**Technická specifikace**

**OBSAH**

[1. Obecná funkční a technická specifikace 2](#_Toc56758750)

[2. PoPIS a požadované parametry služby 4](#_Toc56758751)

[3. požadavky na využívaný HW 5](#_Toc56758752)

[4. Požadavky na parametry VPN 7](#_Toc56758753)

[5. PŘÍSLUŠENSTVÍ 8](#_Toc56758754)

[6. přílohy 9](#_Toc56758755)

[6.1. Závazné technické a funkční požadavky 9](#_Toc56758756)

# 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 funkčnostech, 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 zařízeni tak, aby v případě závady na dodaných zařízeních, kterou není Uchazeč schopen sám odstranit, bylo možné eskalovat závadu přímo k výrobci zařízení. Zároveň je Uchazeč povinen zajistit Zadavateli přistup 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.

# 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

# 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 funkcionalita 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. 2virtuálních 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 připadně 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)

# Požadavky na parametry VPN

Nabízený VPN SW a HW musí splňovat následující vlastnosti:

* Plná kompatibilita se stávajícím VPN klientem nadřízené 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 mechanizmů: MD5, SHA
* Podpora NextGen šifrovacích algoritmů: AES-GCM/GMAC-128, AES-GCM/GMAC-192, AES-GCM/GMAC-256
* Podpora komponentu Suite-B: SHA-2 mechanizmu 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 mechanizmů: 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

# 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 |

# přílohy

## 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. 2
 | Formát zařízení - Appliance, 1RU | PODPORUJE |  |  |
| 1. 3.
 | Minimální počet 1Gb 10/100/1000 BaseT Ethernet pro management, standardně osazených | 1 |  |  |
| 1. 4.
 | Minimální počet 1Gb SFP rozhraní portů pro data | 4 |  |  |
| 1. 5.
 | Minimální počet 1Gb 10/100/1000 BaseT pro data | 8 |  |  |
| 1. 8.
 | Počet současných VPN připojení | 250 |  |  |
|  | Možnost rozšíření současných VPN připojení na - min. 400 | UMOŽŇUJE |  |  |
| 1. 38.
 | Možnost rozšíření o funkce NextGen FW  | UMOŽŇUJE |  |  |
| 1. 39.
 | Možnost rozšíření o funkce NextGen IPS  | UMOŽŇUJE |  |  |
| 1. 9.
 | Podporovaný počet současně otevřených spojení NGFW s AVC | 400 K |  |  |
| 1. 12.
 | Rychlost vytváření nových spojení NGFW s AVC | 22K |  |  |
| 1. 13.
 | Propustnost stavového FW (top parametry) | 6 Gbps |  |  |
| 1. 14.
 | Propustnost NGIPS (top parametry) | 2,2 Gbps |  |  |
| 1. 16.
 | Propustnost aplikačního FW (next-gen FW) – (top parametry) | 2,2 Gbps |  |  |
| 1. 17.
 | Propustnost aplikačního FW + IPS (next-gen FW, IPS) - (top parametry) | 2,2 Gbps |  |  |
| 1. 18.
 | Hardwarové dešifrování TLS | 1,5 Gbps |  |  |
|  | Propustnost IPSec VPN 1024B TCP | 1,2 Gbps |  |  |
| 1. 19.
 | Podpora L2 (transparentního) módu s podporou NAT a PAT | PODPORUJE |  |  |
| 1. 20.
 | Podpora L3 (routovaného) módu s podporou NAT a PAT | PODPORUJE |  |  |
| 1. 22.
 | Podpora stateful failover active/standby | PODPORUJE |  |  |
| 1. 25.
 | Podpora min. 2 virtuálních bezpečnostních kontextů (virtuálních firewallů) | PODPORUJE |  |  |
| 1. 26.
 | Dynamické směrování - podpora alespoň RIP, OSPF, BGP | PODPORUJE |  |  |
| 1. 27.
 | Podpora IPv6 dynamického směrování – alespoň OSPFv3, BGP | PODPORUJE |  |  |
| 1. 28.
 | Podpora Policy based Routing | PODPORUJE |  |  |
| 1. 29.
 | Podpora kontroly paketů TCP provozu s ochranou před útoky jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod. | PODPORUJE |  |  |
| 1. 30.
 | Podpora filtrace IPv4, IPv6 | PODPORUJE |  |  |
| 1. 32.
 | Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD | PODPORUJE |  |  |
| 1. 33.
 | Podpora filtrace podle bezpečnostních skupinových rolí přiřazených na přístupových přepínačích | PODPORUJE |  |  |
| 1. 34.
 | Podpora inspekce IPv6 provozu | PODPORUJE |  |  |
| 1. 35.
 | Podpora NAT64 a DNS64 | PODPORUJE |  |  |
| 1. 36.
 | Možnost integrace cloudových bezpečnostních bran s transparentním směrováním určitého provozu na tyto prvky a zde prováděnou inspekci na škodlivý kód připadně pro řízení přístupu podle uživatelské identity, typu aplikace, apod. | PODPORUJE |  |  |
| 1. 37.
 | Funkce QoS až na úrovni jednotlivých toků (flow) s podporou LLQ | PODPORUJE |  |  |
| 1. 40.
 | Bezpečnostní pravidla mohou kromě adres a portů zohlednit i identitu uživatele | PODPORUJE |  |  |
| 1. 41.
 | Zohlednění kontextových informací o koncovém zařízení (typ, stav, spod.) a využití ve filtrech | PODPORUJE |  |  |
| 1. 42.
 | API rozhraní pro sdílení kontextových informací s dalšími systémy | PODPORUJE |  |  |
| 1. 43.
 | 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 mechanizmů: 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 mechanizmu 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. | Podora 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 operačnícho systému | PODPORUJE |  |  |
| 22. | Podpora autentizačních mechanizmů: 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 |  |  |