Příloha č. 5 – Technická specifikace

1. Obsah

[1. Obsah 1](#_Toc174020715)

[2. Popis současného stavu 2](#_Toc174020716)

[3. Předmět plnění zakázky 2](#_Toc174020717)

[4. Požadavky na systém ADC 3](#_Toc174020718)

[4.1 Reverzní proxy a load balancer 3](#_Toc174020719)

[4.2 Aplikační proxy pro řízení přístupu k aplikacím 3](#_Toc174020720)

[4.2.1 Řízení přístupu ke službě OWA 3](#_Toc174020721)

[4.2.2 Řízení přístupu k ostatním službám MS Exchange 4](#_Toc174020722)

[4.3 Další požadavky na dodávané ADC řešení 4](#_Toc174020723)

[5. Systém MFA 4](#_Toc174020724)

[5.1 Další požadavky na dodávané MFA řešení 5](#_Toc174020725)

[6. Specifikace implementačního procesu a požadovaných produktů a výstupů 5](#_Toc174020726)

[7. Podpora provozu – řešení SLA incidentů 6](#_Toc174020727)

[7.1 Poskytnutí systémové podpory 6](#_Toc174020728)

[7.2 Systémová podpora výrobce na 36 měsíců v režimu minimálně 8x5 6](#_Toc174020729)

[7.3 Služby servisní podpory 6](#_Toc174020730)

[7.4 Řešení a kategorie vad 6](#_Toc174020731)

[8. Požadavky na drobné úpravy a rozvoj 7](#_Toc174020732)

[Příloha č. 1 8](#_Toc174020733)

[1. Tabulka technických parametrů systému ADC 8](#_Toc174020734)

[Příloha č. 2 14](#_Toc174020735)

[2. Tabulka technických parametrů systému MFA 14](#_Toc174020736)

1. Popis současného stavu

Zadavatel provozuje v současné době on-premise poštovní systém Microsoft Exchange Server 2016 (dále jen MS Exchange), který umožňuje uživatelům po autorizaci uživatelským přihlašovacím jménem a heslem přístup k jejich e-mailům, kalendářům, kontaktům a dalším funkcím z internetu a intranetu prostřednictvím těchto protokolů:

* Microsoft Outlook Web Access (dále jen OWA) – čistě webová služba poskytující obdobnou funkcionalitu jako plnohodnotný klient Microsoft Outlook, která je volně dostupná z libovolného webového prohlížeče, ať už uvnitř nebo vně sítě organizace, a zahrnuje webového e-mailového klienta, nástroj kalendáře, správce kontaktů a správce úkolů.
* Microsoft Exchange Web Services (dále jen EWS): Webové služby Exchange jsou rozhraním API, které umožňuje přístup a manipulaci s různými daty MS Exchange serverů, včetně e-mailů, kalendářů, kontaktů, úkolů a poznámek.
* Microsoft Exchange ActiveSync (dále jen EAS): Aktivní synchronizace je protokol, který umožňuje synchronizaci e-mailů, kalendářů, kontaktů a úkolů mezi MS Exchange servery a zařízeními s podporou EAS, jako jsou chytré telefony a tablety.
* Microsoft Messaging Application Programming Interface (dále jen MAPI): MAPI je rozhraní, které umožňuje komunikaci mezi Outlookem a MS Exchange servery prostřednictvím MAPI klienta a MAPI serveru. Tento protokol se používá zejména pro komplexnější funkce, jako je sdílení složek, správa kalendáře a offline přístup.

1. Předmět plnění zakázky

Zadavatel požaduje navýšení zabezpečení služeb MS Exchange následujícím způsobem:

1. **Implementace systému pro vícefaktorové ověřování a dodávka hardware (Položka bude smluvně řešena dílčí smlouvou č.1 na dobu 3 měsíců):**
   1. Hardwarového řešení systému, který bude zajišťovat funkce reverzní proxy, load balanceru a aplikační proxy pro řízení přístupu k aplikacím a službám – dále jen systém ADC (Application Delivery Controller). Tento systém ADC bude umístěn před vlastními servery MS Exchange a bude zajišťovat terminaci HTTPS provozu, autentizaci uživatelů a balancování provozu na cílové servery MS Exchange. Zadavatel požaduje řešení, které bude provozované v režimu vysoké dostupnosti.

V rámci dodávky Zadavatel požaduje, s ohledem na vysokou dostupnost systému ADC, dodat 2 kusy hardware zařízení ADC a to včetně 4 kusů SFP+ 10GBASE-SR Transceiverů.

Pro zařízení požadujeme služby typu:

* Podpora pro výměnu hardware v režimu Next-Business-Day minimálně 8x5,
* Produktovou podporu od výrobce v režimu minimálně 8x5.

Součástí dodávky předpokládáme dodání licence, pokud to je relevantní.

Detailní popis požadavků na systém je uveden v kapitole č. 4 této Technické specifikace.

V tomto bodě dodávky **Zadavatel nepřipouští licenční model typu subskripce.**

* 1. systému poskytujícího funkci dalšího faktoru pro autentizaci uživatelů k současnému způsobu ověření uživatele jménem a heslem – dále jen systém MFA (Multi-Factor Authentication). Detailní popis je uveden v kapitole č. 5 této Technické specifikace.

Součástí dodávku předpokládáme dodání licence a produktové podpory, pokud to je relevantní.

V tomto bodě dodávky **Zadavatel připouští licenční model typu subskripce.**

* 1. Rozšíření stávajícího webového samoobslužného systému ČRo (interní certifikační autorita ČRo) o vydávání konfiguračních profilů s certifikáty pro klientská zařízení Apple iOS

1. **Podpora provozu a rozvoj**
   1. Podpora provozu – řešení SLA incidentů **(Položka bude smluvně řešena dílčí smlouvou č.2 na dobu 36 měsíců).**
   2. Drobné úpravy, konfigurace, konzultace a rozvoj **(Položka bude smluvně řešena podle finančního rozsahu buď objednávkou anebo dílčí smlouvou).** Požadovaná doba podpory a rozvoje je Zadavatelem stanovena na 36 měsíců.
2. Požadavky na systém ADC

Zadavatel požaduje vytvořit návrh, dodání a implementaci systému ADC ve formě hardwarové appliance (zařízení). Zadavatel nepřipouští řešení provozované na virtualizační platformě nebo v cloudu. Systém ADC bude provozován v režimu vysoké dostupnosti – **dvojice hardware zařízení**. Systém ADC bude publikovat definované služby a oddělovat cílové on-premise MS Exchange servery od přistupujících uživatelů. Systém ADC bude realizovat funkci řízení aplikačního provozu a musí splňovat požadavky uvedené v příloze č. 1 této Technické specifikace (Technická specifikace systému ADC.)

* 1. Reverzní proxy a load balancer

Systém ADC bude koncipován jako redundantní a vysoce dostupný cluster, který může fungovat v režimu Active-Active nebo Active-Standby. Systém ADC bude odpovědný za monitoring, řízení a distribuci zátěže na cílové servery MS Exchange. Systém ADC bude také zajišťovat optimalizaci aplikačního provozu s cílem efektivně využívat zdroje aplikace. Systém ADC bude také zodpovědný za optimalizaci TCP provozu, HTTP kompresi a související optimalizaci aplikačního provozu. Systém bude umožňovat provoz alespoň dvou virtuálních ADC na jednom fyzickém zařízení, kdy jeden virtuální ADC bude sloužit pro odbavování provozu v externí DMZ a druhý ADC bude sloužit pro provoz ve vnitřní síti.

Implementaci politik a pravidel pro řízení aplikačního provozu předpokládáme minimálně v rozsahu:

* Zapojení a integrace v prostředí Zadavatele
* Vytvoření HA clusteru
* Monitoring zdraví aplikací a služeb
* TLS terminace, management TLS certifikátů
* Napojení na monitorovací a logovací nástroje
* Reverzní proxy s funkcí NAT44, případně NAT 46, NAT 64
* Optimalizace HTTP provozu (HTTP komprese)
* Zabezpečení HTTP provozu (cookies, manipulace s HTTP záhlavím apod.)
  1. Aplikační proxy pro řízení přístupu k aplikacím

Pro každý přístup k poštovní schránce ČRo z intranetu nebo prostřednictvím VPN bude vyžadováno pouze ověření uživatelským jménem a heslem. Naopak z internetu bude vyžadována jedna ze dvou doplňkových metod ověření a autorizace uživatelů využívající další faktor – MFA.

Popis požadovaného způsobu řízení přístupu k jednotlivým službám MS Exchange je uveden dále.

* + 1. Řízení přístupu ke službě OWA

Při přihlášení uživatele z internetu webovým protokolem OWA proběhne v první fázi ověření uživatele jménem a heslem proti on-premise Active Directory zadavatele, které zprostředkuje systém ADC. Jakmile uživatel projde úspěšně touto první kontrolou, systém ADC zprostředkuje ověření dalším faktorem (MFA autentizaci), kdy kontaktuje příslušnou službu MFA systému, která pro ověřovaného uživatele zašle push notifikaci na příslušné registrované mobilní zařízení s nainstalovanou autorizační aplikací MFA systému. Po schválení přihlášení prostřednictvím autorizační aplikace MFA systému na obrazovce mobilního zařízení uživatele, zajistí ADC balancování a šifrování provozu na cílové servery MS Exchange a předání přihlašovacích údajů prostřednictvím SSO (Single Sign On).

Pokud uživatel projde úspěšně celým ověřovacím procesem na ADC, bude provoz následně balancován na cílové MS Exchange servery, které uživateli zobrazí obsah poštovní schránky. Pokud ale v libovolné fázi ověřovacího procesu dojde k chybě nebo zadání nesprávných údajů, provoz nebude propuštěn na cílové Exchange servery a zobrazí se text s důvodem selhání a stručným popisem příčiny.

* + 1. Řízení přístupu k ostatním službám MS Exchange

Pro přihlášení z internetu prostřednictvím zbývajících protokolů MS Exchange (EWS, EAS, MAPI) z internetu bude v rámci TLS handshake výměny vyžadována autentizace osobním klientským certifikátem přihlašovaného uživatele, která v tomto případě představuje další faktor ověření koncového uživatele/zařízení a bude zprostředkováno ADC systémem. V případě úspěšného sestavení TLS spojení bude následovat ověření jménem a heslem proti on-premise Active Directory zadavatele, opět zprostředkované ADC systémem. V případě úspěšné autentizace bude uživateli povoleno spojení protokolem EWS, EAS nebo MAPI s poštovními servery MS Exchange Českého rozhlasu. ADC systém opět zajistí balancování a šifrování provozu na cílové servery MS Exchange a předání přihlašovacích údajů prostřednictvím SSO (Single Sign On)

V opačném případě ke spojení klientské poštovní aplikace s poštovními servery MS Exchange Českého rozhlasu nedojde.

* 1. Další požadavky na dodávané ADC řešení

Požadované řešení musí poskytovat služby reverzní proxy, load balanceru a aplikační proxy s dostatečným výkonem pro zajištění provozu stávajících i budoucích služeb a aplikací zadavatele.

Kromě toho musí systém ADC podporovat rozšíření o další funkce na základě dokoupení příslušné licence. Zejména se jedná o funkce webového aplikačního firewallu.

1. Systém MFA

Zadavatel požaduje návrh, dodání a implementaci systému MFA, který musí podporovat přímou integraci se systémem ADC prostřednictvím protokolů SAML nebo OAUTH.

Dále musí kromě jiného umožňovat distribuci a instalaci autorizační aplikace MFA systému na mobilní zařízení ověřovaných uživatelů a jejich propojení (registraci) se službou MFA systému. Je požadováno, aby průvodci zajišťující distribuci, instalaci a registraci používali jazykovou lokalizaci dle jazykového nastavení webového prohlížeče. MFA systém musí podporovat správu jednotlivých uživatelských účtů a k nim přiřazených mobilních zařízení a synchronizaci uživatelských účtů s on-premise službou Active Directory zadavatele.

V případě využití cloudového prostředí pro zajištění MFA je pro zajištění funkcionality ověřovacího mechanismu povoleno v cloudovém prostředí poskytovatele služby MFA systému využívat z on-premise Active Directory zadavatele pouze tyto položky: přihlašovací jméno a email uživatele, jméno a příjmení uživatele a telefonní číslo mobilního zařízení uživatele. Jiné položky z Active Directory zadavatele ani samotný obsah poštovní komunikace nebude povoleno zpracovávat na zařízeních poskytovatele mimo prostor budov Českého rozhlasu.

Webová aplikace pro správu i autorizační aplikace pro mobilní zařízení, které budou součástí MFA systému, musí splňovat požadavky na standardizované unifikované řešení již ověřené a užívané v celosvětovém měřítku. Zadavatel nepřipouští softwarové či aplikační řešení šité na míru.

Pokud u uživatele dojde k výměně mobilního zařízení za jiné, bude mít možnost samoobslužně takovou záměnu bezpečně provádět výhradně prostřednictvím zaslání SMS s údaji pro instalaci autorizační aplikace MFA systému a její propojení s autorizačními servery MFA systému na nové mobilní zařízení.

Dodaný systém MFA bude licencován na počet uživatelských účtů. Požadujeme licence pro 2000 ks uživatelů.

Systém MFA bude realizovat funkci vícenásobného ověření uživatele pomocí dalších faktorů a musí splňovat požadavky uvedené v příloze Technická specifikace systému MFA.

* 1. Další požadavky na dodávané MFA řešení

Zadavatel v současné době provozuje intranetovou webovou aplikaci pki.rozhlas.cz, která je používána k automatizovanému vydávání klientských certifikátů interní certifikační autority, založené na Microsoft Active Directory Certificate Services. Po ověření uživatelského jména a hesla zajistí tato Samoobsluha vydání klientského certifikátu podle předem schválené šablony certifikátu.

Zadavatel požaduje rozšíření stávající aplikace o funkcionalitu, která vedle klientských certifikátů umožní přihlášenému uživateli také dynamické vytvoření a stažení jeho osobního konfiguračního profilu pro zařízení s Apple iOS. Tento profil bude obsahovat konfiguraci pro zpřístupnění systému Microsoft Exchange v síti zadavatele, upravenou přesně pro potřeby příslušného koncového uživatele (předem vyplněné uživatelské jméno, adresy server MS Exchange a kompletní sadu certifikátů, včetně osobního certifikátu).

Pro plnění tohoto požadavku budou vítěznému Dodavateli poskytnuty zdrojové kódy ke stávající aplikaci.

1. Specifikace implementačního procesu a požadovaných produktů a výstupů
2. Dodavatel zpracuje na základě analytických schůzek dokument Analýza nasazení systémů ADC a MFA, jehož obsah bude následující:
   * Návrh a obecný popis architektury (High Level Design) dodávaného řešení,
   * popis terminologie, použité v dokumentu,
   * informace o stávajícím prostředí Zadavatele,
   * seznam aplikací, které budou ADC využívat,
   * popis změn v infrastruktuře.
3. Dodavatel zpracuje na základě analytických schůzek dokument Funkční specifikace, jehož obsah bude následující:
   * Vymezení rozsahu řešení,
   * popis funkčních vlastností požadovaného řízení přístupu k aplikacím pomocí systémů ADC a MFA,
   * popis úprav existujícího IT prostředí Zadavatele,
   * schéma řešení včetně integrace do prostředí Zadavatele,
   * popis cílové úpravy vnitřních procesů.
4. Dodavatel zpracuje dokument Low Level Design s následujícím obsahem:
   * Celkový návrh řešení ADC.
   * Typizované konfigurační šablony (soubor pravidel) pro řízení aplikačního provozu.
   * Jmennou konvenci pro ADC řešení.
   * Konfigurace ADC clusteru.
   * Konfigurace politik řízení aplikačního provozu pro aplikace.
   * Vytvoření a implementace standardů (soubor pravidel) pro SSL terminaci.
   * Vytvoření a implementace standardů (soubor pravidel) pro monitoring aplikací.
   * Vytvoření a implementace standardů (soubor pravidel) pro manipulaci s HTTP provozem (vkládání/odebíraní HTTP záhlaví apod.).
   * Vytvoření a implementace standardů pro optimalizaci TCP a HTTP provozu.
   * Konfigurace ostatních aspektů bezpečnostní politiky dle funkční specifikace.
   * Konfigurace MFA služby a integrace s řešením ADC.
   * Konfigurace politik pro řízení přístupu k aplikacím.
   * Konfigurace politik MFA služby.
   * Konfigurace synchronizace uživatelských účtů mezi MFA službou a on-premise Active Directory Zadavatele.
   * Customizace autentizačního procesu.
   * Konfigurace spolupracujících systémů (Active Directory, logovací systém, monitoring a další).
   * Doplnění funkcionality aplikace pki.rozhlas.cz.
5. Dodavatel připraví podrobné akceptační testy ADC a MFA systému včetně scénářů pro otestování vysoké dostupnosti.
6. Dodavatel provede pod dohledem Zadavatele akceptační testy ADC a MFA systému.
7. Dodavatel zpracuje Dokumentaci skutečného provedení, která bude obsahovat popis finálního nastavení jednotlivých komponent řešení a procesů.
8. Podpora provozu – řešení SLA incidentů

Uvedené parametry v této kapitole se týkají podpory systému ADC a systému MFA.

* 1. Poskytnutí systémové podpory
* Systémová podpora na 3 roky v režimu minimálně 8x5 a servisní podpora spojená s provozem systému ADC a systému MFA.
  1. Systémová podpora výrobce na 36 měsíců v režimu minimálně 8x5
* Podpora výrobce zahrnuje dostupnost:
  + Pravidelná údržba, upgrade, update operačního systému a bezpečnostních aktualizací.
  + Poskytování nových verzí a opravných balíčků systému ADC a systému MFA, dle aktuální technologické úrovně.
  + Profylaxe
  1. Služby servisní podpory
* Podpora konzultanta a technika, pro řešenou oblast podpory.
* Poskytování služby HelpDesk/ServiceDesk v režimu 24x7 včetně servisní technické podpory dle parametrů SLA sjednaných Smlouvou. Příjem požadavků přes email, telefonní linku případně webové rozhraní. Podpora také zahrnuje asistenci (telefonickou, osobní, pomocí vzdáleného přístupu) při vyhledávání a řešení funkčních problémů, doporučení, kdy je vhodná doba na údržbu hardwaru systému a asistenci při identifikaci softwarových chyb systému ADC a systému MFA po jejich výskytu a oznámení, a to v neomezeném rozsahu po dobu trvání podpory.
* Poskytování poradenských služeb prostřednictvím Helpdesk při řešení běžných provozních problémů správců informačních systémů v pracovní dobu, tj. v pracovní dny od 9:00 – 17:00 hodin.
* Technická a softwarová podpora zahrnuje povinnost poskytovatele poskytnout Zadavateli licence tzv. zdokonalení SW. Zdokonalení jsou definována jako změny původně dodaných softwarových produktů, které zlepšují jejich činnost nebo poskytují nové užitné vlastnosti.
* Zadavatel nemá žádnou povinnost akceptovat takováto zdokonalení a podle svého vlastního uvážení může instalaci takovýchto zdokonalení odmítnout. Naplňuje-li zdokonalení systému ADC a systému MFA znaky autorského díla, je poskytovatel povinen poskytnout Zadavateli licenci v minimálně stejném rozsahu, v jakém poskytl licenci k softwaru dle této smlouvy, popř. v rozsahu, v jakém ji objednatel již vlastní.
* Technická a softwarová podpora dále zahrnuje telefonické konzultace tak, aby bylo zajištěno správné užívání systému ADC a systému MFA.
  1. Řešení a kategorie vad
* Vady kategorie A (kritická):

Vady, které způsobují provozní problémy a neumožňují využívání systémů k účelu, jemuž jsou určeny. Jedná se o stav, kdy je znemožněna práce se systémem nebo jeho části a nelze použít alternativní postup, nebo je chování systému v rozporu s platnou legislativou ČR.

* Vady kategorie B (závažná):

Méně závažné vady a nedostatky, které funkčně nebo kapacitně omezují využívání systémů k účelu, ke kterému jsou určeny. Jedná se o stav, kdy je omezena práce se systémem nebo jeho částí, ale lze použít alternativní postup.

* Vady kategorie C (nízká):

Vady a nedostatky, které neomezují využívání systémů k účelu, ke kterému jsou určeny, ale nejsou v souladu se správnou funkcí systému. Není vážně omezena funkčnost systému nebo jeho části.

|  |  |  |  |
| --- | --- | --- | --- |
| **Garance** | **Vada kategorie A** | **Vada kategorie B** | **Vada kategorie C** |
| Prvotní reakce (response time) | Do 30 minut od okamžiku nahlášení vady. | Do 4 hodin od okamžiku nahlášení vady. | Do 8 pracovních hodin od okamžiku nahlášení vady. |
| Zprovoznění systému náhradním způsobem | Do 3 hodin od doby nahlášení vady. | Do 24 hodin od doby nahlášení vady. | Do 10 pracovních dnů od doby nahlášení vady. |
| Úplné odstranění závady | Do 5 dnů od doby nahlášení vady. | Do 10 dnů od doby nahlášení vady. | Do 20 pracovních dnů od doby nahlášení vady. |

1. Požadavky na drobné úpravy a rozvoj

V rámci rozvoje se jedná o další odborné služby, drobné úpravy, konfigurace, konzultace a rozvoj, kromě upgradu, update a bezpečnostních aktualizací, budou čerpány na základě skutečně provedené práce vyjádřené v člověkodnech. Dále se bude jednat o požadavky na rozšiřující úpravy stávajících vlastností a funkcionalit systému, úpravy vynucené změnou právních předpisů České republiky anebo změny technologického prostředí Českého rozhlasu. Ke každé úpravě nebo rozvojovému požadavku je Poskytovatel povinen vypracovat návrh řešení a dokumentaci.

Na následující tabulce je příklad služeb, které si zadavatel v rámci drobných úprav nebo rozvoje může zadat.

|  |  |
| --- | --- |
| **Služba** | **Popis** |
| Služba\_01 | Školení dle požadavků Zadavatele. |
| Služba\_02 | Konzultační podpora, drobné úpravy a rozvoj v rozsahu, ve kterém si Zadavatel objedná. |
| Služba\_03 | Součinnost při řešení systémových / integračních problémů systémů třetích stran. |
| Služba\_04 | Součinnost při implementaci systémů / integrací třetích stran. |
| Služba\_05 | Spolupráce při koordinaci třetích stran. |

# Příloha č. 1

1. Tabulka technických parametrů systému ADC

**Dodavatel vyplní u každého řádku žlutě vyznačená pole ve sloupci „Detailní popis naplnění pro nabízené řešení, případně odkaz na dokumentaci“. Dodavatel musí splnit veškeré níže uvedené parametry a vyplní všechny níže uvedená pole, přičemž nesplnění níže uvedených parametrů bude důvodem vyloučení ze zadávacího řízení.**

|  |  |
| --- | --- |
| **Požadovaná funkcionalita/vlastnost** | **Detailní popis naplnění pro nabízené řešení, případně odkaz na dokumentaci** |
| **Platforma** | |
| Nasazení redundantních HW zařízení ve funkci load-balancer s podporou autentizace uživatelů, SSL akcelerátoru a webového aplikačního firewallu. |  |
| Každé zařízení podporuje připojení minimálně 4 x 25/10 Gbps optickými SFP+ a 4x 10/1 Gbps metalickými porty. |  |
| Datová propustnost zařízení alespoň 40 Gbps či více na L4 a 28 Gbps či více na L7 |  |
| Minimální propustnost HTTP požadavků: 2.3 mil.za sekundu |  |
| Minimální propustnost L7 požadavků: 1.1 mil. za sekundu |  |
| Počet současných L4 spojení: 36 mil. |  |
| Offload – SW komprese – propustnost min. 18 Gbps |  |
| SSL akcelerace v HW |  |
| Počet SSL transakcí za sekundu min. 28000 (při použití 2K klíče) |  |
| Počet SSL transakcí za sekundu min. 12000 (při použití ECDSA P-256 klíče) |  |
| Celkový šifrovací výkon 18 Gbps |  |
| Virtualizace HW zdrojů |  |
| Nezávislé rozhraní pro management |  |
| HW podpora následujících funkcí: - SYN Cookie ochrana pro každou virtualizovanou službu - Základní DoS vektory, s možností nastavení každou virtualizovanou službu - SIP a DNS DoS vektory |  |
| Redundantní napájení |  |
| K dispozici jako autonomní box nebo ve formě šasi |  |
| Management: sériový port, GUI, příkazový řádek, iLO |  |
| **Operační systém** | |
| Full-Proxy architektura (plné oddělení klientského a serverového spojení) |  |
| Podpora IPv4 |  |
| Plná podpora IPv6, IPv4/IPv6 gateway (Podpora Ipv4 a Ipv6 na straně klienta i na straně serveru včetně všech možných kombinací) |  |
| Podpora externích šifrovacích karet pro SSL (HSM) |  |
| Podpora ověření certifikátů vydaných podřízenou CA (intermediate CA) |  |
| Podpora Spanning Tree Protokolu (STP) |  |
| Možnost přidat vlastní funkce pomocí skriptování – umožnění plnohodnotné manipulace a správy veškerého IP aplikačního provozu s cílem zachytit, zkontrolovat, transformovat a nasměrovat příchozí nebo odchozí provoz pomocí skriptovacího jazyka/syntaxe. |  |
| Podpora HTTP/2 |  |
| Podpora IPSec IKEv2 |  |
| Podpora konfigurace a správu zařízení přes REST API |  |
| Podpora SNMP (v1/v2c/v3) |  |
| Možnost aktivovat následující funkce na jedné HW platformě: - L4-7 loadbalancing - ICSA certifikovaný Web aplikační firewall - ICSA certifikovaný síťový firewall - Autorizace a autentizace aplikací, SSL VPN - DNS služby a DNS firewall |  |
| Možnost používat knihovny JavaScript třetích stran k úpravě a správě provozu |  |
| Podpora Active-Active a Active-Pasive módu |  |
| Režim HA, cluster: - Active/active, active/passive, transparentní přepínání bez přerušení session, včetně terminovaného SSL spojení.  - Možnost zařadit do HA clusteru min. 3 zařízení. Jednotlivá zařízení mohou být různých HW typů, nebo jako virtuální appliance. - Pokud jsou vyžadovány dodatečné licence, tak musí být součástí nabídky. |  |
| **Řízení provozu (load balancing)** | |
| Možnost připojení k monitorovacím nástrojům třetích stran prostřednictvím otevřeného API |  |
| Podpora REST API |  |
| Autentizace klientů přes LDAP/Radius |  |
| Povolení/zakázání ICMP pro VIP |  |
| Podpora vysokorychlostního granulárního logování / logování per aplikace / bez omezení výkonnosti zařízení |  |
| Podpora alespoň pro 19 metod rozvažování zátěže |  |
| Podpora filtrace paketů |  |
| Podpora ToS, QoS (marking/preservation/mimic) |  |
| Podpora SNMP (v1/v2c/v3) |  |
| Podpora rozvažování zátěže založené na poměrech (ratio) s CARP perzistencí |  |
| Podpora SSL certifikátů podepsaných SHA-2 algoritmem |  |
| Podpora práce s 4096-bit klíči |  |
| Současná podpora ECC a RSA certifikátu |  |
| Podpora pro TLS 1.2 a TLS 1.3 |  |
| Podpora ECC a DH šifer v HW |  |
| Podpora SSL Forward proxy |  |
| Stavové filtrovaní paketů (ACL) |  |
| Podpora vlastních skriptů pro monitorování zdraví a dostupnosti služeb |  |
| Podpora monitorování služeb na základě výkonu konkrétních hostů |  |
| TCP optimalizace síťových toků |  |
| Komprese a cachování specifických služeb |  |
| Zrcadlení SSL spojení (“connection”) a relací (“session”) napříč vícero uzly loadbalancerů – v případě výpadku jednoho zařízení si SSL spojení/relaci přebírá druhý uzel a SSL komunikace je zachována. |  |
| Podpora optimalizace dynamické velikosti TLS bloků (TLS record size) |  |
| **Řízení uživatelských přístupů** | |
| Podpora těchto autentizačních protokolů: - HTTTP basic - HTML form - Certificate - OCSP - CRLDP - Radius - LDAP - Active Directory - NTLM v1/v2 - Kerberos - SAML - SecurID - OAM - Tacacs+ - Local DB |  |
| Podpora Zero Trust konceptu |  |
| Import uživatelských identit IF-MAP |  |
| Podpora pro External logon page |  |
| AAA-server autentizace a vysoká dostupnost |  |
| OTP (generování a ověření) |  |
| Podpora CAPTCHA |  |
| Podpora Google recaptcha v2 |  |
| Autorizace: - Radius - LDAP - Active Directory |  |
| SAML: - SP - IdP |  |
| Modifikace SAML atributů |  |
| Podpora SAML 2.0 |  |
| SSO: - HTTP basic - HTML form - NTLM v1/v2 - Kerberos - SAML |  |
| Cachování uživatelských identit a SSO proxy |  |
| Podpora federace (SSO napříč různými doménami, např. on-prem a SaaS) |  |
| Podpora for Kerberos ticketingu |  |
| PCoIP proxy |  |
| RDP proxy |  |
| Patching: - HTML - JavaScript - CSS - Flash - Java |  |
| Jednotný URL portál |  |
| Uživatelský portál, kde se zobrazují aplikace podle přístupových práv |  |
| Podpora L7 ACL |  |
| Dynamický import ACL |  |
| Dynamická kontrola přístupů |  |
| Podpora ochrany a enkrypce „pracovniho“ prostoru („workspace“) |  |
| Network SSL VPN DTLS |  |
| Separátní SSL VPN tunel pro každou přístupnou aplikaci |  |
| Přístup pomocí Client-less |  |
| OS support: - Windows - MAC - Linux - iOS - Android |  |
| Podpora nativní MDM |  |
| Podpora Oauth 2.0 |  |
| Podpora OpenID Connect |  |
| Podpora IPSEC IKE v2 |  |
| Kontrola zabezpečení koncových bodů a posture kontrol |  |
| Podpora L7 ACL pro uživatelský přístup |  |
| Grafický editor pro správu řízení uživatelských přístupů |  |
| Podpora Microsoft ActiveSync a Outlook Anywhere s client-side NTLM |  |
| Zjednodušené řízení uživatelských přístupů pro Citrix XenApp a XenDesktop |  |
| Step-up autentizace |  |
| Podpora Ping Identity’s Policy Agent protocol |  |
| Podpora forward proxy chaining |  |
| Schopnost integrace se systémy AAA třetích stran pomocí volání API |  |
| Podpora ADFS proxy a ADFS-PIP protokolu |  |

Příloha č. 2

1. Tabulka technických parametrů systému MFA

**Dodavatel vyplní u každého řádku žlutě vyznačená pole ve sloupci „Detailní popis naplnění pro nabízené řešení, případně odkaz na dokumentaci“. Dodavatel musí splnit veškeré níže uvedené parametry a vyplní všechny níže uvedená pole, přičemž nesplnění níže uvedených parametrů bude důvodem vyloučení ze zadávacího řízení.**

|  |  |
| --- | --- |
| **Požadovaná funkcionalita/vlastnost** | **Popis naplnění pro nabízené řešení, případně odkaz na dokumentaci** |
| **Autentizace a enrollment** | |
| Podpora registrace více mobilních zařízení pro ověření uživatele |  |
| Podpora výběru preferovaného mobilního zařízení pro ověření uživatele |  |
| Podpora výběru alternativního mobilního zařízení (registrovaného danému uživateli), pokud není k dispozici jeho primární mobilní zařízení |  |
| Podpora ověření pomocí push notikace zaslané na mobilní zařízení |  |
| Push notifikace používají asymetrické klíče |  |
| Podpora ověření pomocí SMS zaslané na mobilní zařízení |  |
| Podpora mobilní zařízení těchto platforem: - iOS - Android |  |
| Podpor ověření pomocí hardwarových tokenů - tokeny Yubikeys - tokeny třetích stran kompatibilní se SAML / OAUTH |  |
| Podpora ověření pomocí jednorázového hesla (OTP) generovaného z mobilní aplikace |  |
| Podpora ověření pomocí bypass kódu poskytnutého administrátorem pro nouzové případy, kdy uživatel nemůže pro ověření použít své registrované mobilní zařízení |  |
| Podpora provisioning mobilní aplikace pomocí - SMS - QR kódu |  |
| Podpora IP whitelistingu pro jednotlivé uživatele, uživatelské skupiny nebo chráněné aplikace |  |
| Podpora IP whitelistingu v definovaných časových oknech |  |
| Podpora těchto autentizačních metod: - platform authenticator (Touch ID, Face ID, Android biometric) - roaming authenticator (FIDO security klíče – USB, Bluetooth, NFC) - push notifikace s verifikačním kódem - OTP v mobilní aplikaci - OTP přes SMS - phone callback - SAML / OAUTH hardwarové tokeny |  |
| Možnost vytváření vlastních konfigurovatelných politik pro blokování/upozornění na neaktuální software webového prohlížeče a poskytují možnost self-remediace |  |
| Možnost vytváření vlastních konfigurovatelných politik pro blokování nebo vyžadování vyšší úroveň ověření podle geolokace uživatele |  |
| Možnost vytváření vlastních konfigurovatelných politik pro blokování uživatelů s jailbroken/rooted mobilními zařízeními |  |
| Možnost vytváření vlastních konfigurovatelných politik pro zabránění pokusů o přístup z anonymních IP adres (TOR a I2P, HTTP/HTTPS proxy nebo anonymní VPN) |  |
| Možnost vytváření vlastních konfigurovatelných politik, které vyžadují aktivní zámek obrazovky na mobilních zařízeních při schvalování ověřování na těchto zařízeních |  |
| Možnost vytváření vlastních konfigurovatelných politik, které vyžadují použití otisku prstu/TouchID ověření na mobilních zařízeních při schvalování ověřování na těchto zařízeních |  |
| Možnost vytváření vlastních konfigurovatelných politik, které vyžadují plné šifrování disku na mobilních zařízeních při schvalování ověřování na těchto zařízeních |  |
| Možnost vytváření vlastních konfigurovatelných politik, které vyžadují aplikované aktuální bezpečnostní záplaty ověřovací aplikace na mobilních zařízeních při schvalování ověřování na těchto zařízeních |  |
| Možnost vytváření vlastních konfigurovatelných politik, které omezují dostupné metody ověřování |  |
| **Administrace** | |
| Výrobce garantuje SLA pro nabízené řešení |  |
| Zabezpečení a architektura řešení má audit od nezávislých třetích stran |  |
| Řešení založené na SaaS |  |
| Řešení je hostováno u poskytovatele služeb s certifikací PCI DSS, ISO 27001 a auditovaného podle SSAE 16 |  |
| Škálovatelné řešení z pohledu integrace s dalšími výrobci a počtu uživatelů |  |
| Řešení navržené s vysokou dostupností (HA) v rámci několika geografických lokalit a poskytovatelů služeb |  |
| Řešení používá asymetrickou kryptografii pro ověřování |  |
| Řešení neshromažďuje jakékoliv informace o uživatelích využitelné pro jejich identifikaci. |  |
| Řešení je nezávislé na primárním způsobu ověření |  |
| Pro vlastní ověření řešení nevyžaduje jakékoli dedikované on-premise servery |  |
| Podpora přímé integrace se systémy ADC pomocí protokolů SAML / OAUTH |  |
| Podpora synchronizace kontaktů s Microsoft Active Directory prostřednictvím LDAP protokolu |  |