1. Migrace a instalace + HW + licence MS

Popis stávajícího řešení:
V současné době KKKV provozuje servery s následující funkcionalitou.
Jde o virtuální servery s operačním systémem **Windows 2008R2** a jako virtualizační platforma bude sloužit **VMware ve verzi 5.1.**

Migrace proběhne na stávajícím HW KKKV a je popsána viz níže.

Aktuální HW v KKKV:

Virtualizace

2x HP ProLiant BL460C G6, 8 CPUs x 2,66 GHz, 96 GB RAM, VMware 5.1.0 799733
Procesor Sockets: 2, Cores per socket 4, Logical procesor: 16,
Využití ESX
esx1 20-45% CPU, 50 GB RAM
esx2 20-450% CPU 45 GB RAM
1x HP ProLiant BL460C G8, 12 CPUs x 2,0 GHz 128 RAM, VMware 5.1.0 799733
Procesor Sockets: 2 Cores per socket 6, Logical procesor: 24
Využití ESX
esx3 10% CPU, 90 GB RAM

Diskové prostory virtualizace

SAN1 - SAN4 - fyzické prostor: 1,6 TB, 682 GB, 3,27 TB, 1,09
SAN 1 - SAN4 - volné prostory: 1,05 TB, 256 GB, 1,63 TB, 964 GB)

Připojení k internetu + stávající připojení :

- Wolfnet - Down: 100 Mb/s Up: 100 Mb/s
- 140x zařízení - Serverů, PC, Vzdělávací, veřejnost PC
- max. 60x zařízení připojení přes WiFi
- Antivirová ochrana – SYMANTEC ENDPOINT PROTECTION 12.1.6. (licence 120+20) + lokálně SYMANTEC ENDPOINT PROTECTION 14. (Win10)
- Firewall – TMG – ForeFront 2010 + GFI WebMonitor 2013

Server V1

- DNS, DHCP, Active Directory (Zaměstnanci)
- SYMANTEC ENDPOINT PROTECTION 12.1.x - konzole
- Sdílené složky
- Klient CA BrighStore

Server V2

- DNS, DHCP, Active Directory (Veřejnost)
- SYMANTEC ENDPOINT PROTECTION 12.1.x - konzole
- Sdílené složky
- Klient CA BrighStore

Server V3

- Kerio Connect - 8.2.4 (2550) x86. Licencováno pro **100** uživatelů
- Klient CA BrighStore

Server V5

- FileZilla Server 0.9.56 beta (odkládání dat z Escaneru do složky escan)
- Sdílené složky
- Klienta CA BrighStore

Server zálohy

Zálohovací server s aplikací **CA BrighStore** pro V1, V2, V3, V5 - data uložena na NAS(1)

Popis cílového stavu:

Je poptáváno softwarové vybavení a práce pro migraci stávajících serverů na platformu Windows Server 2016 dle následujícího popisu cílového stavu a požadavků na instalaci serverů a aplikací. Všechny dále zmíněné servery budou virtuální a jako virtualizační platforma bude sloužit **VMware ve verzi 5.5**. Migrace bude prováděna na stávajícím HW KKKV určeného pro virtualizaci. Následně musí být splněna funkčnost jako na verzi **VMware ve verzi 5.1**. a to se všemi souvisejícími službami: např. VMware vCenter Server Appliance, 4x vSphere Data Protection, nastavení skriptů a funkčnosti - Revert (vrací zpět virtuální server k danému snapshotu) a Save Snathot (vytváří snapshot severu). Které budou na novém migrovaném serveru pro Veřejnost - V2. Pro ovládání serverů TS02, TS03, TS04.

Virtuální server V1

Migrace konfigurace a nastavení ze stávajícího serveru V1 a to především:

- Instalace **Windows Server 2016**
- Migrace **Active Directory**. V rámci migrace je požadována aktualizace stávající struktury Active Directory na Windows 2016 na funkční level 2016.
- Migrace nastavení **DNS**
- Migrace nastavení **DHCP**
- Přenesení sdílených složek + nastavení práv dle požadavků KKKV.
- Nastavení Kvót u sdílených složek dle požadavků KKKV.
- Nastavení propojení autentifikace **Safeq** serverů S2 s V7 do Active Directory tohoto serveru.
- Nastavení propojení autentifikace serveru **v Dochazka** do Active Directory tohoto serveru.
- Instalace klienta/ lokální **SYMANTEC ENDPOINT PROTECTION 14**
- Instalace a nastavení klienta **CA BrighStore** (zálohovací řešení)
- Instalace **VMware Tools**
- Přidání všech PC do Active Directory v součinnosti s KKKV.

Virtuální server V2

Migrace konfigurace a nastavení ze stávajícího serveru V2 a to především:

- Instalace **Windows Server 2016**
- Migrace **Active Directory**. V rámci migrace je požadována aktualizace stávající struktury Active Directory na Windows 2016 na funkční level 2016.
- Migrace nastavení **DNS**
- Migrace nastavení **DHCP**
- Přenesení sdílených složek + nastavení práv dle požadavků KKKV.
- Instalace klienta/**lokální SYMANTEC ENDPOINT PROTECTION 14**,
- Instalace a nastavení klienta **CA BrighStore** (zálohovací řešení)
- Instalace **VMware Tools**
- Přidání všech PC do Active Directory v součinnosti s KKKV.
- nastavení skriptů a funkčnosti - Revert (vrací zpět virtuální server k danému snapshotu) a Save Snathot (vytváří snapshot severu).

Emailový server V3 (virtuální server)

Migrace konfigurace a nastavení ze stávajícího serveru V3 a to především:

- Instalace Windows Server 2016

- Migrace stávajícího řešení + aktualizace emailového serveru na aktuální verzi
- Instalace klienta/ lokální SYMANTEC ENDPOINT PROTECTION 14
- Instalace VMware Tools

Datový server V5 (virtuální server)

Migrace konfigurace a nastavení ze stávajícího serveru V5 a to především:

- Instalace Windows Server 2016
- Instalace a konfigurace FTP server (Filezilla Server)
- Nastavení sdílených složek pro aplikace dle požadavků KKKV
- Instalace klienta/ lokální SYMANTEC ENDPOINT PROTECTION 14
- Instalace VMware Tools

Zálohovací Server - sever CA BrighStore - fyzický server - (HP Proliant DL 380 - G4)

Migrace konfigurace a nastavení ze stávajícího zálohovacího serveru a to především:

- Instalace **Windows 2008 R2 (64bit)**
- Instalace a konfigurace **CA BrighStore -Server**
- Nastavení **zálohovaní dat** z klientských serverů na:
  - nový **NAS** součástí výběrového řízení
  - pásková mechanika **HP DAT 72x6**

NAS - Datové úložiště - externí box pro 4x 2.5/3.5" SATA III HDD/SSD, Intel minimálně 2.0GHz Quad-core, **RAID** (Basic/JBOD/0/1/5/6/10), 4GB DDR3L RAM, 2x GLAN, 2x USB 3.0, eSATA

+ k NAS zařízení je potřeba přidat disky
4x 6TB Pevný disk 3.5" **SATA III**, 128MB cache, 7200ot, určeno pro datová centra
+ 1x 6TB Pevný disk 3.5" **SATA III**, 128MB cache, 7200ot, určeno pro datová centra (náhradní)

Sekundární DNS - Samostatné servery - Windows 2016

1x **Sekundární DNS, DHCP, Active Directory** - Samostatný server - Windows 2016 - záložní DNS, DHCP, Active Directory

- pro VLAN: **Zaměstnanci**
- Instalace Windows 2016 (64bit)
- Instalace a konfigurace sekundárního DNS DHCP, Active Directory a začlenění do infrastruktury KKKV

1x **Sekundární DNS DHCP, Active Directory** - Samostatný server - Windows 2016 - záložní DNS, DHCP, Active Directory - pro VLAN: **VZC, Veřejnost**.

- Instalace Windows 2016 (64bit)
- Instalace a konfigurace sekundárního DNS, DHCP, Active Directory a začlenění do infrastruktury KKKV

WSUS - Samostatné servery - Windows 2016

1x **WSUS** - Samostatný server - Windows 2016 - WSUS aktualizace **VLAN Zaměstnanci**

- Instalace Windows 2016 (64bit)
- Instalace a konfigurace WSUS pro VLAN Zaměstnanci
- nastavení a otestování Windows Update pro servery KKKV a PC

Firma řeší všechny vzniklé problémy ve spolupráci s KKKV dle požadavků KKKV. Musí být zachována funkčnost před migrací.
Součástí dodávky je dokumentace a zaškolení (bude dále specifikováno).

2. Firewall

2.1. Firewall

Je požadováno dodání 1ks fyzického firewallu, který splňuje vlastnosti dle následující specifikace:

Technická specifikace

Základní vlastnosti

- Montáž do 19“ racku
- 1 napájecí zdroj AC

Kapacitní požadavky a počty portů

- Počet WAN rozhraní copper, RJ45 RJ45 10/100/1000 – min 2x
- Počet interních síťových rozhraní copper, RJ45 10/100/1000 - min 12x.
- Počet SFP: 2 x GbE SFP.
- 1x console port

Výkonnostní parametry HW

- RIP, BGP, OSPF, IS-IS.
- Policy routing.
- Traffic Shaping, QoS s podporou DSCP markování a ToS.
- Bezdrátový kontrolér, podpora vytváření inteligentní bezdrátové sítě, funkce ARRP (Automatic Radio Resource Provisioning), možnost detekce a reportování tzv. Rogue AP), bezdrátová sítě je založená na principu tenkých AP s inteligentní správou kontrolérem.
- Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu.
- WAN optimalizace (optimalizace vybraných protokolů, byte chaching), Web Cache, Explicitní Proxy, Reverzní proxy, WCCP.
- Podpora silné autentizace uživatelů - integrovaná podpora generátor jednorázových hesel (OTP) - dvoufaktorová autentizace, podpora certifikátů pro ověření uživatelů.
- Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B- min 7.0/ 7.0 / 4.0 Gbps
- Latence firewallu (64 B UDP paket) - max. 5 mikro sec.
- Výkon firewall **cca** 6.0Mpps
- Počet naráz otevřených spojení – min 1,8 M.
- Počet nových spojení za sekundu - min. 25 000.
- Propustnost IPSEC VPN (512 B paket) - min. 3,5 Gbps.
- Propustnost SSL VPN min 250 Mbps.
- Propustnost IPS – min 1,7 Gbps
- Podpora virtualizace (min 10 virtuálních kontextů).
- Podpora funkce bezdrátový kontrolér
- Integrovaná podpora

Funkce L2/L3

- Podpora pro režim vysoké dostupnosti, L2, Active Active, Active Passive, full mesh HA, VRRP, synchronizace stavové tabulky mezi nódy v clusteru.
- Režim fungování L2 - transparentní režim, L3 - NAT/Router.
- Podpora multicast, vytváření politiky pro multicast routování.
- Podpora High availability - v budoucnosti zakoupení druhého firewallu

Podpora VPN

- (portálový režim, tunelový režim), podpora protokolu

Funkce firewallu

- Možnost nastavovat firewall politiku na základě geografických údajů.
- Podpora Identity based policy - nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru.
- Funkce Load Balancing - možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora healt check funkcí, podpora SSL offload.
- Podpora centrální NATovácí tabulky, stavová inspekce SCTP komunikace.
- UTM funkce, možnost výběru mezi file based režimem (buffer) nebo flow based (inspekce on-the-fly).
- Antivirus pro vybrané protokoly, možnost volby různých databází, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV engine, možnost detekce tzv. Grayware (rootkit, malware, spywave, keylogger, atd).
- E-mail filter - jednoduchá antispamová a antivirová inspekce elektronické pošty.
- Intrusion Protection System - detekce útoků založena na signaturové části a na anomálním filtru, možnost vytvářet vlastní signatury.
- Web Filter - založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorii na uživatele či skupinu, možnost kvóty - uživatel může navštěvovat určitou kategorii jen po určitou dobu během dne.
- Data Leak Prevention s funkcí document fingerprinting.
- Application Control - detekce, monitoring, povolení či zakázání síťových aplikací na základě signatury dané aplikace, nikoliv dle portu.
- Deep scanning - možnost kontroly komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S,…).
- DoS Policy prevence proti základním útokům typu DoS, syn proxy.
- Endpoint Control a monitoring - kontrola připojené pracovní stanice na patch level, instalovaný vhodný service pack, antivirový software, personální firewall či jiný software.
- Vulnerability Scan - možnost naplánování aktvního testu vnitřní sítě na známé zranitelnosti, test je založen na signaturové databázi. Možnost vygenerování report.
- Ověřování uživatelů LDAP, Active Directory, ověřování na základě certifikátu
- Dynamické profily - možnost přiřadit konkrétní profil uživateli na základě jeho ověření.

Management

- Cluster boxů s full UTM supportem celkem na 3 roky

Podpora

- Záruka 3 roky, v režimu 24hod x 7dnů.
- Podpora včetně AV/AS, IPS, App. Control a Webfiltering.

Konfigurační požadavky

- Konfigurace WAN připojení včetně zakončení 4 veřejných IP adres.
- Konfigurace VLAN dle požadavků KKKV (cca 5ti VLAN s možností rozšíření na 10).
- Napojení na 2 domény Active Directory (zaměstnanci a veřejnost) a autorizace uživatelů.
- Nastavení filtrování a blokace nevhodné komunikace (P2P sítě, Torrent, Spotify atd).
- Filtrování webů dle obsahu a následná blokace webů (pornografii, sex, zbraně, drogy, sociální sítě, produktivita práce. atd).
- Konfigurace pravidel dle stávajícího firewallu nebo ekvivalentních po schválení KKKV (**cca 150 pravidel**).
- Nastavení VPN – **3x profily**
    - **1x Administrator, 1x zaměstnanci, 1x pobočka; celkem 15 uživatelů.**

Firma řeší všechny vzniklé problémy ve spolupráci s KKKV dle požadavků KKKV. Musí být zachována funkčnost před migrací. Součástí dodávky je dokumentace konfigurace firewallu a zaškolení (bude dále specifikováno).

2.2. Systém pro ukládání a korelaci logů

Je požadováno dodání systému pro ukládaní a korelaci provozních logů firewallu (dále jen logovací systém), který poskytne rozšířenou funkcionalitu a analýzu logů firewallu a to:

- Logovaní dat z více firewallů (je plánováno zakoupení druhého kusu firewallu pro zajištění Hight availability módu).
- Logování dat po dobu minimálně 12ti měsíců – nyní cca 35 GB dat měsíčně (z TMG 25GB, z GFI 10GB)
- Možnost tvorby užití výrobcem definovaných a uživatelsky vytvořených pravidel pro upozornění na závadnou činnost.
- Možnost tvorby reportů vyhodnocujících chování uživatelů a aplikací.
- Možnost vyhledávaní v datech provozu dle zdrojové nebo cílové adresy, aplikace nebo cílového portu a export těchto dat.
- pokud bude použit virtuální server možnost zvětšování disk prostoru.
- pokud bude použit virtuální server Windows nutno zakoupit licenci Windows 2016 (x64 bit)

Pro logovací systém je požadována instalace na vlastním hardware firmy (appliance nebo hardware dodaný firmou) nebo do virtuálního prostředí KKKV, které je provozováno na platformě vmWare 5.1.
Součástí řešení musí být všechny nezbytné licence pro provoz logovacího systému a dostatečné diskové nebo logovací kapacity, pokud je použité jiné než virtualizované řešení nebo je množství logovaných dat licenčně omezeno, pro ukládaní logů firewallu dle dále specifikovaných požadavků. Součástí dodávky musí být licence pro operační systém, pokud toto řešení vyžaduje pro svůj provoz licencovaný operační systém. V případě OS Windows je požadována verze **Windows server 2016 (64bit) + licence Win 2016 (64bit)**
Je požadováno, aby do řešení bylo možné připojit druhý firewall bez nutnosti rozšíření licence.

Popis cílového stavu:
Je požadováno dosažení následujícího cílového stavu:

- instalace a konfigurace logovacího systému
- konfigurace firewallu pro ukládání logů do logovacího systému, nastavení retencí pro uchovávaní dat
- vytvořené 10ti pravidel a 10ti reportů dle požadavků KKKV
- Jednoduché stažení dat dle IP v případě incidentu
- firma řeší všechny vzniklé problémy ve spolupráci s KKKV a dle požadavků KKKV
- Zaškolení zaměstnanců KKKV (rozsah bude dále specifikován).
- Vytvoření dokumentace popisující cílový stav (rozsah bude dále specifikován).

Součástí dodávky je zakoupení podpory pro řešení na 3 roky.

3. Aktualizace a migrace Symantec Endpoint Protection Manager

Popis stávajícího řešení:
Symantec Endpoint Protection Manager konzole je v současné době provozována ve dvou oddělených instancích a to:

- Instance na serveru V1 (zaměstnanci) - s 40 x Windows 7 a XP + (přidání 10 PC s Windows 10 - prozatím lokální instalace)
- Instance na serveru V2 (veřejnost) - 10x Windows 10, Win 2008 (klienti SYMANTEC ENDPOINT PROTECTIONu) + (přidání 3x PC s Windows 10 - prozatím lokální instalace)

Obě instance jsou provozovány na virtualizovaných serverech s operačním systémem Windows 2008R2 (64bit).

Popis cílového stavu:
Je požadováno dosažení následujícího cílového stavu:

- Upgrade antivirového systému Symantec Endpoint Protection 12.1x na verzi 14.x a jeho přenesení na virtuální server V1 a virtuální server V2, které jsou popsané v bodu 1 tak, že:
    - 1x Instalace Windows 2016 (x64 bit) pro VLAN Zaměstnanci 1x Instalace Windows 2016 (x64 bit) pro VLAN VZC, Veřejnost, WiFi
    - Symantec Endpoint Protection 14.0.1 management Console - konzole na virtuálním serveru 1 bude sloužit pro stanice v síti Zaměstnanci
    - Symantec Endpoint Protection 14.0.1 management Console- konzole na virtuálním serveru 2 bude sloužit pro síť Veřejnost, VZC, WiFi
    - Firma ve spolupráci s KKKV řeší možné problémy, které vzniknou při migraci a instalaci antivirového programu na servery a klientské PC dle požadavků KKKV k zajištění plné funkčnosti, které musí byt minimálně zachována jako před migrací. A to především:
        - Ochrana před viry a spywarem
        - Lokální firewall
        - Prevence narušení
        - Řízení aplikací a zařízení
        - Live Update
        - Výjimky
        - Rozdělení klientů do skupin dle rozdělení KKKV
        - Vytvoření instalačních balíčků pro 32 a 64 bit
        - Testovací instalace na PC a aplikování pravidel.
- Zaškolení zaměstnanců KKKV (rozsah bude dále specifikován).
- Vytvoření dokumentace popisující cílový stav (rozsah bude dále specifikován).

4. Prodloužení podpory HP pro stávající HW

Je požadováno prodloužení záruky stávajícího HW o 1 rok, s platností od konce platnosti stávající podpory v září 2018. Požadovaná záruku minimálně na úrovní HPE FC NBD
Seznam stávajícího HW:

HP P2000 Dual I/O LFF Drive Enclosure	SN: 2S6223D459
HP B-series 8/12c BladeSystem SAN Switch	SN: CN8226A01G
HP P2000 G3 MSA FC Dual Cntrl SFF Array	SN: 2S6029B293
HP BLc7000 CTO 3 IN LCD ROHS Encl	SN: GB80323KEW

5. Licence

Je požadováno dodání všech licencí nutných pro instalaci aktualizovaných serverů definovaných v bodech 1 a 3, případně dalších serverů nutných pro provoz řešení definovaného v bodu 2 nebo dále vyžadovaných firmou pro korektní funkcionality navrhovaného řešení. Je požadováno použití Windows Sever 2016 (64bit) pro virtuální server. Fyzický server je osazen 2x CPU s 8 Core per CPU) + 4x licence Windows Windows Sever 2016 (64bit).
Je požadováno dodání **120 ks device** Windows server 2016 CAL.

6. Zaškolení

Je požadováno zaškolení personálu KKKV v následujícím rozsahu
Servery – 1 MD
Práce se Symantec Endpoint Console dle specifikace KKKV – 0,5 MD
Základní konfigurace FW – 1 MD
Základní práce se systémem pro ukládání a korelaci logů – 1 MD
Zaškolení práce s Firewallem - 1MD

7. Dokumentace

Je požadováno vytvoření dokumentace popisující cílový stav jednotlivých prací a to

- dokumentace, kde budou specifikovány technické parametry a konfigurační změny nad rámec standardní instalace a katalog instalovaných aplikací dle seznamu požadavků definovaných v bodu 1 a včetně
    - popisu uživatelských přístupů a skupin oprávnění
    - konfigurací subsystémů Windows (DNS, DHCP, Active Directory atd.) nad rámec standardní instalace
    - specifická nastavení nutné pro provoz požadovaných aplikaci
    - nastavení antiviru pro 2x řídící server
    - nastavení 2x záložní servery DNS, DHCP, Active Directory
    - nastavení WSUS - Windows Server Update Services
    - nastavení MailServeru

  případně další parametrů, které bylo nutné nastavit pro korektní provoz daného řešení.
- popis zapojení a konfigurace firewallu a software pro sběr logů dle bodu 2 a to především
    - popis uživatelských přístupů a skupin oprávnění
    - popis rozhraní a jejich adresací
    - popis použitých pravidel firewallu
    - konfigurace antivirus a antispam pravidel, pokud tato budou nastavena
    - konfigurace VPN pravidel, pokud tato budou nastavena

  případně další parametrů, které bylo nutné nastavit pro korektní provoz daného řešení.
- popis cílové konfigurace antivirového řešení Symantec v rozsahu požadovaných dle bodu 3.

- Dokumentace prováděných migrací a akcí v průběhu tohoto VŘ

8. Délka záruční doby

- 6 měsíců | práce
- Ostatní záruka je uvedena v předcházejících bodech.