Technická specifikace předmětu veřejné zakázky malého rozsahu „Nákup síťových prvků“

Prvky s funkcionalitou NAT/FW/IDS/IPS

Požadujeme dva prvky typu NGFW zapojený v režimu vysoké dostupnosti, dle níže uvedené specifikace. Nové firewall řešení bude využito pro více účelů a z toho důvodu klademe požadavky na výkonnost a možnosti práce s virtuálními kontexty.
Dodávka musí obsahovat všechny HW komponenty a licence na dobu 5 let pro všechny požadované bezpečnostní a síťové funkce. Pokud navrhované řešení využívá licence pro škálování výkonnosti, tak součástí nabídky musí být licence splňující všechny výkonové požadavky od dodávky po dobu minimálně 5 let. Pokud dosažení požadované výkonnosti vyžaduje doplnění řešení a jakýkoliv typ HW akceleračního modulu, tak tento modul musí být součástí dodávky.
Součástí dodávky také musí být přímá technická podpora výrobce (zadavatel musí mít přímý kontakt na centrum technické podpory výrobce) na stejnou dobu, a to v režimu 24x7. Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány.
Zadavatel má v plánu sestavit cluster dvou zařízení v jedné své lokalitě a ve druhé lokalitě mít jedno toto samostatné zařízení, přičemž požaduje u těchto dvou geograficky oddělených instalací oddělenou správu. Zároveň je požadována on-line synchronizace stavu spojení bezi těmito dvěma instalacemi tak, aby bylo možné provozovat toto zapojení v režimu active-active, popř. selektivně směrovat síťový IPv4/IPv6 provoz pomoci dynamických směrovacích protokolů (BPG, OSPF).

Požadavky na dodaná zařízení

Dodavatel poskytne Zadavateli po dobu trvání podpory všechny relevantní SW vydání a verze SW nabízené výrobcem tak, aby dodané řešení vyhovovalo zadání Zadavatele a fungovalo bez závad. Dodavatel se zároveň zavazuje informovat Zadavatele o nových programových verzích a funkčnostech, které mohou rozšiřovat dodané řešení způsobem, který Zadavatel shledá ve shodě s potřebami dalšího rozvoje dodaného řešení. Dodavatel se dále zavazuje získat potřebné SW produkty legálním způsobem za podmínek stanovených výrobcem zařízení.
Dodavatel je povinen řádným způsobem uzavřít dohodu o podpoře s výrobcem zařízení tak, aby v případě závady na dodaných zařízeních, kterou není Dodavatel schopen sám odstranit, bylo možné tuto závadu eskalovat přímo k výrobci zařízení. Zároveň je Dodavatel povinen zajistit Zadavateli přístup k dokumentaci výrobce zařízení a znalostní bázi, kterou výrobce v rámci své podpory poskytuje.
Dodavatel je povinen zajistit dostupnost náhradních dílů od výrobce a dostupnost vlastní podpory pro dodané řešení za podmínek specifikovaných Zadavatelem.
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. Rozsah školení je 2x8h, školení bude probíhat v sídle Zadavatele na adrese Na Jízdárně 2824/2, 702 00 Ostrava.

Dodavatel je povinen s dodávkou doložit oficiální potvrzení zastoupení výrobce o určení dodávaného HW (seznamu sériových čísel dodávaných zařízení) pro český trh a koncového zákazníka, pokud o to Zadavatel požádá. Zadavatel požaduje originální a nové zařízení, licencované ve jménu zákazníka tak, aby bylo možné eskalovat případné závady na technickou podporu výrobce.
Zadavatel požaduje dodat taková zařízení, u kterých je výrobcem deklarovaná produktová podpora a stabilita minimálně 5 let od data dodávky, a to včetně nových programových verzí, údržby a rozvoje programového vybavení a možnosti prodloužení HW i SW podpory u výrobce.

Požadavky na záruku

Po celou dobu záruky v délce trvání minimálně 60 měsíců bude servisní podpora zahrnovat minimálně:

- výměnu vadného dílu nebo zařízení v místě plnění do následujícího pracovního dne po ohlášení závady (8x5xNBD),
- nárok na bezplatnou instalaci všech nových verzí firmware v rozsahu dodané licence,
- nárok na přímou podporu výrobce v případě softwarových nebo hardwarových závad, jejichž řešení nebude v silách dodavatele.

Minimální výkonové požadavky

Požadované výkonové parametry je nutné doložit oficiálním produktovým listem výrobce. Dodavatel garantuje demonstraci dosažení minimálních výkonových parametrů propustností vybraných funkcí na vyžádání. Zadavatel si zároveň vyhrazuje právo na otestování výkonových parametrů, stejně jako vybraných bezpečnostních funkcí.

Technická specifikace

HW požadavky
HW appliance (VM appliance ani software řešení není akceptovatelné)
Podpora režimu vysoké dostupnosti minimálně jako active/active a active/passive, cluster o dvou fyzických zařízeních
Velikost 1 RU
Podpora duálního napájení (redundantní zdroj)
Minimálně 4x 10 GbE SFP+ sítová rozhraní
Minimálně 8x 1 GbE SFP síťová rozhraní
Minimálně 16x 1 GbE RJ45 síťová rozhraní
Management rozhraní 2x 1 GbE RJ45 a sériový konzolový port
Integrovaný pevný disk SSD s celkovou kapacitou min. 480 GB pro lokální úložiště provozních informací (logů)
Výkonové požadavky
Minimální propustnost firewallu pro IPv4 i IPv6 provoz 25 Gbps (měřeno na UDP komunikaci o paketech s velikostí 512 B).
Počet současně navázaných spojení firewallu min. 3 000 000, počet nových spojení za sekundu min. 250 000
Celková propustnost IPSEC VPN min. 12 Gbps
Propustnost SSL VPN min. 2 Gbps
Propustnost funkce SSL inspekce min 4 Gbps

Počet CPS u spojení kontrolovaných pomocí SSL inspekce min. 3500 (spojení za sekundu)
Propustnost funkce IPS min. 5 Gbps (reálná hodnota, měřeno na běžném provozu – real world traffic, včetně logování)
Propustnost funkcí next generation firewallingu (stavový firewall, IPS, analýza aplikací) min. 3 Gbps (reálná hodnota, měřeno na běžném provozu – real world traffic)
Propustnost funkcí ochrany před hrozbami (stavový firewall, IPS, analýza aplikací, ochrana před škodlivým kódem) min. 3 Gbps (reálná hodnota, měřeno na běžném provozu – real world traffic)
Udávaná latence firewallu (udp provoz) max. 4,8 µs
Min. počet současně připojených uživatelů SSL VPN 500
Min. počet site-to-site IPSEC tunelů 16000
Funkční požadavky
Grafické konfigurační rozhraní (např. webový prohlížeč) a příkazový řádek bez omezení na počet administrátorů
Bezpečnostní funkce obecně označovaných jako Next Generation firewall
Podpora virtualizace na daném HW, vytváření a provozování tzv. virtuálních kontextů – min. 10 virtuálních kontextů v ceně zařízení; každý virtuální kontext musí pracovat izolovaně, možnost propojovat jednotlivé virtuální kontext pomocí interní virtuálních propojů bez nutnosti použití fyzických interface
Podpora stavového firewallingu pro IPv4 i IPv6, podpora nat 64/46
Možnost nasazení ve všech z následujících režimu (kombinace možné pomocí použití různých režimů pro různé virtuální kontexty): L2 bridge režim (inline), L3 router/NAT režim (inline), explicitní proxy (inline/out of path), transparentní proxy (inline)
Plnohodnotná správy z lokálního management rozhraní (a to i v případě využití nástroje centrální správy, neboť i v takovém případě musí být možné firewall, resp. firewall cluster, plnohodnotně konfigurovat ve chvíli, kdy z jakéhokoliv důvodu centrální správa nebude dostupná)
Ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign On
Podpora lokální databáze a vzdálené databáze (radius, ldap, tacacs+, saml, kerberos) pro ověřování uživatelů
Ověřování uživatelů pomocí SSO funkcionality pomocí Radius Single Sign On a AD pollingu
Funkce QoS, traffic shaping a SD-WAN miminálně v režimu vytvoření overlay a underlay virtuálních sítových rozhraní zahrnující fyzické propoje, IPSEC tunely či jiná rozhraní s možností definice pravidel pro řízení směrování, strategie využívání jednotlivých linek současně a monitorování stavu jednotlivých linek
Podpora funkcí VPN brány - IPSec VPN (dle platných standardů pro možnost propojení se zařízeními třetích stran); - SSL VPN pro klientský přístup s tunelovacím režimem včetně klienta pro osobní počítače i mobilní platformy, portálový režim pro bezklientský přístup;
VPN klient pro neomezený počet přistupujících zařízení součástí nabídky
Podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3
Antivirový engine musí být vybaven lokální databází vzorků škodlivého kódu a AI/ML enginem pro identifikaci podezřelých či neznámých vzorků
Funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (tzv. mobile malware), detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak), podpora sanitarizace aktivního obsahu běžných kancelářských dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby); podpora napojení na sandboxovací funkce včetně funkce akceptace lokálních signaturových databází generovaných sandboxem, vše bez nutnosti instalace pluginů do prohlížeče.

Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 4000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace
Možnost definice zakázaných slov pro vyhledávání na internetu
Podpora funkce safe search pro populární vyhledavače
Funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), podpora definice časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit, výrobcem aktualizovaná a udržovaná databáze, vynikající pokrytí českého internetu; požadované akce – povolení stránky, logování stránky, brouzdání s proklikem, nutnost autentizace uživatele pro určitou kategorii, možnost definice časových kvót pro uživatele a kategorie webu
Podopra kategorizace stremovaných videí a kanálů min. pro platformu Youtube a Vimeo
Funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů
Možnost blokovat sítový provoz na základě URL, kategorie webové stránky, IP adresy (rozsahu), GeoIP databáze, data a času
Funkce ochrany před unikem citlivých dat (data leak prevention), která umí zachytit pokus o odeslaní/upload označeného dokumentu přes internet na základě vodoznaků, popisu regulárním výrazem atp.
Podpora dvoufaktorové autentizace pomocí HW nebo mobilních OTP tokenů, součástí nabídky musí být 2 testovací HW/mobilní tokeny a plně funkční řešení dvoufaktorového OTP ověřování uživatelů pro administrátory a uživatele VPN
Obousměrná integrace (min. ve smyslu sdílení informací o odhalených hrozbách a provozně/telemetrický informací) nabízeného firewallu s dalšími instalovanými bezpečnostní prvky (mailová brána, sandbox, nástroj pro sběr a vyhodnocování logů, nástroj pro centrální správu)
Podpora řežimu nasazení v režimu WCCP (WCCP v2)
Podpora konfiguračních PAC souborů pro režim nasazení explicitní proxy
Podpora ICAP rozhraní pro obousměrnou integraci s externími servery
Podpora tunelování provozu pomocí technologie GRE
Podopra automaticky aktivovaného bypass režimu v případě přetížení systému a jeho inspekčních funkcí
Analýza a zabezpeční DNS dotazů (ochrana před DNS posoningem), filtrování DNS dotazů na základě kategorizace
Možnost filtrovat Java applety, ActiveX prvky, Cookie soubory ve webovém provozu
Integrovaná funkce load balancingu (reverzní proxy) s podporou základní algorimtů pro rozklad zátěže (round robing, váhování, nejkratší odezva, nejmenší počet aktivních spojení) s detekcí stavu reálných serverů na pozadí, podpora funkce ssl offloading a ssl inspekce pro rozkládaný provoz

Ing. RNDr. Alois Slovák
Digitálně podepsal Ing. RNDr. Alois Slovák
Datum: 2022.06.27 08:19:49 +02'00'

Bc. Vladimír Vybíral, MBA
Digitálně podepsal Bc. Vladimír Vybíral, MBA
Datum: 2022.06.24 12:19:43 +02'00'