Příloha č. 1 – Technická specifikace

Fortinet FortiAnalyzer 200F

FortiAnalyzer = Systém pro ukládání, analýzu a korelaci logů

Zařízení pro rychlé a efektivní zpracování velkých objemů dat z bezpečnostních zařízení v podnikové síti včetně historického přehledu a znalosti kontextu u dynamických hrozeb.

Specifikace modelu FortiAnalyzer 200F:

Kapacita a výkon	
Záznam logů v GB/1 den	100
Analytická udržitelná hodnota (logů/sekunda)	3000
Udržitelná hodnota kolektoru (logů/sekunda)	4500
Počet zařízení/VDOMů (Maximum)	150
Maximální počet dní Analytiky	40
Podporované možnosti	
FortiGuard indikátor ohrožení (IOC)	ANO
Hardware specifikace	
Rozměr pro uložení do RACK	1 RU Rackmount
Celkový počet rozhraní LAN	2 x RJ45 GE
Kapacita úložiště	4 TB (1 x 4 TB)
Použitelná kapacita úložiště	4 TB
Dimensions	
Výška x Šířka x Délka (cm)	4.4 x 43.2 x 38.1
Váha	7.8 kg
Parametry prostředí	
AC napájecí zdroj	100–240V AC, 60–50 Hz
Spotřeba (průměr / maximum)	49W / 114W
Tepelné ztráty	390 BTU/h
Pracovní teplota	0 – 40° C
Teplota úložiště	-35–70° C
Vlhkost	20 to 90% nnekondenzující
Pracovní nadmořská výška	až do 2.250 m
Vyhovuje normám	
Bezpečnostní certifikace	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB

Zdůvodnění požadavků pro nákup modelu FortiAnalyzer 200F:

- Systém musí být plně kompatibilní se současnými firewally Fortinet FortiGate 100E a platformou sandbox
- Musí plně podporovat analýzu logů z daného prostředí.
- Musí být schopný poskytovat reporty nad logy a informovat správce systému o hrozbách, které byly v síti odhaleny.
- Plná funkční kompatibilita s firewallem a sandbox platformou musí být oficiálně doložena výrobcem těchto platforem.
- Požadujeme HW appliance o velikosti 1RU.
- HW appliance znamená operační systém i aplikaci vytvořenou pro specifický HW určený přímo pro funkci ukládání a korelaci logů.
- Tento celek bude krytý stejnou servisní smlouvou výrobce (maintenance).
- Řešení postavené na virtuální appliance nebude akceptováno.
- Požadujeme obousměrnou komunikaci mezi FW a logovací platformou.
- Obousměrnou komunikací rozumíme možnost prohledávat logy, uložené na logovací platformě přímo z GUI prostředí firewallu.
- Kapacita úložiště min. 4TB.
- Řešení musí být schopno přijímat minimálně 80 GB logů za den.
- Pokud je pro dosažení této hodnoty vyžadována licence, tak tato musí být součástí dodávky.
- Výkonnost řešení musí zaručit příjem min. 2 800 událostí/sec.
- Pokud je pro dosažení této hodnoty vyžadována licence, tak tato musí být součástí dodávky.
- Možnost rozdělení zařízení na oddělené administrativní sekce
  (každá virtuální instance firewallu může být v jiné administrativní sekci centrálního logovacího zařízení).
- Možnost dostat se z vizuálního zobrazení ke konkrétním logům jednoduchým proklikem.
- Možnost prohlížení a prohledávání historických logů stejně jako logů v reálném čase.
- Korelace logů.
- Samostatná sekce informující o hrozbách v síti.
- Podpora reportů nad logy ve formátu HTML/CSV/XML/PDF.

- Generování reportů v pravidelných intervalech.
- Předdefinované vzory pro reporty na nejčastější použití.
- Možnost vytváření vlastních reportů na základě konkrétních SELECT dotazů do databáze.
- Podpora prohlížení statistických údajů nad logy.
- Upozorňování na důležité informace z logů – emailem a SNMP trapy.
- Event Management.
- Předpřipravený dashboard pro využití dohledovým centrem.
- Možnost rozšíření o funkci retrospektivní kontroly logů za využití aktuálních informací typu threat feeds, reputační databáze, atd.

Požadavek na podporu:

• Požadujeme podporu v režimu 24x7, a to na dobu 5 let, a to pro dodaný HW i SW.

Základní charakteristika technologických vlastností modelu FortiAnalyzer 200F:

A. Okamžitý přehled, rychlá reakce na bezpečnostní incidenty

Zde se uplatňuje bezpečnostní architektura Fortinet Security Fabric, která nabízí sjednocenou, komplexní ochranu proti pokročilým perzistentním hrozbám pomocí podnikových firewallů Fortinet. Zařízení FortiAnalyzer v této architektuře poskytuje podrobný přehled a bezpečnostní výstrahy, na něž lze ihned reagovat nebo s jejich pomocí automatizovat obranu.

FortiAnalyzer umožňuje na jednom místě shromažďovat, analyzovat a porovnávat data ze záznamů událostí z distribuované sítě podnikových firewallů Fortinet a na jednom terminálu zobrazovat veškerý provoz na firewallech a generovat reporty. Při propojení se službou indikátorů narušení FortiGuard (IOC) dokáže poskytovat seznam narušených serverů seřazený podle priorit, což umožňuje rychlou reakci.

B. Hlavní výhody

Centralizované vyhledávání a reporting	Jednoduché a intuitivní vyhledávání ve stylu Google a reporty o síťovém provozu, hrozbách, aktivitě a trendech v síti.
Automatizované indikátory narušení (IOC)	Služba FortiGuard IOC vyhledává v bezpečnostních záznamech známky pokročilých perzistentních hrozeb.
Přehled o aktivitě v síti v reálném čase a historické záznamy	Souhrn aplikací, zdrojů, destinací, internetových stránek, bezpečnostních hrozeb, správcovských úprav a systémových událostí.
Základní nástroje pro řízení událostí	Přednastaveným bezpečnostním událostem lze snadno přiřadit automatizované výstrahy.
Hladké zapojení do bezpečnostní architektury Fortinet Security Fabric	Získává informace ze záznamů událostí ze zařízení FortiClient, FortiSandbox, FortiWeb, FortiMail atd. pro dokonalejší přehled.

C. Přehled funkcí a vlastností

FortiView — podrobný přehled o síti
- Přizpůsobitelný interaktivní situační přehled umožňuje rychle identifikovat a řešit problémy
- Intuitivní souhrny síťového provozu, hrozeb, aplikací a mnoha dalších informací
- Podrobný přehled o uživatelích bezdrátové sítě, cizích přístupových bodech a zranitelnostech koncových zařízení
- Vizualizace s bublinovými grafy a geografickou mapou hrozeb
- Detailní zkoumání dat umožňuje sledovat stopu útočníka, průběh transakcí a získávat nové poznatky

Indikátory narušení FortiGuard — služba automatizovaného porovnávání dat
- Zkoumá bezpečnostní záznamy o provozu ze zařízení FortiGate a vyhledává v nich podezřelé vzorce
- Automatizovaný systém obrany proti průniku, který nepřetržitě sleduje známky útoku na síť
- Poskytuje podle priority seřazený seznam serverů, u nichž došlo k narušení a je nutné podniknout další kroky
- IOC zvyšuje úroveň zabezpečení a pomáhá chránit podnik přesnou a spolehlivou detekcí pokročilých hrozeb

Reporting
- Více než 28 předpřipravených šablon připravených k použití se vzorovými reporty
- Generování reportů na vyžádání nebo podle harmonogramu s automatickým upozorňováním e-mailem a zobrazením v kalendáři
- Flexibilní formáty reportů: HTML/CSV/XML/PDF
- Vlastní reporty: přes 300 předdefinovaných grafů pro vlastní reporty a intuitivní nástroj pro tvorbu grafů, který umožňuje snadno vytvářet vlastní grafy z výsledků vyhledávání v záznamech

Monitorování a výstrahy
- Aktivní monitorování sítě v reálném čase pro vyhledávání nedostatků, problémů a útoků
- Přes 20 předpřipravených definic událostí připravených k použití, s širokými možnostmi vlastních úprav
- Automatizované zasílání výstrah umožňuje rychlou reakci
- Možnost zkoumání záznamů na velmi podrobné úrovni umožňuje rychlé vyšetření bezpečnostních událostí

Multitenantní uspořádání s flexibilním nastavováním kvót
- nastavitelná časová pravidla pro archivování a analýzu dat pro jednotlivé správcovské domény (ADOM)
- Automatizovaná správa kvót podle nastavených pravidel

- Grafické zobrazení trendů pomáhá při nastavování pravidel na sledování využití

Log Fetch pro forenzní analýzu

- Možnost zpětného vyhledávání v archivovaných záznamech kvůli forenzní analýze z historických dat
- Flexibilní možnosti výběru z archivu: vše, nebo pouze vybrané záznamy za určité časové období
- Snadné nastavení vzdáleného získávání archivovaných záznamů ze serveru na několik kliknutí

Předávání záznamů dalším systémům

- Předávání záznamů systémům jako Syslog server, CEF log server nebo FortiAnalyzer pro účely dlouhodobého ukládání, forenzní analýzy nebo jako zákonná povinnost
- Flexibilní nastavení: předávání všech záznamů nebo pouze vybraných na základě filtrů
- Možnost nastavit, která pole záznamu budou předávána serverům Syslog nebo CEF