PŘÍLOHA Č. 1

Technická specifikace

„ŘEŠENÍ PRO ŘÍZENÍ SÍTĚ, VIZUALIZACI A EVIDENCI ICT AKTIV“

Specifikace plnění

Předmětem plnění je dodávka, implementace a podpora provozu řešení IT bezpečnosti (technologie), které bude nástrojem pro bezpečnostní specialisty dodavatele, IT a bezpečnostní specialisty Zadavatele a které umožní spravovat IP adresní prostor organizace, vizualizovat a definovat vztahy IT aktiv a služeb organizace, získat přehled o dění v síti a řídit lokální a vzdálené přístupy známých i neznámých zařízení k síti.

Nedílnou součástí dodávky je následná podpora výrobce a dodavatele řešení po dobu 3 let.

Cena za implementační práce a školení bude nabídnuta jako celková cena.

V Ceně za Dodávku technologie bude obsažena i cena za služby spojené s počátečním naplněním systému informacemi o aktivech, a to v předpokládané pracnosti a rozsahu 145MD.

Cena za podporu výrobce pro období 3 let i cena za servisní podporu dodavatele pro období 3 let bude obsažena v ceně dodávky, přičemž předpokládaná pracnost servisní podporu dodavatele je v rozsahu 65 MD služeb dodavatele za rok (MD jsou převoditelné v rámci jednotlivých roků), tj. celkem 195MD za 3 roky, při očekávaných plánovaných změnách zadavatele v ICT infrastruktuře.

Řešení poskytne tyto funkcionality:

- Správa IP adresního plánu organizace
- Provoz a podpora služeb DNS a DHCP
- Řízení přístupu do sítě v rozsahu nástrojů:
  - Network Access Control (NAC)
  - SSL VPN
- Monitoring chování sítě pro úrovně L2, L3 a L4
- Vizualizace vztahů IT aktiv a provozovaných služeb organizace
- Evidence popisných informací IT aktiv pro podporu šetření bezpečnostních událostí
- Modelování logických vrstev pro definici vztahů klíčových procesů organizace na IT aktiva

Systém musí poskytovat jednotné integrované uživatelské webové rozhraní pro práci specialistů s dodávaným řešením (nevztahuje se na komponentu SSL VPN, která bude zakomponována do vnějšího perimetru sítě Zadavatele).

Plnění projektu bude obsahovat tyto fáze:

1) Dodávka technologie
2) Implementační práce
3) Podpora výrobce - Podpora výrobce na 3 roky
4) Servisní podpora - Servisní podpora spojená s provozem a údržbou řešení na 3 roky

Technické požadavky na požadované řešení

Řešení bude složeno z integrovaných komponent pro L2 monitoring sítě, správu IP adresního prostoru, systému řízení přístupových politik a vizibilitu chování síťové infrastruktury ve vazbě na provozované služby organizace.

Nástroj pro zajištění centrální správy IP adresního prostoru musí obsahovat integrované nástroje základních síťových služeb DNS a DHCP, L2 monitoring sítě a řízení přístupu do sítě (NAC - založený na standardu Radius) – s jednotnou uživatelskou správou přes GUI.

Komponenta pro vizualizaci chování síťových IT aktiv, katalog IT aktiv a nástroj pro definici a modelování služeb organizace bude integrovanou součástí nabízeného řešení, přičemž bude zajištěno vzájemné sdílení informací.

Požadavky na celý systém jsou rozděleny do několika částí, ale tvoří jeden funkční celek s unifikovaným a jednotným GUI.

Dodatečnou komponentou požadovaného řešení je modul pro řízení vzdálených přístupů. Tato komponenta bude zajišťovat funkci SSL VPN pro vzdálené přístupy k definovaným službám, aplikacím a částem sítě.

Obecné požadavky na systém

Definice požadavku	**Splněno Ano/Ne**	**Způsob splnění**
Řídící servery systému musí podporovat možnost provozu ve virtuálním prostředí (VMware)	Ano	Standardní podpora deploymentu prostředí Novicom appliancí do virtuálního prostředí

Definice požadavku	Splněno Ano/Ne	Způsob splnění
Výkonné servery ve formě fyzických appliancí musí využívat zabezpečený operační systém, být schopné poskytovat požadované funkce i v případě nedostupnosti síťového připojení k centrálnímu serveru a komunikovat s centrálním serverem přes zabezpečený protokol (zabezpečení integrity přenášených dat a obsahu přenášených dat před odposloucháváním na síti)	Ano	Díky využití vlastností technologické platformy (grid - SGP, komunikační protokol – SDP a zabezpečení appliance)
Systém appliancí musí podporovat možnost nasazení v on-line clusteru a podporovat vícenásobnou redundanci i přes různé lokality	Ano	Díky využití vlastností technologické platformy (grid - SGP, komunikační protokol – SDP a zabezpečení appliance)
Systém musí obsahovat samostatný systém pro centrální správu a nastavení appliancí	Ano	Grid manager pro centrální správu systémových konfigurací
Systém musí být schopen integrace se systémy pokročilé síťové analýzy (NBA) nebo SIEM	Ano	Aplikační integrací – zajištění přechodu mezi aplikacemi na detail IP/MAC, Datovou integrací – předáváním dat o provozu formou

Definice požadavku	Splněno Ano/Ne	Způsob splnění
		Syslog zpráv
Systém musí podporovat možnost napojení na SMS bránu pro odesílání autentizačních informací uživatelům	Ano	Standardní vlastnost BYOD modulu
GUI systému musí být k dispozici v českém a anglickém jazyce	Ano	Standardní možnost přepínání mezi ČJ a AJ

Systém pro adresní plánování

Definice požadavku	Splněno Ano/Ne	Způsob splnění
Je nástrojem pro návrh a definici IP adresního plánu s možností definice sítí, výběr konkrétní sítě a práce s ní	Ano	Standardní vlastnost DDI – části IPAMu
Systém musí podporovat v sítích možnost definice bloků adres, výběry dle bloků adres	Ano	Standardní vlastnost DDI – části IPAMu – podpora přiřazování IP adres z rezervací
Systém musí podporovat import MAC/IP adres z online monitoringu sítě, automatický výběr správné sítě pro importované adresy	Ano	Standardní vlastnost DDI – části IPAMu – vazba na L2 a DHCP monitoring

Systém musí podporovat import/export záznamů do/z adresního plánování v XML nebo CSV formátu	Ano	Standardní vlastnost DDI – části IPAMu
Systém musí podporovat automatické generování pravidel pro DHCP servery z adresního plánování	Ano	Standardní vlastnost DDI – části IPAMu - díky integraci s částí DNS
Systém musí podporovat automatické vytváření DNS záznamů z adresního plánování	Ano	Standardní vlastnost DDI – části IPAMu – díky integraci s částí DNS
Systém musí podporovat vytváření profilů dle sítí, po výběru profilu zobrazení a možnost práce pouze s IP adresami sítí daných profilem	Ano	Standardní vlastnost DDI – části IPAMu
Systém musí podporovat nástroj pro hromadné práce s definovanými skupinami zařízení a podporu krizového řízení	Ano	Standardní vlastnost DDI – části IPAMu

Systém pro monitoring sítě

Definice požadavku	**Splněno Ano/Ne**	**Způsob splnění**
Systém musí podporovat monitoring na L2 vrstvě - MAC a IP adres v reálném čase, včetně toho, na kterém fyzickém portu switche se daná MAC adresa nachází, pokud switch tuto možnost poskytuje (na kterém portu kterého switche je připojené zařízení s danou MAC adresou), včetně podpory historie	Ano	Standardní vlastnost DDI – části L2 monitoringu

Definice požadavku	Splněno Ano/Ne	Způsob splnění
Systém musí podporovat dostupnost monitoringu i v lokalitách, kde je přístup přes třetí vrstvu (routované lokality), data musí být online k dispozici přes uživatelské rozhraní na centrální lokalitě	Ano	Standardní vlastnost DDI – části L2 monitoringu
Systém musí podporovat online sledování a vyhodnocení monitoringu ve formě: povolená dvojice MAC-IP, zakázaná dvojice MAC-IP, nekorektní DHCP MAC-IP, neznámá MAC-IP	Ano	Standardní vlastnost DDI – části L2 monitoringu
Systém musí podporovat vypsání „mrtvých" MAC nebo IP adres (adresy, které se v síti nevyskytly např. půl roku), s možností přes uživatelské rozhraní provést vymazání z DHCP, DNS a Radius záznamů a vrácení příslušných IP adres do adresního plánování	Ano	Standardní vlastnost DDI – části L2 monitoringu – díky kontinuálnímu ARP monitoringu
Systém musí podporovat export odmonitorovaných záznamů do XML nebo CSV	Ano	Standardní vlastnost DDI – části L2 a DHCP monitoringu

Integrovaný DHCP server

Definice požadavku	Splněno Ano/Ne	Způsob splnění
Musí se jednat o distribuovaný DHCP systém s možností existence více DHCP serverů na stejné síti (redundance)	Ano	Standardní vlastnost DDI – části DHCP

Definice požadavku	Splněno Ano/Ne	Způsob splnění
Systém musí podporovat centrální řízení a zakládání pravidel	Ano	Standardní vlastnost DDI – je řízen z jednotného prostředí IPAMu
Systém musí podporovat redundanci řídícího serveru, nezávislé na lokalitě	Ano	Standardní vlastnost DDI – části DHCP, možnost samostatného fungování DHCP i při nedostupnosti primárního i záložního řídícího serveru
Systém musí podporovat uživatelsky definované DHCP volby	Ano	Standardní vlastnost DDI – části DHCP
Systém musí podporovat definice adresních skupin, k nim vázané DHCP volby	Ano	Standardní vlastnost DDI – části DHCP
Systém musí podporovat vytvoření DHCP pravidla s vazbou více MAC na více IP adres	Ano	Standardní vlastnost DDI – části DHCP
Systém musí podporovat možnost definice i statického záznamu (pro danou MAC není přidělovaná adresa DHCP serverem, pouze existuje záznam pro Radius server a monitoring, že daná	Ano	Standardní vlastnost DDI – je

Definice požadavku	Splněno Ano/Ne	Způsob splnění
MAC a IP adresa je na síti platná)		řízeno z IPAMu
Systém musí podporovat možnost existence DHCP záznamů jedné MAC adresy ve více různých sítích - v každé síti obdrží daná MAC adresa přesně svou IP adresu z rozsahu dané sítě - cestující uživatelé	Ano	Standardní vlastnost DDI – části DHCP
Systém musí podporovat automatické vytvoření/změna/smazání DHCP záznamu při operacích v adresním plánování	Ano	Standardní vlastnost DDI – části DHCP, díky řízení z jednotného prostředí IPAMu
Systém musí podporovat automatickou propagaci MAC adres z DHCP záznamů v uživatelsky definovaném formátu do Radius serverů pro realizaci dalších bezpečnostních mechanizmů prostřednictvím aktivních prvků sítě (podpora heterogenních aktivních prvků pro 802.1x autentizaci)	Ano	Standardní vlastnost DDI a NAC – díky integraci s aktivními prvky a NAC

Integrovaný DNS server

Definice požadavku	Splněno Ano/Ne	Způsob splnění
Systém musí podporovat centrální řízení a zakládání pravidel	Ano	Standardní vlastnost DDI – části DNS
Systém musí podporovat automatické vytváření A a PTR záznamů z adresního plánování	Ano	Standardní vlastnost DDI – části DNS

Definice požadavku	Splněno Ano/Ne	Způsob splnění
Systém musí podporovat automatické vytváření A a PTR záznamů z adresního Systém musí podporovat centrální řízení a zakládání pravidel	Ano	Standardní vlastnost DDI – části DNS
Centrální řídící server musí mít redundanci nezávislou na lokalitě	Ano	Standardní vlastnost DDI – části DNS, díky vlastnostem technologické platformy (SGP, SDP)
Systém musí podporovat možnost rozdělení zón na vnitřní a vnější pro stejnou zónu, definice vazby na vnitřní nebo vnější zónu dle IP adres (sítí) DNS klientů (klienti ve vnější sítí dostávají odpovědi pouze pro DNS záznamy z vnější zóny, klienti z vnitřní zóny dostávají DNS odpovědi pro vnitřní i vnější zónu)	Ano	Standardní vlastnost DDI – části DNS
Systém musí podporovat replikaci zvolených zónových souborů na podřízený DNS server	Ano	Standardní vlastnost DDI – části DNS
Systém musí podporovat automatického vytváření PTR reverzních záznamů při zakládání "A" záznamů	Ano	Standardní vlastnost DDI – části DNS
Systém musí nastavování oprávnění k zónovým souborům a SOA záznamům	Ano	Standardní vlastnost DDI – části DNS

Definice požadavku	Splněno Ano/Ne	Způsob splnění
Systém musí podporovat porovnání DNS z Adresního plánování s DNS záznamy na DNS serveru, včetně automatizovaného nástroje pro řešení rozdílů	Ano	Standardní vlastnost DDI – části DNS
Systém musí podporovat automatická kontrola existence reverzního záznamu k primárnímu A záznamu a naopak	Ano	Standardní vlastnost DDI – části DNS

Bezpečnostní část/NAC

Definice požadavku	Splněno Ano/Ne	Způsob splnění
Systém musí podporovat řízení přístupu do sítě s využitím 802.1x/MAC autentizace a následné Autorizace (dynamické přidělení VLAN)	Ano	Standardní vlastnost NAC
Systém musí podporovat automatické vytváření záznamů pro 802.1x a jejich automatická propagace do příslušných AAA zařízení z IPAMu	Ano	Standardní vlastnost NAC – díky integraci s DDI (IPAM)
Systém musí podporovat možnost definice politik přístupů pro neznámé zařízení	Ano	Standardní vlastnost NAC
Systém musí podporovat možnost definice politik přístupů pro důvěryhodná zařízení vyskytující se v jiné části sítě, než do které normálně patří (cestující uživatelé s Notebooky apod.). Pro tato zařízení definovat globální politiky bez nutnosti vytvářet exaktní pravidla pro každé jednotlivé zařízení. Např. důvěryhodná zařízení po úspěšné autentikaci jsou autorizovány (automaticky	Ano	Standardní vlastnost NAC – využívá integraci s DDI (DHCP) a L2 monitoringu

Definice požadavku	Splněno Ano/Ne	Způsob splnění
přemístěny) do VLAN definované globální politikou a následně automaticky zasíťovány.		
Systém musí podporovat schopnost definovat komplexní síťové politiky, kdy podle výsledku procesu autentizace je aplikována vybraná síťová politika – definované IP a DHCP parametry	Ano	Standardní vlastnost NAC – využívá integraci s DDI (DHCP) a L2 monitoringu
Systém musí podporovat krizové řízení – schopnost hromadné deaktivace síťové komunikace pro všechny zařízení mimo vyjmenovanou kritickou infrastrukturu organizace	Ano	Standardní vlastnost NAC
Systém musí podporovat uživatelské rozhraní s možností přidělování různých stupňů oprávnění. Audit musí být schopen zaznamenat minimálně kdo, kdy a jaké typy operací v systému prováděl	Ano	Standardní vlastnost NAC – systém využívá kombinací nastavení práce Rolí, uživatelů a ACL, s možným omezením pro vybrané části sítě
Systém musí podporovat sledování incidentů na síti s možností generování bezpečnostních reportů	Ano	Standardní vlastnost NAC – díky integraci s detailním reportingem (protokol)

Spolupráce s aktivními prvky

Definice požadavku	Splněno Ano/Ne	Způsob splnění
Systém musí podporovat automatické zálohování konfigurací aktivních prvků	Ano	Standardní vlastnost SIO modulu – bez ohledu na výrobce přes SSH/Telnet
Systém musí podporovat sledování výskytu MAC adres na portech s historií pro účely určení, kde se v daném čase vyskytuje nebo vyskytovala MAC adresa	Ano	Standardní vlastnost SIO modulu – vazba na L2 monitoring s kabelovou knihu
Systém musí podporovat automatické repository - informace o verzi firmware, typu zařízení, S/N apod.	Ano	Standardní vlastnost SIO modulu
Systém musí podporovat sledování využití portů síťových prvků v čase - detekce nepoužívaných	Ano	Standardní vlastnost SIO modulu
Systém musí podporovat heterogenního prostředí (podpora více výrobců síťových technologií - switchů)	Ano	Standardní vlastnost SIO modulu – podpora všech zařízení s možnou správou přes CLI a podporo Radius

BYOD část – (Wi-Fi sítě)

Definice požadavku	Splněno Ano/Ne	Způsob splnění
podporovaná veškerá funkcionalita rovněž pro mobilní zařízení s přístupem přes WiFi	Ano	Standardní vlastnost BYOD modulu – kompletní L2 montioring, DDI a NAC
podpora samoobslužného rozhraní pro automatizovanou IP správu nových zařízení v síti	Ano	Standardní vlastnost BYOD modulu – s možností napojení na SMS autentizaci
možnost vytváření recepčních zón pro zajištění přístupů návštěv (Guest zóna)	Ano	Standardní vlastnost BYOD modulu

Správa a vizualizace chování IT aktiv a vztahu na klíčové procesy organizace

Definice požadavku	Splněno Ano/Ne	Způsob splnění
Identifikace vztahů mezi objekty, které jsou součástí síťové komunikace	Ano	Řešení umožňuje vizualizaci objektů jak na úrovni infrastruktury (hierarchický model vztahů zóny > segmenty > IP

Definice požadavku	Splněno Ano/Ne	Způsob splnění
		adresy > porty), tak na úrovni síťové komunikace, kdy jsou zachyceny komunikace mezi vybranými IP adresami
Možnost pohybovat se ve vztazích hierarchickým způsobem od hlavních uzlů a síťových segmentů, přes IP adresy zařízení až po služby provozované na souvisejících portech (drill-down)	Ano	Požadovaný postup je možný s podporou pro vizualizaci síťových komunikací na vybraných portech. Drill-down probíhá procházením stromové struktury nebo vycentrováním prvku v rámci fulltext vyhledávání. Je možné vytvářet libovolně síťové segmenty, do nichž se budou IP adresy dynamicky zařazovat ihned po jejich detekci v rámci síťové

Definice požadavku	Splněno Ano/Ne	Způsob splnění
		komunikace.
Vizualizace hierarchických a komunikačních vztahů v infrastruktuře • Hierarchické zobrazení objektů síťové infrastruktury • Zobrazení komunikačních vztahů vybraných aktiv • Zobrazení vztahů IT aktiv a klíčových služeb organizace	Ano	Hierarchické zobrazení je možné v několika vizuálních módech (např. lineární, paprsčitý, hierarchický). Modul komunikace zobrazuje na místo statického stavu hierarchie infrastruktury rovněž pohled na dynamiku komunikací ve vybraném časovém rozmezí. S využitím tagování (štítkování IT aktiv) je možné rovněž vytvářet vazby na služby a procesy organizace
Upozorňování na změny v infrastruktuře, notifikace vlastníků aktiva na změny	Ano	Režim notifikace upozorňuje správce daného segmentu (zóny nebo dalšího objektu dle výběru)

Definice požadavku	Splněno Ano/Ne	Způsob splnění
		v případě, že dojde ke změně atributu některého hierarchicky podřízeného prvku. Změnou může být např. nová IP adresa v segmentu, nová služba na IP (nový port), změna popisu zařízení, přesun IP mezi segmenty a další.
Hledání v datech metodou full-text • IP, názvy, sítě, porty, štítky, vlastníci	Ano	Plná podpora full-text vyhledávání s možnostmi regulárních výrazů a složitějších dotazů s využitím operátorů AND, IN atp.
Využití autonomní sondy. Přenos metadat pro účely vizualizace je možný jak v téměř reálném čase, tak i dávkově. Základní informace o komunikačních vazbách (segment sítě, IP zdroj, IP cíl, cílová služba, tj. cílový komunikační port)	Ano	Pro sběr dat se využívají sondy komunikační (záznam komunikace mezi zařízeními) a assetové (pro

Definice požadavku	Splněno Ano/Ne	Způsob splnění
		párování hodnot MAC-IP a získání seznamu aktiv v síti). Je možné data do nástroje přenést načtením .pcap souboru pro offline vizualizaci.
Pro účely seskupování prvků podléhajících auditním požadavkům nebo interním směrnicím) je možné zařízení označovat dle libovolných tagů.	Ano	Podpora štítkování (privátní čili soukromé pro vlastníka daného objektu nebo systémové viditelné napříč systémem pro všechny uživatele).
IP adresa komunikující na další služby, včetně opačného zobrazení, tj. příchozí komunikace na služby provozované na portech tohoto aktiva	Ano	Nástroj podporuje 2 druhy zobrazení: 1) Po drill down IP adresy a výběru portu lze zobrazit, jaké další IP komunikují na tento port 2) Po výběru Ip adresy je možné

Definice požadavku	Splněno Ano/Ne	Způsob splnění
		zobrazit, na jaké další služby (porty) jiných IP adresa daná IP komunikuje.
Evidence popisných informací: • název aktiva, • typ aktiva, • identifikátor aktiva (dle typu aktiva, např. IP adresa, MAC, port…) • technický vlastník (správce), • čas prvního a posledního spatření aktiva • čas poslední zaznamenané komunikace • stav (nový, schválený, zamítnutý) • popis aktiva	Ano	Nástroj podporuje uváděné atributy. Popisné informace mohou být buď automaticky generované z dat sond, anebo manuálně plněné.
Přehledový katalogu IT aktiv: • Zařízení • MAC adresy • Síťové segmenty (VLAN) • IP adresy • Komunikační porty	Ano	Podpora pro tabulkový přehled nad aktuálním seznamem IT aktiv (IP adresy, porty, segmenty, zóny). Možnost řazení, hledání, exportu
Umožňuje porovnávat aktuální stav infrastruktury s vybraným časovým okamžikem v minulosti (např. zvýraznění nově identifikovaných aktiv v infrastruktuře)	Ano	Časové vyjádření stavu síťové infrastruktury a zároveň

Definice požadavku	Splněno Ano/Ne	Způsob splnění
		jednotlivých vztahů mezi aktivy je možná. Navíc je změnový stav vyjádřen alertem.
Úvodní portál (dashboard) s přehledem událostí, možnost aktivní práce s grafy (např. zoom na detail vybraných prvků) Upozorňování na nová neschválená zařízení umožní předcházet incidentům (alerting)	Ano	Plně přizpůsobitelný portál s možnostmi definic libovolných dotazů do dat. Načítání předpřipravených šablon z knihovny, podpora tabulkových a grafových přehledů.
Umožní vyhledat zařízení dle libovolných atributů	Ano	Podpora fulltext vyhledávání s možnostmi využití regulárních výrazů a operátorů.
Možnost práce řešení ve vysoké dostupnosti	Ano	Architektura řešení umožňuje, aby všechny komponenty řešení pracovaly v režimu vysoké dostupnosti.

Definice požadavku	Splněno Ano/Ne	Způsob splnění
Autentizace uživatelů, bezpečný přístup k aplikaci na základě vytvořených rolí a přidělování rolí uživatelům dle příslušných funkčních oblastí aplikace	Ano	Předdefinovaná oprávnění pro role Administrátor systému, IT/síťový administrátor, Bezpečnostní analytik, Architekt IS, Operátor bezpečnostního, monitoringu, Bezpečnostní manažer, Servisní manažer. Funkce vztažené k jednotlivým rolím jdou napříč systémem – využívání a přístup k modulům, funkcím jako schvalování nových zařízení a zejména možnosti editace/čtení.
Modelování vztahů mezi různými typy služeb a prostředků, jedná se především o modelování vztahů mezi business službami, aplikacemi, IT službami a IT prostředky	Ano	Grafická metoda vytváření vztahů mezi procesy (business službami),

Definice požadavku	Splněno Ano/Ne	Způsob splnění
		aplikacemi, IT službami a zařízeními.
Sledování stavu business služeb v rámci servisního modelu (které služby jsou provozované, jaký je jejich stav s ohledem na kybernetická rizika, na jakých prostředcích běží, popřípadě jak je optimalizovat v rámci celého servisního portfolia).	Ano	Možnost definování různých atributů u business služeb včetně hodnoty rizika. Vizualizace vztahů a závislostí služeb na IT prostředcích umožňuje lepší řízení dostupnosti služeb a rovněž zpřehledňuje prioritizaci servisních zásahů na IT prostředcích, na nichž jsou provozovány primární procesy a služby.
Monitoring ohrožení aktiv a služeb s definicí hodnoty akceptovatelného rizika služby.	Ano	Přidružené atributy k business službám umožňují evidovat bezpečnostním manažerům a servisním

Definice požadavku	Splněno Ano/Ne	Způsob splnění
		manažerům hodnoty akceptovatelného rizika a sledovat rizika na související infrastruktuře.
Automatizovaný neinvazivní (pasivní) sběr informací o komunikační infrastruktuře • Offline – zpracování informací z .pcap souboru (výstup TCPDUMP/WIRESHARK) • Online – přímé propojení se sítí (monitoring rozhraní – SPAN port)	Ano	Obě varianty jsou podporované.

Zabezpečený systém appliancí

Definice požadavku	Splněno Ano/Ne	Způsob splnění
zabezpečený systém appliancí, umožňují udržet konzistenci systémové prostředí po rebootu zařízení	Ano	Systém je uložený na zabezpečeném úložišti, který není možné pozměnit. Teprve po rebootu dojde k dekryptování a rozbalení systému do prostředí.
flexibilní instalace systémového nastavení appliancí s využitím nástroje centrální správy	Ano	appliance mají systém centrální správy a updatů –

Definice požadavku	Splněno Ano/Ne	Způsob splnění
		pomocí Grid Manageru
appliance musí mít dostatečné systémové zdroje pro zajištění provozu výše uvedeného funkčního rozsahu	Ano	Appliance jsou navrženy tak, aby umožnily současný běh všech požadovaných komponent, tj. monitoring (L2 a DHCP), základní síťové služby (DHCP/DNS a NAC) Výkonnější appliacne jsou připravené navíc pro sběr flow dat pro jejich vyhodnocení v části NVM.

Řízení vzdálených přístupů SSL VPN

Definice požadavku	Splněno Ano/Ne	Způsob splnění
Schopnost zakončit spojení typu SSL VPN pro přistupující uživatele	Ano	SSL VPN umožňuje zakončit spojení iniciované klientským VPN klientem, nebo

Definice požadavku	Splněno Ano/Ne	Způsob splnění
		spojený navázané z internetového prohlížeče.
Zprostředkování přístupu k chráněným částem sítě pomocí: • SSL VPN portál – publikace informací (reverzní PROXY) • SSL VPN portál – publikace aplikací • Plnohodnotného síťového spojení (VPN tunelování)	Ano	Všechny zmíněné metody jsou řešením podporované a lze je libovolně kombinovat pro stejné uživatele za využití stejné licence.
Možnost řízení přístupu uživatelů dle definovaných bezpečnostních pravidel	Ano	Granularita pravidel je možná na úroveň jednotlivých uživatelů, cílových serverů a konkrétních služeb.
Schopnost provádět autentizaci uživatelů formou více-faktorové autentizace	Ano	Uživatelská autentizace je možná dle standardních mechanismů: - Interní uživatelská databáze - PKI - Radius

Definice požadavku	Splněno Ano/Ne	Způsob splnění
		- SMS
Možnost integrace na SIEM	Ano	Plnohodnotná integrace se SIEM pomocí rozhraní OPSEC / LEA / Syslog

Požadavky na vykonání implementačních prací a podporu řešení

Dodavatel provede úplnou implementaci v datovém centru Magistrátu hl. m. Prahy. Zároveň je vyžadována následná podpora a správa při úpravě stávajících a tvorbě nových bezpečnostních politik a konfigurací.

Školení

Prodávající provede pro kupujícím určené osoby:

- Uživatelské školení, počet účastníků až 4;
- Administrátorské školení, počet účastníků až 4.

Definice rozsahu nasazení

Systém bude nasazen v následujícím rozsahu:

Systém pro monitoring sítě, správu adresního prostoru a systém řízení přístupových politik

Systém podporující redundanci a distribuovanost zajišťovaných služeb. Řídící servery systému budou provozovány ve virtuálním prostředí objednatele (VMware). Výkonné servery L2 monitoringu a provozu síťových služeb (DHCP/DNS/NAC) budou provozovány v hardwarových appliancích.

Implementace, je předpokládána v následujícím rozsahu:

- Celkové množství IP zařízení – do 5.000 IP zařízení
- 4 lokality (2 datová centra a 2 lokality)

Správa a vizualizace chování IT aktiv a vztahu na klíčové procesy organizace

Systém bude dodán v podobě licencí a potřebných komponent, bude provedena instalace do prostředí Zadavatele a dojde k integraci se síťovým prostředím určeným k sledování a automatickému sběru informací o IT aktivech. Tímto bude dosaženo úvodní fáze projektu, kdy řešení poskytuje své automatizované funkce a je možné jej využívat k orientaci v chráněném prostředí.

Řešení pro bezpečný vzdálený přístup

Prvek pro rozšíření bezpečnostní funkcionality perimetru o schopnost zakončit bezpečné vzdálené připojení uživatelů k poskytovaným cílům infrastruktury Zadavatele a to bez omezení počtu přistupujících uživatelů.

Zadavatel požaduje dodání patřičných komponent řešení, jeho licencí a implementaci do prostředí současného perimetru sítě Zadavatele.

Rozsah implementačních prací

1. implementace zahrnuje zprovoznění systému správy adresní a přístupové politiky v centrální lokalitě (i v případných vzdálených lokalitách – vzdáleně z centrály)
2. centrálně nasazený systém podporující redundanci a distribuovanost služeb L2 monitoringu, DHCP/DNS/NAC v hlavní a záložní lokalitě
3. vzdálené lokality budou řešeny distribuovaným modelem nasazených služeb L2 monitoringu a DHCP/DNS/NAC a zálohou poskytovanou z hlavní a záložní lokality
    a. celkové množství vzdálených lokalit – 2 lokality
4. implementace proběhne s využitím standardní implementační metodiky výrobce
5. provedení integrací na další systémy objednatele
    a. MS ActiveDirectory
    b. NBA – připravenost pro budoucí systém behaviorální analýzy postavený nad flow daty
6. provedení integrace s provozovaným systémem SIEM (Qradar)
7. poskytování dat ze všech lokalit o provozu DNS, DHCP a RADIUS
8. integrace s klíčovými částmi infrastruktury pomocí TAP/SPAN pro automatizovanou správu aktiv
9. provedení aplikační integrace umožňující operátorovi SIEMu provádět okamžitý incident response (use-case odpojení nebo izolace zařízení v systému správy adresní a přístupové politiky)

Rozsah poskytované servisní podpory

- standardní podpora dodaných technologií po dobu 36 měsíců, zahrnující službu poskytování nových verzí systému a telefonního hot-line pro hlášení servisních požadavků v pracovní době 9.00 až 17.00,
- záruka na technické zařízení po dobu 36 měsíců
- rozšířená podpora spočívající v poskytování technických a aplikačních konzultací na vyžádání v po dobu 36 měsíců. Rozsah poskytované rozšířené podpory je 16 hodin měsíčně s garancí zahájení poskytování konzultací do 8 pracovních hodin, služba poskytována v pracovní dobu: pondělí až pátek – 9.00 až -17.00.
- Podpora tvorby logických prvků do nástroje pro vizualizaci vztahů IT aktiv a klíčových služeb organizace, podpora evidence klíčových popisných informací ke sledovaným IT aktivům a modelování vztahů IT aktiv a služeb organizace. Služba poskytována v pracovní dobu: pondělí až pátek – 9.00 až -17.00.