Příloha č. 1 – Technická specifikace

Technické požadavky zadavatele

[1 Obecné požadavky na celé řešení 2](#_Toc13644303)

[2 Realizace centrálních firewallů včetně systémů pro jejich analyzování, vyhodnocování a reportování klíčových bezpečnostních a komunikačních parametrů 2](#_Toc13644304)

[2.1 Požadavky na Centrální Firewall (2 ks v režimu HA) 2](#_Toc13644305)

[2.2 Požadavky na Firewall do vzdálených lokalit (dvě lokality, celkem 4 ks) 4](#_Toc13644306)

[2.3 Požadavky na centrální správu všech Firewallů 4](#_Toc13644307)

[2.4 Požadavky na Antivirové řešení na klientech 5](#_Toc13644308)

[3 Požadavky na nástroj pro Management logů 6](#_Toc13644309)

[4 Požadavky na nástroj SIEM 7](#_Toc13644310)

[5 Definice rozsahu dodávky 8](#_Toc13644311)

# Obecné požadavky na celé řešení

Zadavatel požaduje splnění všech požadavků v běžném provozu.

Součástí nabízeného řešení musí být všechny potřebné optické členy, propojovací/patch a napájecí kabely. Zařízení musí fungovat jako celek bez nutnosti instalace dalších komponent

# Realizace centrálních firewallů včetně systémů pro jejich analyzování, vyhodnocování a reportování klíčových bezpečnostních a komunikačních parametrů

Požadavky na celý systém jsou rozděleny do několika částí, ale ve výsledku tvoří jeden funkční celek s unifikovaným a jednotným GUI.

## Požadavky na Centrální Firewall (2 ks v režimu HA)

Oba Firewally budou umístěny v jedné lokalitě, každý z Firewallů bude umístěn v jiném datovém centru. Pro jejich propojení je plánováno využití MM optických vláken, které jsou ukončeny v obou datových centrech, v optické vaně osazené LC konektory.

| **Název požadavku** | **Popis požadavku** | **Míra splnění (ANO/NE)** |
| --- | --- | --- |
| Typ | HW Appliance do Racku | Doplní účastník |
| Velikost | Max. 2U | Doplní účastník |
| Redundance | Active-Active/Active-Standby s automatickou synchronizací konfigurace | Doplní účastník |
| Zdroje / napájení | Redundantní | Doplní účastník |
| Lokální disky / úložiště | Redundantní (min. RAID1) | Doplní účastník |
| Počet virtuálních FW/kontext/VDOM/… | Min. 5 | Doplní účastník |
| Požadavek na virtuální FW/kontext/VDOM/… | Manuální přirazení HW CPU a RAM zdrojů pro jednotlivé virtuální FW/kontext/VDOM/… | Doplní účastník |
| Požadavek na virtuální FW/kontext/VDOM/… | Load balancing virtuálních firewall instancí mezi fyzické členy clusteru firewall platformy | Doplní účastník |
| Požadavek na virtuální FW/kontext/VDOM/… | Možnost L2 přepínaní a L3 směrovaní paketů mezi virtuálními firewally, a mezi virtuálními firewally a externími segmenty | Doplní účastník |
| Počet 10GE portů SFP+ pro připojení k LAN/WAN, synchronizaci clusteru | Min. 4 | Doplní účastník |
| Počet 10GE SFP+ MM modulů jako součást dodávky pro každý box | Min. 4 | Doplní účastník |
| Agregace fyzických portů | Podpora agregace fyzických 10GE portů LACP (802.3ad) v HW | Doplní účastník |
| Počet 1GE portů RJ45 | Min. 8 | Doplní účastník |
| Propustnost v režimu Firewall | Min. 40Gbps | Doplní účastník |
| Propustnost v režimu IPS/IDS | Min. 20Gbps | Doplní účastník |
| Propustnost v režimu NGFW (Firewall, Application control, IPS/IDS) | Min. 10Gbps | Doplní účastník |
| Propustnost v režimu Threat Prevention | Min. 5Gbps | Doplní účastník |
| Propustnost VPN (SSL) | Min. 2Gbps | Doplní účastník |
| Propustnost VPN (IPSec) | Min. 5Gbps | Doplní účastník |
| Počet SSL VPN uživatelů (zalicencovaných) | Min. 250 | Doplní účastník |
| Požadovaná funkcionalita | FW, Application Control, IDS, IPS, Antivirus, AntiSpam, URL filtering, VPN, VPN SSL, VPN S2S, DLP | Doplní účastník |
| Požadovaná funkcionalita | Tenký VPN klient (možnost použití pouze VPN klienta bez dalších funkcionalit) | Doplní účastník |
| Podporované OS pro VPN klienty | Minimálně Microsoft Windows, Apple Mac OS, Apple iOS, Android | Doplní účastník |
| Ukládání logů | Možnost lokálního ukládání logů při výpadku centrálního managementu | Doplní účastník |
| Ukládání logů | Lokální úložiště min. 400GB pro případ výpadku centrálního managementu | Doplní účastník |
| Ukládání logů | Bezpečnostní logy musí být ukládány na fyzicky oddělený management | Doplní účastník |
| Ukládání logů | Plnohodnotná integrace s dodávaným LOG serverem a nástrojem typu SIEM | Doplní účastník |
| Požadavek na IPS | Předdefinované IPS/IDS politiky od výrobce | Doplní účastník |
| Požadavek na IPS | Možnost definice IPS výjmek dle kombinace: zdrojová IP, cílová IP, služba, signatura | Doplní účastník |
| Požadavek na IPS | Možnost vypnutí IPS ochrany pro konkrétní virtuální firewall instance v případě přetížení HW zdrojů | Doplní účastník |
| Politiky | Definice politik na základě uživatele (User-Based Policy) | Doplní účastník |
| Integrace | Integrace s Microsoft AD pro vyčítání uživatelů pro uživatelské politiky | Doplní účastník |
| Integrace | Ověřování VPN uživatelů v Microsoft AD | Doplní účastník |
| Aktualizace signatur | Aktualizace signatur Antivirus, AntiSpam, IDS, IPS po celou dobu podpory řešení | Doplní účastník |

## Požadavky na Firewall do vzdálených lokalit (dvě lokality, celkem 4 ks)

|  |  |  |
| --- | --- | --- |
| **Název požadavku** | **Popis požadavku** | **Míra splnění (ANO/NE)** |
| Typ | HW Appliance | Doplní účastník |
| Počet | 2ks do každé lokality, celkem 4ks | Doplní účastník |
| Velikost | Max. 1U | Doplní účastník |
| Redundance | Active-Active/Active-Standby s automatickou synchronizací konfigurace | Doplní účastník |
| Počet 1GE portů RJ45 | Min. 8 | Doplní účastník |
| Propustnost v režimu Firewall | Min. 4Gbps | Doplní účastník |
| Propustnost VPN (IPSec) | Min. 1Gbps | Doplní účastník |
| Požadovaná funkcionalita | FW, VPN (IPSec - S2S) | Doplní účastník |
| Ukládání logů | Možnost lokálního ukládání logů při výpadku centrálního managementu | Doplní účastník |
| Lokální úložiště | Min. 30GB pro případ výpadku centrálního managementu | Doplní účastník |
| Ukládání logů | Plnohodnotná integrace s dodávaným LOG serverem a nástrojem typu SIEM | Doplní účastník |
| Politiky | Definice politik na základě uživatele (User-Based Policy) | Doplní účastník |
| Integrace | Integrace s Microsoft AD pro vyčítání uživatelů pro uživatelské politiky | Doplní účastník |
| Aktualizace signatur | Aktualizace signatur Antivirus, AntiSpam, IDS, IPS po celou dobu podpory řešení | Doplní účastník |

## Požadavky na centrální správu všech Firewallů

| **Název požadavku** | **Popis požadavku** | **Míra splnění (ANO/NE)** |
| --- | --- | --- |
| Typ | HW Appliance nebo VM v prostředí VMware | Doplní účastník |
| Požadavek | Centrální jednotná správa politik všech dodávaných FW z jednoho GUI | Doplní účastník |
| Ukládání logů | Centrální ukládaní logů ze všech dodávancýh Firewallů | Doplní účastník |
| Objem logů ze všech firewallů za den | Min. 6GB za den | Doplní účastník |
| Požadavek na management | Konsolidovaný centrální management politik, analýza logů a reporting na jednom zařízení (případně jednom virtuálním serveru) | Doplní účastník |
| Požadavek na management | Možnost sledování zatížení/využití CPU, RAM, počet spojení, počet nových spojení graficky v reálném čase | Doplní účastník |
| Požadavek na management | Možnost prohledávání logů ze všech dodávaných Firewallů a ze všech funkcionalit na jednom místě | Doplní účastník |
| Požadavek na management | Možnost filtrování logů min. dle zdroje, funkcionality, zdrojové IP, cílové IP, síťové služby | Doplní účastník |
| Požadavek na management | Možnost vytváření uživatelských grafických reportů | Doplní účastník |
| Administrátorské účty | Podpora administrátorských účtů s definovanými oprávněními (zápis, čtení, ...) | Doplní účastník |
| Administrátorské účty | Možnost přidělení práv administrátorům jen pro definovaný seznam politik | Doplní účastník |
| Politiky | Definice politik na základě uživatele (User-Based Policy) | Doplní účastník |
| Integrace | Integrace s Microsoft AD pro vyčítání uživatelů pro uživatelské politiky, VPN atd. | Doplní účastník |

## Požadavky na Antivirové řešení na klientech

|  |  |  |
| --- | --- | --- |
| **Název požadavku** | **Popis požadavku** | **Míra splnění (ANO/NE)** |
| Požadovaná funkcionalita | Klient Anitivirového řešení integrovaný s klientem pro SSL VPN | Doplní účastník |
| Požadovaná funkcionalita | AntiMalware, AntiVir, AntiPhising, AntiRansomware, AntiBot, Application Control, Compliance | Doplní účastník |
| Centrání správa | Ano | Doplní účastník |
| Podporované OS | Minimálně Microsoft Windows, Apple Mac OS | Doplní účastník |
| Možnosti instalace | Podpora automatické instalace např. MSI balíček | Doplní účastník |
| Počet klientů | 400 | Doplní účastník |

# Požadavky na nástroj pro Management logů

| **Název požadavku** | **Popis požadavku** | **Míra splnění (ANO/NE)** |
| --- | --- | --- |
| Typ | HW Appliance do Racku | Doplní účastník |
| Připojení do LAN | Redundantní, pomocí agregace min. 2 fyzických portů GE RJ45 | Doplní účastník |
| Počet zařízení pro sběr logů (zalicencovaných) | Min. 1500 | Doplní účastník |
| Počet Logů za vteřinu | Min. 5000 Logů za vteřinu | Doplní účastník |
| Objem logů za den | Min. 150GB za den | Doplní účastník |
| Počet dní po které budou uchovávany logy | Min. 200 dní | Doplní účastník |
| Celkový objem uložených logů | Min. 30TB | Doplní účastník |
| Redundance disků | Min. redundance pro výpadek jednoho fyzického disku | Doplní účastník |
| Sběr a automatické parsování logů | Sběr a parsování logů z nabízených Firewallů a nabízeného Antivirového řešení | Doplní účastník |
| Sběr a automatické parsování logů ze zařízení v síti Zadavatele | Aktivní prvky HUAWEI/Cisco, OS Windows/Windows Server/Linux, VMWare, FlowMon, Novicom AddNet | Doplní účastník |
| Požadovaná funkcionalita | Sběr logů minimálně ve formátech RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259 | Doplní účastník |
| Požadovaná funkcionalita | RealTime / Online vyhledávání ve všech uložených logách za celou dobu | Doplní účastník |
| Požadovaná funkcionalita | Sběr logů z operačních systémů Windows/Windows Server za pomoci agentů | Doplní účastník |
| Požadovaná funkcionalita | Možnost definice vlastních pravidel zpracování logů | Doplní účastník |
| Požadovaná funkcionalita | Možnost vizuálního / grafického programování, resp. definici pravidel pro zpracování logů | Doplní účastník |
| Požadovaná funkcionalita | Systém musí umožňovat grafickou vizualizaci logů a událostí v čase | Doplní účastník |
| Požadovaná funkcionalita | Možnost definice vlastních alertů / tresholdů | Doplní účastník |
| Požadovaná funkcionalita | Jednotné GUI pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa i analýza logů. | Doplní účastník |
| Administrátorské účty | Podpora administrátorských účtů s definovanými oprávněními (zápis, čtení, ...) | Doplní účastník |
| Počet Windows/Windows Server OS | 500 | Doplní účastník |

# Požadavky na nástroj SIEM

| **Název požadavku** | **Popis požadavku** | **Míra splnění (ANO/NE)** |
| --- | --- | --- |
| Typ | HW Appliance do Racku | Doplní účastník |
| Počet zařízení pro sběr logů (zalicencovaných) | Min. 1500 | Doplní účastník |
| Počet Logů za vteřinu | Min. 5000 Logů za vteřinu | Doplní účastník |
| Počet dní po které budou uchovávany logy | Min. 200 dní | Doplní účastník |
| Celkový objem uložených logů | Min. 30TB | Doplní účastník |
| Redundance disků | Min. redundance pro výpadek jednoho fyzického disku | Doplní účastník |
| Sběr logů | Sběr logů z nabízených Firewallů a nabízeného Antivirového řešení | Doplní účastník |
| Sběr logů ze zařízení v síti Zadavatele | Aktivní prvky HUAWEI/Cisco, OS Windows/Windows Server/Linux, VMWare, FlowMon, Novicom AddNet | Doplní účastník |
| Požadovaná funkcionalita | Okamžitá normalizace a korelace událostí | Doplní účastník |
| Požadovaná funkcionalita | RealTime / Online vyhledávání ve všech uložených logách za celou dobu | Doplní účastník |
| Požadovaná funkcionalita | Sběr logů z operačních systémů Windows/Windows Server za pomoci agentů | Doplní účastník |
| Požadovaná funkcionalita | Definice retenčních politik | Doplní účastník |
| Požadovaná funkcionalita | Možnost definice vlastních pravidel zpracování logů | Doplní účastník |
| Požadovaná funkcionalita | Možnost vizuálního / grafického programování, resp. definici pravidel pro zpracování logů | Doplní účastník |
| Požadovaná funkcionalita | Systém musí umožňovat grafickou vizualizaci logů a událostí v čase | Doplní účastník |
| Požadovaná funkcionalita | Možnost definice vlastních alertů / tresholdů | Doplní účastník |
| Soulad se Zákonem č. 181/2014 Sb. o kybernetické bezpečnosti, který nařizuje zavedení konkrétních technických opatření a to: | § 11 - Řízení přístupu a bezpečné chování uživatelů § 21 - Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů § 22 - Nástroj pro detekci kybernetických bezpečnostních událostí § 23 - Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí | Doplní účastník |
| Administrátorské účty | Podpora administrátorských účtů s definovanými oprávněními (zápis, čtení, ...) | Doplní účastník |
| Počet Windows/Windows Server OS | 500 | Doplní účastník |

# Definice rozsahu dodávky

Systém, jako funkční celek, bude nasazen v následujícím rozsahu:

|  |  |
| --- | --- |
| **Položka** | **Počet** |
| Centrální Firewall | 2 ks |
| Firewall do vzdálených lokalit | 4 ks |
| Centrální správa všech Firewallů | 1 ks |
| Antivirové řešení na klientech | 1 ks |
| Nástroj pro Management logů | 1 ks |
| Nástroj SIEM | 1 ks |