|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Výzva na predloženie ponuky**  v zmysle § 117 ods. 1 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov   |  |  |  |  | | --- | --- | --- | --- | | Názov verejného obstarávateľa | **Slovenská konsolidačná, a.s.** |  |  | | Poštová adresa | Cintorínska č. 21 |  |  | | Mesto | Bratislava | PSČ | 814 99 | | IČO | 35776005 |  |  | | Kontaktná osoba | **Ján Ribárszki,**e-mail: [jan.ribarszki@konsolidacna.sk](mailto:jan.ribarszki@konsolidacna.sk) | Tel: 02/ 57 289 192 | | |  |

1. **Predmet zákazky**

Predmetom zákazky je obstaranie 2 ks Interných bezpečnostných firewallov NGFW (Next Generation Firewall) na obdobie 36 mesiacov pre Slovenskú konsolidačnú, a.s. (ďalej aj „verejný obstarávateľ“).

1. **Technická špecifikácia**

Verejný obstarávateľ obstaráva 2 ks Interných bezpečnostných firewallov NGFW s nasledovnou technickou špecifikáciou:

|  |
| --- |
| **Základné požiadavky:** |
| Bezpečnostné zariadenie typu firewall (ďalej aj „FW“) musí byť ako celok zložený z komponentov jedného výrobcu, vrátane všetkých poskytovaných funkcionalít typu IPS, AV, AS signatúr, databáz pre URL kategorizáciu, sandbox definícií a pod. Zároveň musí byť týmto jedným výrobcom zaistená podpora minimálne po dobu plánovanej životnosti FW. Verejný obstarávateľ požaduje dodávku dvoch zariadení v HA clustri. |
|  |
| **Požiadavky na HW architektúru:** |
| Všetky parametre priepustnosti musí dodávateľ uvádzať v real world mix paketoch, tzv. "Application mix". |
| FW musí byť typu HW appliance. Verejný obstarávateľ požaduje dodávku dvoch zariadení v HA clustri. |
| Modul pre spracovanie dát musí byť v architektúre firewallu hardwarovo oddelený od ďalších podporných modulov (správa zariadenia a riadiaci modul pre podporné sieťové činnosti), aby nemohlo dôjsť k ich vzájomnému ovplyvneniu. |
| FW musí obsahovať jeden dedikovaný port pre správu pomocou konzoly pre prístup k CLI. |
| FW musí obsahovať minimálne 4 SFP dátové rozhrania s rýchlosťou 1Gb / s a ​​4 SFP+ dátové rozhrania s rýchlosťou 10Gb / s. |
| FW musí obsahovať aspoň jeden dedikovaný OOB management port pre plnohodnotnú správu FW. |
| FW musí byť schopný ukladať "logovať" údaje na interný SSD disk s veľkosťou minimálne 240 GB. |
| FW musí podporovať agregáciu portov pomocou protokolu 802.3ad (LACP). |
| FW musí byť rozmerovo kompatibilný s 19 "rozvádzačom. |
| FW musí podporovať dva nezávislé redundantné zdroje napájania AC 230V. |
|  |
| **Požiadavky na High Availability (HA):** |
| FW musí podporovať režim HA v móde Active-Active zložený aspoň z dvoch zariadení. |
| FW musí podporovať režim HA v móde Active-Standby zložený aspoň z dvoch zariadení. |
| FW musí podporovať režim clusteringu, využiteľný pre prípadné dodatočné zvýšenie priepustnosti |
| V oboch typoch HA musia byť všetky informácie o prebiehajúcej prevádzke synchronizované tak, aby pri výpadku jedného z boxov nedošlo k strate informácií NAT a k prerušeniu aktívnych spojení prevádzky typu TCP aj UDP prechádzajúceho cez FW. |
| FW musí byť schopný vykonať HA failover na základe stavu interface (up / down), nedostupnosti druhého FW v HA, nedostupnosti špecifikovanej IP adresy. |
|  |
| **Všeobecné výkonové parametre:** |
| Priepustnosť firewallu pri plnej aplikačnej kontrole musí dosahovať hodnoty aspoň 2 Gb / s (app mix). |
| Priepustnosť firewallu pri plnej aplikačnej kontrole a zapnutí všetkých dostupných signatúr IPS a AV musí dosahovať hodnoty aspoň 1,2 Gb / s (app mix). |
| Minimálny počet súbežných spojení musí dosahovať hodnoty aspoň 190 000. |
| Minimálny počet nových spojení za sekundu musí byť minimálne 12 500. |
|  |
| **Sieťová funkcionalita:** |
| FW musí plne podporovať IPv4 aj IPv6. |
| FW musí podporovať zapojenie v režimoch L2 (s virtuálnym L3 rozhraním), L3, transparent a TAP. |
| FW musí podporovať preklady adries typu Static NAT, Dynamic NAT, PAT, NAT64. |
| FW musí podporovať smerovanie typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBR (Policy Based Routing). |
| PBR musí byť možné nakonfigurovať na základe všetkých dostupných metrík typu interface, zóna, IP adresa, užívateľ. |
|  |
| **VPN:** |
| FW musí podporovať site-to-site VPN pomocou protokolu IPSec. Počet tunelov nesmú byť licenčne obmedzený. |
| FW musí podporovať Remote Access VPN pomocou protokolov IPSec a SSL (TLS, či DTLS). |
| Počet súčasne pripojených užívateľov nesmie byť licenčne obmedzený. |
| Dodávané riešenie musí obsahovať funkcionalitu kontroly pripájaných zariadení, ktorá musí byť v súlade s preddefinovanými podmienkami. Napr. verzia OS, nainštalovaný antivírusový nástroj pod. |
| FW musí pre Remote Access VPN poskytovať pripojenie z klientskych operačných systémov Windows, MacOSX, Linux, Android a iOS. |
| Priepustnosť IPSec musí byť aspoň 1,5 Gb / s. |
|  |
| **Manažment:** |
| HW appliance musí obsahovať plnohodnotné grafické rozhranie (GUI) pre správu a čítanie logových záznamov bez nutnosti používania centrálneho management servera. Pripojenie ku GUI musí podporovať šifrovanie. |
| GUI musí obsahovať offline kontextovú nápovedu. |
| HW appliance musí obsahovať plnohodnotné textové rozhranie (CLI) pre správu a čítanie logových záznamov bez nutnosti používania centrálneho management servera. Vzdialené pripojenie k CLI musí podporovať šifrovanie. |
| HW appliance musí obsahovať plnohodnotné API rozhranie pre čítanie a konfiguráciu všetkých nastavení, týkajúcich sa bezpečnostných a ďalších pravidiel aj rozhrania a smerovanie. |
| HW appliance musí umožňovať použitie šablón pre bootstraping nových FW použitím USB flash disku. |
| FW musí pre autentizáciu a autorizáciu administrátorov podporovať protokoly LDAP, Radius, TACACS +, Kerberos a osobný certifikát. |
| FW musí obsahovať natívne nástroje pre debugging problémových situácií v úrovni L2 - L7 ISO / OSI modelu. |
| FW musí podporovať natívne nástroj pre odchytenie prevádzky. |
| FW musí byť možné spravovať z administrátorských staníc s OS Windows a MacOS. |
| FW manažment musí podporovať prácu viacerých administrátorov v rovnakom čase, vrátane aplikácie politík a nastavení vytvorených iba konkrétnym administrátorom. |
| Súčasťou dodávky musí byť nástroj, určený pre analýzu a zjednodušenie prevodu L3 / L4 pravidiel na pravidlá L7. Tento nástroj nemusí byť súčasťou FW. |
|  |
| **Aplikačné kontrola:** |
| FW musí podporovať aplikačnú detekciu a kontrolu ako svoju natívnu funkcionalitu. |
| Priradenie "povolené" a "zakázané" aplikácie musí byť natívne súčasťou vytvárania štandardného bezpečnostného pravidla. |
| Definovaná aplikácia musí predstavovať "match kritérium" pri policy lookup. |
| FW musí podporovať identifikáciu aplikácií naprieč všetkými portami / protokolmi. |
| FW musí podporovať identifikáciu aplikácií na neštandardných portoch. |
| Identifikácia aplikácie musí prebiehať priamo vo FW. |
| FW musí detekovať a zabrániť aplikácii meniť porty, tzv. Port-hopping. |
| FW musí podporovať riadenie neznámej prevádzky. |
| FW musí umožňovať tvorbu užívateľsky definovaných aplikácií bez nutnosti využitia externého nástroja alebo zásahu výrobcu / dodávateľa. |
|  |
| **Kontrola na úrovni používateľských identít:** |
| FW musí podporovať vytváranie bezpečnostných pravidiel na základe používateľských identít. |
| Voľba užívateľskej identity musí byť natívne súčasťou vytvárania štandardného bezpečnostného pravidla |
| Užívateľská identita musí predstavovať "match kritérium" pri policy lookup. |
| FW musí podporovať získavanie väzby IP adresa-užívateľské meno, bez nutnosti inštalácie klienta na koncové zariadenie. |
| FW musí podporovať získavanie väzby IP adresa-užívateľské meno, bez nutnosti inštalácie klienta na doménový kontrolér. |
| FW musí podporovať získavanie väzby IP adresa-užívateľské meno, bez nutnosti inštalácie ďalších komponentov mimo samotnej HW appliance. |
| FW musí podporovať získavanie väzby IP adresa-užívateľské meno z Active Directory za pomoci doménového účtu s čo najnižšími možnými právami pre čítanie Security logov, bez nutnosti disponovať rizikovými úrovňami oprávnení (napr. Domain Admins). |
| FW musí podporovať získavanie väzby IP adresa-užívateľské meno zo systému Cisco ISE |
| FW musí podporovať získavanie väzby IP adresa-užívateľské meno prostredníctvom načítania informácie z logového záznamu, získaného pomocou zabezpečeného protokolu Syslog. |
| FW musí podporovať získavanie väzby IP adresa-užívateľské meno z terminálových serverov MS (možné za pomoci nainštalovaného agenta). |
|  |
| **Dešifrovanie:** |
| FW musí podporovať dešifrovanie odchádzajúcej SSL / TLS prevádzky, za pomoci "podvrhnutého" serverového certifikátu klientom. |
| FW musí podporovať dešifrovanie prichádzajúcej SSL / TLS prevádzky, za pomoci naimportovaného privátneho kľúča interného servera. |
| FW musí podporovať dešifrovanie Secure Shell (SSH proxy) a kontrolovať tunelované aplikácie. |
| Dešifrovanú prevádzku musí byť možné definovať na základe URL kategórií, aj všetkých ďalších typických parametrov, ako sú zdrojová a cieľová IP adresa, port, užívateľská identita. |
| FW musí podporovať dešifrovanie pomocou ECC (Elliptical Curve Cryptography), vrátane DHE a ECDHE pre prichádzajúcu a odchádzajúcu prevádzku. |
| FW musí podporovať dešifrovanie protokolu TLS verzia 1.3. |
| FW musí podporovať preposielanie dešifrovanej prevádzky na iné skenovacie zariadenie tretích strán napr. DLP, analýza prevádzky a súborov a pod. Zariadenie 3 strany následne prepošle čisto prefiltrované dáta späť do FW. (Tzv. Decryption broker). |
| FW musí podporovať preposielanie dešifrovanej prevádzky na špecifický port pre potreby archivácie prevádzky. |
|  |
| **Sandboxing:** |
| Firewall musí podporovať možnosť odoslať do sandboxu na inšpekciu neznáme vzorky prechádzajúce protokolom HTTP, HTTPS, SMTP, SMTPS, IMAP, IMAPS, FTP a SMB. |
| Sandbox systém musí byť od rovnakého výrobcu ako je FW, ale nemusí byť HW súčasťou FW. |
| Sandbox systém musí byť schopný okamžite automaticky vytvoriť IPS / AV signatúry pre FW, v prípade, keď je testovaná vzorka vyhodnotená ako škodlivá. |
| Sandbox musí byť schopný automaticky upraviť kategórie používanej URL databázy ak zistí, že testovaná vzorka je škodliva a komunikuje na konkrétne URL. |
| Sandbox musí poskytovať aktualizácie signatúr pre AV, Webfiltering, DNS, C & C. |
| Sandbox musí podporovať analýzu vzorky na operačnom systéme inštalovanom priamo na hardvéri, tzn. nie vo virtuálnom prostredí. |
| Sandbox musí podporovať operačné systémy Windows, Linux, MacOS a Android. |
| Report z analýzy odoslanej vzorky do sandboxu musí byť prístupný priamo z rozhrania FW. |
| Aktualizácia zero-day signatúr musí byť inštalovaná do FW v intervale max. 5 minút. |
| FW musí byť schopný detekovať a zablokovať prevzatie neznámeho škodlivého súboru v reálnom čase, bez toho, aby bol doručený na koncový bod. |
|  |
| **Bezpečnostné funkcionality:** |
| FW musí podporovať zavedenie tzv. Pozitívneho bezpečnostného modelu - povolenie iba vybraných aplikácií a zákaz všetkých ostatných aplikácií, vrátane neznámej prevádzky. |
| FW musí obsahovať integrovaný systém ochrany proti zraniteľnostiam (virtual patching) a sieťovým útokom (IPS). Databáza IPS signatúr musí byť uložená priamo vo FW. Aplikácia IPS profilu musí byť granulárna, na úrovni bezpečnostného pravidla. |
| FW musí umožňovať tvorbu užívateľsky definovaných IPS signatúr bez nutnosti využitia externého nástroja alebo zásahu výrobcu / dodávateľa. |
| FW musí obsahovať integrovaný systém ochrany proti prítomnosti vírusov a škodlivého kódu. Databáza AV signatúr musí byť uložená priamo vo FW. Aplikácia AV profilu musí byť granulárna, na úrovni bezpečnostného pravidla. |
| Antivirus musí byť schopný kontrolovať prevádzku v minimálne týchto aplikáciách - SMTP, POP3, IMAP, HTTP, HTTPS, HTTP / 2, FTP a SMB. |
| FW musí umožňovať tvorbu užívateľsky definovaných spyware signatúr bez nutnosti využitia externého nástroja alebo zásahu výrobcu / dodávateľa. |
| FW musí podporovať možnosť zablokovania útoku využívajúceho známe C&C centrá aj v prípade, že je prevádzka šifrovaná a nie je možné vykonávať SSL dekrypciu. |
| FW musí v bezpečnostných predpisoch podporovať použitie externých dynamických zoznamov; FW musí poskytovať možnosť overiť na základe certifikátov pravosť týchto dynamických zoznamov. |
| FW musí podporovať import Snort signatúr. |
| FW musí pre prístup ku kritickým aplikáciám poskytovať možnosť vynútiť multifaktorové overenie prostredníctvom webového portálu, bez ohľadu na to, či cieľová aplikácia podporuje viacfaktorovú autentizáciu; táto vlastnosť musí byť konfigurovateľná na úrovní bezpečnostného pravidla. |
| FW musí poskytovať možnosť zabrániť odoslaniu doménových užívateľských prihlasovacích údajov do iných, než povolených URL kategórií, pre zabránenie phishingu. |
| FW musí poskytovať funkciu k ochrane proti tzv. Drive-by downloadom; spôsob ochrany musí byť pre používateľa interaktívny s možnosťou voľby akceptácie rizika a stiahnutia súboru. |
| FW musí podporovať analýzu DNS dopytu tzv. Sinkhole funkciou, ktorá na dopyt malware DNS URL vráti podvrhnutú IP adresu pre detailnejšiu analýzu a zároveň sa stanica na pôvodnú malware stránku nedostane. |
| FW musí pobsahovať funkcionalitu pokročilej analýzy DNS dopytov proti technikám používajúcim DGA (domain generation algorithm) v reálnom čase. |
| FW musí podporovať integráciu so systémom Cisco ISE pre zaradenie koncovej stanice do karantény pri detekovaní nevhodného správania. |
|  |
| **Ochrana proti DoS:** |
| FW musí obsahovať natívnu službu pre ochranu proti útoku typu DoS pomocou limitácie počtu spojení na úrovni zdrojová a cieľová IP adresa, užívateľská identita a aplikácia. |
|  |
| **QoS:** |
| FW musí poskytovať možnosť prioritizácie prevádzky a obmedzenie využívanej šírky pásma na základe zdrojovej a cieľovej IP adresy, portu, užívateľskej identity, aplikácie a času (od - do, deň v týždni + čas a pod.). |
| FW musí podporovať prioritizáciu prevádzky na základe DSCP. |
| FW musí podporovať prioritizáciu prevádzky na základe identifikovanej aplikácie. |
|  |
| **URL filtering:** |
| FW musí obsahovať natívnu podporu pre využívanie databázy URL. |
| URL databázy musia byť od toho istého výrobcu ako FW. |
| FW musí byť schopný použiť URL kategóriu v definícii bezpečnostného pravidla. |
| FW musí podporovať vytváranie užívateľsky definovaných kategórií, bez nutnosti využiť externý nástroj a bez nutnosti zásahu výrobcu / dodávateľa. |
| URL databáza musí byť dynamicky aktualizovaná na základe novo zistených URL, vedúcich na škodlivý obsah alebo C & C centra. |
| URL databáza musí podporovať možnosť zaradenia do aspoň dvoch kategórií naraz pre jedinú URL. |
| FW musí umožňovať požiadať o rekategorizáciu nevhodne zaradených URL priamo v grafickom rozhraní FW bez nutnosti kontaktovania technickej podpory. |
|  |
| **Logovanie:** |
| FW musí obsahovať lokálne úložisko logov. |
| FW musí obsahovať nástroj na analýzu logov bez nutnosti využitia ďalšieho systému mimo GUI |
| FW musí podporovať agregované zobrazenie logov na základe jedného filtrovacieho pravidla, naprieč jednotlivými typmi logov, ako sú prevádzkové logy, logy bezpečnostných incidentov a logy prístupov na URL. |
| FW musí podporovať preposielanie logov na zariadenia tretích strán. |
| FW musí umožňovať výber preposielaných logov na úrovni bezpečnostného pravidla. |
| Preposielané logy z FW musia byť automaticky rozpoznané najčastejšie používanými typmi SIEM (uvedených v Leaders kvadrante aktuálneho Gartner MQ). |
|  |
| **Servisná podpora a licenčný plán:** |
| FW musí podporovať licenčný model nezávislý od počtu ochraňovaných koncových systémov alebo užívateľov. |
| Požadovaná dĺžka podpory a platnosti licencií je 3 roky od nasadenia zariadenia do siete objednávateľa. |
|  |
| **Ostatné:** |
| Vrátane dopravy na miesto plnenia. |

1. **Obsah ponuky:**

V nadväznosti na uvedené si Vás verejný obstarávateľ. dovoľuje požiadať o predloženie ponuky na celý predmet zákazky opísaný v bodoch 1. a 2. tejto Výzvy.

***Ponuka musí obsahovať:***

* 1. Základné identifikačné údaje uchádzača v zmysle **Prílohy č. 1.**
  2. Cenovú ponuku predloženú v zmysle **Prílohy č. 1.**
  3. Uchádzač predloží zoznam kontaktných osôb zodpovedných za plnenie zákazky.
  4. Uchádzač je povinný predložiť verejnému obstarávateľovi vlastný návrh na plnenie predmetu zákazky pre všetky položky. Vlastný návrh na plnenie predmetu zákazky uchádzač predkladá na účely kontroly či ponúkaný tovar zodpovedá technickej špecifikácii predmetu zákazky.
  5. Uchádzač je povinný preukázať, že pre úspešnú realizáciu zákazky disponuje vlastným expertom s platnou technickou certifikáciou výrobcu pre všetky ponúkané zariadenia formou predloženia (sken) požadovaného certifikátu alebo jeho ekvivalentu. Podmienkou pre akceptáciu dodávky je realizácia dodávky týmto expertom.
  6. Uchádzač je povinný preukázať, že pre úspešnú realizáciu diela je certifikovaným partnerom výrobcu FW s oprávnením pre dodávku, implementáciu a podporu uvedeného systému formou predloženia (sken) požadovaného certifikátu alebo jeho ekvivalentu.
  7. Úspešný uchádzač je oprávnený fakturovať iba celý predmet zákazky naraz po dodaní všetkých položiek, nie sú prípustné faktúry za čiastkové plnenie.
  8. Právo na vystavenie faktúry a zaplatenie ceny za dodávku vznikne úspešnému uchádzačovi riadnym dodaním a odovzdaním predmetu zákazky verejnému obstarávateľovi. Podkladom pre úhradu ceny za dodanie bude faktúra vystavená úspešným uchádzačom, doložená súpisom dodaných služieb a Akceptačným protokolom o ich odovzdaní.
  9. Doklad (sken) o oprávnení uchádzača poskytovať službu podľa § 32 ods. 1 písm. e) zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov, ktorý zodpovedá predmetu zákazky.
  10. Čestné prehlásenie (sken) o skutočnosti, že uchádzač nemá uložený zákaz účasti vo verejnom obstarávaní potvrdený konečným rozhodnutím v Slovenskej republike alebo v štáte sídla, miesta podnikania alebo obvyklého pobytu v zmysle ustanovenia § 32 ods. 1 písm. f) zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov. Čestné prehlásenie musí byť podpísané štatutárnym zástupcom uchádzača, alebo iným zástupcom uchádzača, ktorý je oprávnený konať v jeho mene.

1. **Miesto dodania predmetu zákazky:**

Cintorínska 21, 811 08 Bratislava 1

1. **Kritérium na hodnotenie ponúk:**

Kritériom na hodnotenie ponúk je najnižšia cena v zmysle **Prílohy č. 1.** za celý predmet zákazky opísaný v bodoch 1. a 2. tejto Výzvy.

1. **Zmluvné podmienky:**

Po vyhodnotení ponúk uchádzačov bude úspešnému uchádzačovi vystavená objednávka. Lehota na dodanie predmetu zákazky opísaného v bodoch 1. a 2. tejto Výzvy je maximálne ***60 pracovných dní*** od doručenia mailovej objednávky verejným obstarávateľom na mailovú adresu uvedenú v cenovej ponuke v zmysle **Prílohy č. 1.** Odovzdanie predmetu zákazky uvedeného v bodoch 1. a 2. tejto Výzvy nastane dňom podpisu Akceptačného protokolu zodpovednými zástupcami oboch strán.

1. **Lehota na predkladanie ponúk:**

**7.7.2021**

1. **Forma a spôsob predloženia ponúk:**

Ponuky verejný obstarávateľ žiada doručiť mailom na adresu:

[obstaravanie@konsolidacna.sk](mailto:obstaravanie@konsolidacna.sk)

1. **Dôvody zrušenia zadania zákazky:**

Ak nebola predložená ani jedna ponuka,

ak ani jeden z uchádzačov nesplnil podmienky výzvy,

ak ani jedna z ponúk nevyhovuje požiadavkám verejného obstarávateľa,

ak sa zmenili okolnosti, za ktorých bolo obstarávanie vyhlásené.

Verejný obstarávateľ si vyhradzuje právo odmietnuť všetky predložené ponuky.

Príloha č. 1: Cenová ponuka