Kupní smlouva
na systém ochrany - firewall

CompuNet s.r.o.
zastoupena jednatelem Ing. Pavlem Pikhartem
se sídlem Zubatého 295/5, 150 00 Praha 5
IČ: 27608514
DIČ: CZ27608514
Bankovní spojení: Komerční banka a.s., 51-1998450287/0100
Kontaktní osoba: Martin Pokorný, tel.: 724 812 911, email: pokorny@compunet.cz

dále jen „Prodávající“
na straně jedné

a

Archiv bezpečnostních složek
zastoupen Mgr. Světlanou Ptáčníkovou, ředitelkou
se sídlem Siwiecova 2, 130 00 Praha 3
IČ: 75112817
organizační složka státu zřízena zákonem č.181/2007Sb.
Bankovní spojení: ČNB Na příkopě 28. Praha 1, 115 03, číslo účtu: 6926031/0710
Kontaktní osoba: Albert Sidó, tel: 221 008 227, email: albert.sdio@abscr.cz

dále jen „Kupující“
na straně druhé

uzavřeli níže uvedeného dne, měsíce a roku dle zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, tuto kupní smlouvu (dále jen “smlouva“)

I. Předmět smlouvy

1.Prodávající se zavazuje dodat Kupujícímu zboží specifikované v Příloze č. 1 této smlouvy na základě veřejné zakázky č N006/21/V00021944 (dále v této smlouvě též jako „Zboží“) a převést na Kupujícího vlastnické právo ke Zboží.

2.Kupující se zavazuje dodané Zboží od Prodávajícího převzít, převzetí písemně potvrdit, a dále se zavazuje zaplatit Prodávajícímu sjednanou kupní cenu za Zboží.

II. Kupní cena

1. Kupní cena za předmět Kupní smlouvy činí:

Cena celkem bez DPH	**421 518,00- Kč.**
DPH	**88 518,78- Kč.**
Cena celkem s DPH	**510 036,78- Kč.**

2. Cena zahrnuje náklady na dopravení předmětu kupní smlouvy na místo určené kupujícím.

3. Kupující není plátcem DPH.

4. Sjednaná kupní cena je nejvýše přípustná a zahrnuje v sobě náklady na dopravu Zboží do místa dodání, náklady na balení Zboží a náklady na předání Zboží.

III. Termín plnění

1. Prodávající se zavazuje předmět smlouvy dodat nejpozději do 1. 12. 2021.

2. Dodávka je považována za splněnou provedením instalace zboží v místě uvedením v bodě IV písm. 2.

IV. Dodací podmínky, místo plnění

1. Termín dodání: nejdéle do 1. 12. 2021.

2. Místo plnění: Archiv bezpečnostních složek, Branické nám. 777/2, Praha 4 – Braník.

3. Prodávající vystaví dodací list, který bude podepsán při předání/převzetí oběma smluvními stranami.

4. Prodávající informuje o termínu předání zboží kontaktní osobu Kupujícího písemně emailem nejméně 3 pracovní dny před předáním zboží.

5. Prodávající uvede zboží do provozu a zaškolí obsluhu.

V. Platební podmínky

Smluvní strany se dohodly, že kupní cena Předmětu koupě bude uhrazena na základě vystavené faktury se splatností 21 dní ode dne uvedení do provozu a zaškolení obsluhy. Kupní cena Předmětu koupě bude hrazena bezhotovostním převodem na bankovní účet Prodávajícího uvedený v daňovém dokladu.

VI. Záruční podmínky

1. Prodávající prohlašuje a odpovídá za to, že dodané zboží je nové a nepoužívané.

2. Prodávající poskytuje na dodané zboží dle této smlouvy záruku v trvání 24 měsíců.

3. Prodávající poskytne záruční servis po celou dobu záruky.

4. Zboží, u kterého bude od dodání zjištěna výrobní vada, bude prodávajícím neprodleně vyměněn za nový shodný výrobek.

5. Záruční doba počíná běžet dnem instalace předmětu koupě Prodávajícím. O zprovoznění předmětu koupě bude vyhotoven písemný záznam, který podepíše zástupce Prodávajícího a Kupujícího.

VII. Smluvní pokuta a úroky z prodlení

1. Nedodá-li Prodávající zboží do uplynutí sjednané dodací lhůty, zaplatí Kupujícímu smluvní pokutu ve výši 0,01% z ceny Předmětu koupě včetně DPH za každý, byť započatý den prodlení. Zaplacením smluvní pokuty není dotčen nárok Kupujícího na náhradu škody.

2. Nezaplatí-li Kupující kupní cenu včas, je povinen zaplatit Prodávajícímu úrok z prodlení ve výši 0,01% z nezaplacené částky za každý, byť započatý den prodlení.

VIII. Možnost odstoupení od smlouvy

Jestliže jedna ze smluvních stran poruší některé z ustanovení této smlouvy, je druhá strana oprávněna od smlouvy odstoupit.

IX. Závěrečná ustanovení

1. Tato Kupní smlouva je sepsána v elektronickém vyhotovení včetně elektronických podpisů. Předání proběhne prostřednictvím datových schránek. Veškeré změny nebo doplňky této smlouvy musí být činěny pouze elektronickou formou číslovaného dodatku podepsaného oběma smluvními stranami.

2. Veškeré závazkové právní vztahy spojené s touto Kupní smlouvou se řídí právním řádem České republiky, zejména příslušnými ustanoveními zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

3. Prodávající souhlasí s uveřejněním této smlouvy v registru smluv podle zákona č. 340/2015 Sb., o registru smluv, podle něhož je Kupující povinen smlouvy do registru vkládat pod sankcí neplatnosti.

4. Kupující při zpracování osobních údajů postupuje v souladu s právními předpisy Evropské unie a České republiky. Podrobnější informace jsou uvedeny na www.abscr.cz.

5. Tato kupní smlouva nabývá platnosti a účinnosti dnem podpisu, kterým smluvní strany potvrzují její autentičnost. Smluvní strany dále potvrzují, že tato smlouva byla uzavřena svobodně a vážně, že nebyla ujednána v tísni ani za jinak jednostranně nevýhodných podmínek.

6. Smluvní strany prohlašují, že předmět plnění je v této smlouvě a její Příloze č. 1, která je nedílnou součástí smlouvy, vymezen jednoznačným způsobem.

7. Smluvní strany prohlašují, že si smlouvu řádně přečetly, s celým jejím obsahem souhlasí a na důkaz toho, že se jedná o projev jejich svobodné a vážné vůle, který není činěn v tísni ani za nápadně nevýhodných podmínek, připojují své podpisy.

V Praze

Ing. Pavel Pikhart
Digitálně podepsal Ing. Pavel Pikhart
Datum: 2021.10.04 08:46:55 +02'00'

_____

Ing. Pavel Pikhart
jednatel
podepsáno elektronicky

Za prodávajícího

V Praze

Mgr. Světlana Ptáčníková
Digitální podpis: 01.10.2021 15:07

_____

Mgr. Světlana Ptáčníková
ředitelka
podepsáno elektronicky

Za kupujícího

Příloha č. 1

Nákup dvojice firewallů Fortigate FG 200F

Základní parametry

- Platforma postavená na HW akcelerované architektuře (tj. zařízení vybavené kombinací CPU + specializované obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekrypce, porovnávání se signaturovou databází…).
- Celá dodávka musí obsahovat všechny HW komponenty a licence na dobu 2 let. 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. roadmap nebudou akceptovány.
- Dodání zařízení musí být ve formátu HW appliance o velikosti 1RU.
- Součástí bude veškeré příslušenství (montážní prvky) pro montáž do RACKu.
- Možnost rozšíření platformy i další prvek typu NGFW jehož cílem bude zajišťování sdílení telemetrických informací, vizualizace stavu sítě, zařízení a klientů, přičemž celé řešení musí být podporováno výrobcem.
- Možnost o rozšíření platformy pro sběr logů a grafického reportingu včetně oboustranné komunikace (tím se rozumí minimálně odeslání a zpětné načítání logů pro účel vizualizace), přičemž zde musí existovat garantovaná podpora funkcionality.

Hardware požadavky

- Počet síťových rozhraní copper, RJ45 10/100/1000 - min 16x.
- Počet GE SFP – min 8x.
- Počet 10 GE SFP – min 4x.
- Konzolový port pro management.
- Dedikovaný port RJ45 pro management.
- Dedikovaný port RJ45 pro HA konfiguraci.
- Redundantní napájecí zdroj.

Propustnost a další výkonové parametry

- Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B- min 26000 Mbps, 26000 Mbps, 10000 Mbps.
- Latence firewallu (64 B UDP paket) - max 5 mikro sec.
- Počet naráz otevřených spojení – min 2,7 M.
- Počet nových spojení za sekundu - min. 260 000.
- Počet firewall pravidel až 10 000.
- Podpora virtualizace (min 10 virtuálních kontextů).
- Podpora funkce bezdrátový kontrolér - 128 APOD.
- Podpora funkce integrovaný switch controller – podpora až 64 switchů.

Funkcionalita – Networking a vysoká dostupnost (HA)

- Podpora režimu vysoké dostupnosti, L2, Active - Active, Active - Passive, full mesh HA, VRRP, synchronizace stavové tabulky a IPsec SAs mezi nody v clusteru.
- Režim fungování L2 – transparentní režim, L3 – NAT/Router.
- Podpora VLAN.
- Podpora multicast, vytváření politiky pro multicast routing.
- Podpora 802.3ad link aggregation.
- Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálné servery, podpora health check funkcí, podpora SSL offloading.
- Podpora centrální NATovácí tabulky, stavová inspekce SCTP komunikace.
- Podpora dynamických routovacích protokolů BGP, OSPF, ISIS, RIP.
- Policy-based routing.
- Funkce SD WAN – možnost rozkládání provozu mezi více linek na základě aplikačních signatur, IP adres a portů u známých aplikací, kvality linky včetně automatické detekce nefunkčnosti linky.

Funkcionalita - VPN

- Funkce SSL VPN:
  - Podpora klientského i bezklientského (portálového) režimu.
  - Minimální počet současně navázaných SSL VPN tunelů: 450.
  - Minimální propustnost SSL VPN: 1900Mbps.
- Funkce IPSEC VPN:
  - Podpora site-to-site VPN.
  - Podpora klientských VPN.
  - Dostupnost VPN klienta pro koncové stanice (Windows, MacOS).
  - Funkce klientských IPSec VPN nesmí být licencovaná na počet uživatelů. V opačném případě požadujeme dodání neomezené licence.
  - Minimální počet IPSEC VPN tunelů typu lokalita-lokalita: 2300.
  - Minimální počet klientských IPSEC VPN tunelů: 15000.
  - Propustnost IPSec VPN min. 12,5 Gbps (měřeno při AES256-SHA256).
  - Podpora konfigurace redundantních IPSec VPN tunelů za pomoci statického směrování.
  - Podpora konfigurace redundantních IPSec VPN tunelů za pomoci dynamického směrování.
  - Podpora funkce dynamického navazování IPsec tunelů dle potřeby komunikace.
- Podpora VXLAN.
- Podpora L2TP, PPTP, GRE.
- Podpora dynamických routovací protokolů OSPF, BGP ve VPN IPsec.

Funkcionalita - UTM

- Funkce detekce aplikací na L7 (Application Control):
  - Detekce známých aplikací na základě signatur.
  - Signaturový database automaticky aktualizované výrobcem.
  - Alespoň 4000 podporovaných aplikací.
  - Pro populární cloudové aplikace (minimálně Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) požadujeme pokročilé akce typu blokování upload/download souborů, blokování her v rámci aplikace, blokování login atd. (relevantní k dané aplikaci).
  - Možnost tvorby vlastních signatur.
  - Detekované aplikace je možné: povolit, monitorovat, blokovat.
  - Na základě typu aplikace musí být možné omezit šířku pásma pro danou aplikaci.

    - Funkce AppCtr se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. Alternativně požadujeme možnost využití v rámci tzv. NGFW pravidel popsaných výše.
- Funkce detekce a potlačení narušení (IPS/IDS):
    - Signatury automaticky aktualizované výrobcem.
    - Alespoň 11.000 rozpoznávaných hrozeb (signatur) definovaných výrobcem.
    - Možnost tvorby vlastních signatur.
    - Funkce IPS se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům.
    - Propustnost funkce IPS včetně logování min. 4800Mbps (měřeno na komunikaci typu mix aplikací).
- Funkce antivirové kontroly:
    - Ochrana před škodlivým kódem (malware, trojské koně, atp.), včetně ochrany před polymorfním kódem.
    - Signatury automaticky aktualizované výrobcem.
    - Požadujeme AV kontrolu rozšířenou o inspekci tzv. sandbox technikou, poskytovanou formou služby dodávané výrobcem FW (licence musí být součástí dodávky).
    - Možnost rozšíření o inspekci tzv. sandbox technikou formou lokálné HW appliance stejného výrobce.
    - Deklarovaná propustnost AV kontroly, v kombinaci s IPS, Application Control a zapnutým logováním min. 2900 Mbps.
    - Funkce AV kontroly se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům.
    - Podpora služby výrobce, která umožńí detekovat malware, který byl objevený v době od poslední aktualizace AV signaturové databáze pomocí globální́ a rychle se aktualizující databáze hashů.
    - Funkce odstranění aktivního obsahu z dokumentů kancelářských aplikací – AV engine na firewallu/bezpečnostní emailové bráně v reálném čase odstraní aktivní obsah z dokumentu, dokument zůstává v původním formátu, jsou z něj odstraněny všechny aktivní prvky. Upravený dokument jde k původnímu příjemci, originální dokument se odešle do sandboxu.
- Funkce kategorizace webových stránek :
    - Založená na centrálně spravované databázi výrobce.
    - Minimálně 50 filtračních kategorií.
    - Možnost definice vlastních kategorií.
    - Možnost definice vlastních seznamů zakázaných URL.
    - Kategorizace musí zahrnovat i české a slovenské internetové stránky.
- Funkce DNS filtru:
    - Možnost blokovat DNS dotazy na základě příslušnosti k URL kategorii (obdobné kategorie jako u předchozího bodu).
    - Možnost definovat vlastní tzv. blacklist domén.
    - Možnost přesměrovat komunikace se zakázanými doménami na vlastní portal/URL.
    - Možnost importu seznamu blokovaných domén do DNS filtru.
    - Detekce a blokování komunikace do botnet sítí.
- Funkce ochrany před únikem citlivých informací (DLP):
    - Možnost analýzy běžných typů dokumentů a protokolů.
    - Možnost definice pravidel min. na základě regulárních výrazů, watermarkovacího nástroje a typu kontroly typu file checksum.
- Email filter – jednoduchá antispamová a antivirová inspekce elektronické pošty.
- Podpora SSL dekrypce/SSL inspekce s minimální propustností 3900Mbps.
- DoS Policy prevence proti základním útokům typu DoS.
- Firewall musí být vybaven bezpečnostním modulem pro ukládání citlivých informacích založeným na bázi HW (TPM).

Firewall

- Možnost nastavovat firewall politiku na základě geografických údajů.
- Aplikace firewall policy na známé internetové služby, kde databáze těchto služeb je pravidelně aktualizována výrobcem.
- Možnost snadné integrace cloudové služby. Minimálně na: MS Azure, Amazon Web Services, Google Cloud.
- Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru.
- Viditelnost do provozu na aplikační úrovni.
- 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 application control, nikoliv pouhý TCP/UDP port) resp. kategorie URL filteringu (nikoliv jako AppCtrl resp URL filtering profil aplikovaný na dané pravidlo).
- Ověřování uživatelů LDAP, Active Directory, Single Sign On, Radius, TACACS+, ověřování na základě certifikátu.
- Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření.
- Traffic Shaping, QoS s podporou priroritizace provozu na základě DSCP markování a ToS, aplikace traffic shaping na konkrétní aplikaci nebo webovou kategorii.
- Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu.
- Podpora funkce reverzní proxy.
- Podpora silné autentizace uživatelů – integrovaná podpora generátoru jednorázových hesel (OTP) – pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů.
- Explicit proxy:
    - Podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl, DLP).
    - Podpora transparentního ověřování uživatele proti MS AD protokolem Kerberos.
    - Funkce transparentní proxy, kdy dochází k automatickému přesměrování provozu na proxy server bez nutnosti konfigurovat klienta.
    - Funkce transparentního ověřování uživatelů pomocí domény (MS Active Directory) včetně podpory autentizace uživatel na terminálovém serveru.

Integrovaný controller bezdrátových (Wifi) sítí

- Wifi controller integrovaný do NGFW platformy.
- Každá bezdrátová síť (SSID) bude reprezentována virtuálním síťovým rozhraním.
- Podpora bezpečnostních profilů (AV, AppControl, Webfilter, DLP) přímo na wifi controlleru.
- Podpora SSL dekrypce uživatelského provozu přímo na wifi controlleru.
- Podpora wifi přístupových bodů stejného výrobce s výrobcem FW řešení.
- Možnost volby z různých modelů (např. 802.11abgn, 802.11ac, 802.11ac wave2, indoor, outdoor).
- On-wire rogue AP detekce a mitigace.
- Podpora fast-roamingu (802.11 k,v,r).
- Podpora více PSK u jednoho SSID.
- Podpora IPSEC tunelu pro šifrování data plane (uživatelských dat).
- Podpora WPA3 šifrování.
- Podpora WiFi 6 standardu.
- Podpora BSS coloring (WiFi 6).
- Podpora diagnostických WiFi nástrojů, například pro analýzu spektra.

Funkcionalita - virtualizace

- Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext musí být plnohodnotné řešení včetně odděleného GUI, management účtů, atp.
- Součástí dodávky musí být licence na min. 10 virtuálních kontextů (včetně licence na kompletní podporu požadovaných bezpečnostních funkcí v těchto virtuálních kontextech).
- Každý virtuální kontext je zároveň samostatným wifi controllerem.
- Podporou izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů).

Funkcionalita - management

- 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.
- Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě.
- Podpora otevřeného API (možnost integrace vybraných funkcí do stávající management infrastruktury).