec (IKEv2) i SSL VPN	PODPORUJE		

11.	SSL VPN klient k dispozici pro všechny běžné desktopové OS: XP SP2+ 32-bit(x86) a 64-bit(x64), Vista (32-bit a 64-bit), Windows 7 (32-bit a 64-bit), MAC OS X(10.5, 10.6.x, 10.7.x, 10.8.x), Linux	PODPORUJE		
12.	Distribuce VPN klient SW může poskytnout i jednotný 802.1X supplicant s autentizačními metodami: EAP-TLS, tunelovaný EAP-TLS, EAP-MSCHAPv2 nebo EAP-GTC, chráněný pomocí EAP-PEAP, EAP-FAST nebo EAP-TTLS	PODPORUJE		
13.	VPN klient může být distribuovaný s 802.1X modulem řešící i efektivní machine/user autentizaci podle EAP-FAST (EAP Chaining)	PODPORUJE		
14.	VPN klient má vlastní modul pro diagnózu a reporting pro řešení případných problémů	PODPORUJE		
15.	SSL VPN klient je k dispozici pro moderní mobilní platformy na bázi Android a Apple iOS.	PODPORUJE		
16.	Podpora TLS i DTLS pro SSL připojení	PODPORUJE		
17.	Podpora současné autentizace koncové stanice i uživatele	PODPORUJE		
18.	Podpora definice pravidel pro VPN přístup přímo prostředky FW a jejich automatická distribuce VPN připojeným klientům	PODPORUJE		
19.	Jednotná správa VPN přístupů pro různé mobilní platformy a různé OS, včetně smart-phone a tabletů	PODPORUJE		
20.	Možnost definovat specifická přístupová oprávnění (bezpečnostní politiky, ACL, atd.) podle identity nebo skupiny uživatele (např. v AD)	PODPORUJE		

21.	Možnost dynamického přiřazení bezpečnostních politik (způsob a možnosti přístupu) podle aktuálního stavu koncové stanice: detekce instalovaných verzí bezpečnostního SW, detekce typu platformy a operačního systému	PODPORUJE		
22.	Podpora autentizačních mechanismů: lokální databáze na FW, RADIUS, Lightweight Directory Access Protocol (LDAP)	PODPORUJE		
23.	Podpora veřejných CA, včetně možnosti CA přímo na firewallu	PODPORUJE		
24.	Možnost současné autentizace AAA a certifikátem	PODPORUJE		

Cenový přehled

Cena za služby

Zřízení služby

Číslo	Popis	MJ	Počet	Cena/MJ	Celkem
		ks	0	0	0
		ks	0	0	0
		ks	0	0	0
		ks	0	0	0
		ks	0	0	0

Provoz služby v délce trvání 3 roky

Číslo	Popis	MJ	Počet	Cena/MJ	Celkem
		ks	0	0	0
		ks	0	0	0
		ks	0	0	0
		ks	0	0	0

Změnové požadavky - celkem 6 MD

Číslo	Popis	MJ	Počet	Cena/MJ	Celkem
		MD	6	0	0

Souhrn nákladů

Dodávka					0
Cena celkem bez DPH					0
DPH 21%			0,21		0
Cena celkem s DPH					0