Příloha č. 1 kupní smlouvy
-
Technická specifikace předmětu plnění

1. Předmět výběrové řízení

Předmětem výběrového řízení je nákup pěti (5) kusů NG firewallu geocluster hardware appliance. Zadavatel požaduje podporu řešení v délce tří let v režimu 24x7 včetně zahrnutí aktualizací všech níže zmíněných bezpečnostních funkcí, aktualizaci operačního systému, technickou podporu a RMA.

2. Požadavky na hw appliance

Požadovaná konfigurace služeb a funkcí:

- Konzolový a management port.
- Podpora VLAN, podpora LACP.
- Virtualizace v HW/OS pro min. 10 virtuálních kontextů, s možností definování maximálních povolených zdrojů (Při překročení přidělených zdrojů bude ovlivněn pouze daný virtuální kontext).
- Podpora izolovaných administrátorských účtů pro jednotlivé virtuální kontexty.
- Možnost funkce v L2 režimu (transparentní inspekční režim) nebo v L3 režimu (router).
- Funkce SSL VPN v tunelovém režimu a režimu přístupu ke vnitřním službám přes webovou proxy s podporou aplikací RDP, SSH a HTTP; součástí nabídky VPN klient pro neomezený počet uživatelů, podpora dvoufaktorové autentizace uživatelů; jsou-li funkce SSL VPN licencovány na počet uživatelů, součástí nabídky v současné době musí být licence pro min. 500 uživatelů.
- Požadované bezpečností funkce (pokryté licencí): antivirová inspekce, kategorizace webu/web filtering, L7 analýza aplikací, detekce narušení (IPS/IDS), ochrana před únikem citlivých dat (DLP), DNS filtr, vše s podporou výrobce na 3 roky.
- Podpora antivirové inspekce: signatury automaticky aktualizované výrobcem, s možností rozšíření o inspekci tzv. sandbox technikou, ve formě cloud služby, s možností rozšíření o lokální VM/HW appliance.
- Funkce rozlišování aplikací pomocí L7 charakteristiky, možnost definovat vlastní aplikace pomocí signatur, automatická aktualizace od výrobce.
- Funkce kategorizace webových stránek a web filtering s podporou českých a slovenských stránek s podporou minimálně 60 kategorií.
- Funkce ochrany úniku citlivých dat (DLP).
- Funkce Loadbalancingu provozu.
- Funkce transparentního ověřování uživatelů komunikujících skrz NGFW pomocí domény (MS Active
- Funkce ověřování uživatelů pomocí LDAP, RADIUS, SSO, Kerberos... s možností práce se skupinami uživatelů.
- Funkce automatického auditu vlastní konfigurace firewallu s ohledem na detekci kritických zranitelností, chyb v konfiguraci bezpečnostní politiky a generování série doporučovaných akcí vedoucí k nápravě a posílení úrovně zabezpečení sítě; součástí funkce musí být pravidelná aktualizace auditních pravidel výrobcem
- Funkce GEO IP databáze, možnosti definování politiky pomocí geolokační databáze.
- Funkce reputační databáze IP adress a blokace známých botnet C&C center.
- Funkce překladu IP adres (NAT).

- Integrovaná podpora autentizace vlastním jednorázovým heslem (OTP) s aplikací pro mobilní platformy iPhone a Android.
- Nabízení řešení musí být plně kompatibilním s OTP generátorem, který již zadavatel provozuje. Provozovaný typ generátoru je Fortitoken FT200.
- Musí splňovat požadavky na logování podle vyhlášky 316/2014 §21 jako kritický informační systém. Pro logování podporovat Syslog protokol s podporou TCP a TLS (podle RFC 5425) s možností volby cíle pro logy.
- Logy musí být ve strukturovaném, zdokumentovaném tvaru.
- Funkce hloubkové analýzy provozu (packet capture) pro případ řešení problému v provozu (Debug mod).
- Funkce přeposílání dešifrovaného provozu, který prošel SSL inspekcí na externí IP adresu.
- FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici.
- Funkce explicitní proxy přímo na firewallu (včetně autentizace uživatelů, proxy-chainingu, podpora inspekčních mechanismů a bezpečnostních funkcí (AV, IPS, Webfilter) s kapacitou pro 1000 uživatelů.
- Možnost definice FW pravidel v tzv. NGFW režimu (tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace (definované v rámci funkce rozlišování aplikací dle L7 charakteru (AppControl), nikoliv pouhý TCP/UDP port), resp. kategorie URL filteringu (nikoliv jako AppControl resp. URL filtering profil aplikovaný na dané pravidlo).
- Funkce reverzní proxy (publikování webových serverů) s funkcionalitou WAF (detekce Cross Site Scripting, SQL injection, generických útoků, detekce Information Disclosure a známých exploitů, detekce Bad Botů, možnost definice a omezení parametrů (Constraint) u tolerované délky hlavičky či těla, počtu URL parametrů, Cookie), podpora manipulace s HTTP metodami (get/put/post/head/connect/options) včetně funkce Load Balancingu (round robin, static, váha, nejkratší odezva, nejmenší počet spojení) a funkce SSL offloadingu (včetně definice použitého certifikátu).
- Podpora režimu redundatní IPSEC VPN se statickým routingem (bez nutnosti použití dynamického routingu).
- Podpora vytváření virtuálních sítových propojů mezi jednotlivými virtuálními kontexty firewallu a to včetně akcelerace HW moduly.
- Pracují v režimu vysoké dostupnosti v módu Active-Active/Active-Pasive/Cluster.
- Redundantní napájení s funkcí Hotswap. Součástí nabídky musí být i plně kompatibilní náhradní zdroj s nabízenou hw appliance.
- Min. 2x 10 GE SFP+ rozhraní na každém firewallu. Součástí nabídky musí být 2x optický SPF+ typu LR modul plně kompatibilní s nabízenou hw appliance.
- Min. 8x 1 GE SFP rozhraní na každém firewallu. Součástí nabídky musí být 4x optický SPF typu SX modul plně kompatibilní s nabízenou hw appliance.
- Min. 8x 1 GE RJ45 rozhraní na každém firewallu.
- Propustnost firewallu min. 22 Gbps pro IPv4 (UDP pakety 64 B) i IPv6 (UDP pakety 86B).
- Počet spojení na firewallu minimálně 8 miliónů celkem v jeden okamžik, min. 300 000 nových spojení za sekundu.
- Propustnost IPSEC VPN při použití algoritmu AES256-SHA256 min. 20 Gbps.
- Propustnost funkce IPS min. 11 Gbps.
- Propustnost funkcí next generation firewallingu (stavový firewall, IPS, analýza aplikací) min. 5 Gbps (reálná hodnota, měřeno na běžném provozu – real world traffic).
- Podpora funkce inspekce SSL provozu s propustností min. 6.8 Gbps v rámci jedné lokality.
- Latence firewallu < 3 µs (udp pakety 64 B).
- Řešení stavového firewallu a celého šifrování na HW modulech (hlavní šifrování a dešifrování provádí zabudované nebo dodané HW moduly).

- Splňovat minimální požadavky na všechny kryptografické funkcionality podle zákona 181/2014 a jeho vyhlášek.
- Montáž do 19" racku.
- Umístění výrobce zařízení v NSS LABS NEXT GENERATION FIREWALL testu v roce 2017 a 2018 nadprůměrně v obou posuzovaných parametrech. Test musel proběhnout podle metodiky NSS LABS popsané na: https://www.nsslabs.com/security-test/nss-labs-test-policies/
- Dodavatel garantuje demonstraci dosažení minimálních výkonových parametrů propustností vybraných funkcí na vyžádání, pro tyto účely zároveň zapůjčí i testovací platformu.

Požadavky na software a firmware

- Aktualizace firmware, ovladačů a dalšího software, musí být volně dostupná na stránkách výrobce. Popřípadě na stránkách výrobce po registraci nebo přihlášení.
- Dodaný hardware musí být registrován přímo na Národní úřad pro kybernetickou a infomační bezpečnost nikoliv na dodavatele nebo subdodavatele.
- Dodavatel musí být autorizovaným partnerem výrobce nabízeného HW oprávněným dodat a implementovat předmět VZ .

3. Dodatečné požadavky

Nabízené řešení musí splňovat tyto požadavky:

- Dodavatel je povinen do nabídky zahrnout veškerou kabeláž potřebnou pro instalaci navrhovaných zařízení a veškerou síťovou kabeláž nutnou pro připojení jednotlivých instalovaných zařízení do LAN. Ethernet kabeláž minimálně Cat6 . Optické kabely musí být typu 62,5/125mikrometru kategorie OM3.
- Veškerá nabízená zařízení musí být dodaná ve verzi pro instalaci do standardních 19“ skříňových rozvaděčů hloubky 1000 mm s čtvercovými otvory (square hole rack) a to včetně všech potřebných rack mount kitů a dalšího montážního příslušenství. Skříňové rozvaděče, UPS a PDU s C13 zástrčkami v jednotlivých rozvaděčích zajistí zadavatel.
- Součástí cenové nabídky je veškerý HW a SW, i ten který nebyl v této zadávací dokumentaci specifikován a je potřebný ke zprovoznění nabízeného řešení.
- Veškeré přístupové údaje (login, hesla, atd.) v nabízeném řešení musí být zadavatelem měnitelné.
- Všechna zařízení (moduly, atd.) musí být zcela spravovatelné z vnitřní sítě zadavatele, nebude tedy potřeba zřízení VPN a jiných spojení určených pro správu směrem od dodavatele.

4. Požadavky na implementační služby

Součástí nabízeného řešení musí být veškeré implementační služby pro veškeré nabízené komponenty minimálně v následujícím:

- Doprava veškerého hardware na adresu Mučednická 1125/31 Brno-Žabovřesky.
- Zprovoznění celého řešení v souladu s požadavky této VZ včetně uzpůsobení konfigurace na danou LAN a SAN síť.
- Projektový management po celou dobu instalace.
- Vypracování dokumentace popisující předaný stav řešení.
- Dodatečných 5 člověkodnů na předem nespecifikované práce a konzultace.
- Součástí nabídkové ceny musí být instalace zařízení do racků, propojení LAN kabeláže, oživení a zpřístupnění management rozhraní.

- Školení pracovníků zadavatele na administraci všech dodaných komponent v rozsahu minimálně 1 den pro 2 osoby.
- Součástí dodávky bude veškerá optická a metalická kabeláž potřebná pro vznik funkčního celku.
- Instalace a konfigurace všech technologií budou provedeny v souladu s platnými technickými a právními předpisy v České republice a Evropské unii a doporučením výrobců.
- Veškeré instalační a implementační služby musí být prováděny prostřednictvím specialistů s komunikací v českém jazyce.

5. Požadavky na dodavatele

Dodavatel bude certifikovaným partnerem výrobce nabízené technologie - doloží kopií certifikátu, jeden člen realizačního týmu bude mít min. jednu zkušenost s implementací nabízené technologie v HA řešení – doloží čestným prohlášením s uvedením odběratele daného řešení včetně uvedení kontaktní osoby pro ověření této reference, uvedený člen realizačního týmu bude zároveň proškolen výrobcem v oblasti implementace dodávané technologie – doloží kopií certifikátu nebo potvrzením o absolvování školení.