Příloha č. 1: Podrobné vymezení díla

Dodávka a implementace bezpečnostních prvků komunikační sítě, ochrany e-mailové komunikace a koncových zařízení včetně zajištění následné podpory

Obsah

Příloha č. 1: Podrobné vymezení díla 1

Popis současného prostředí 3

1. Modernizace aktivních prvků komunikační sítě 3

1.1 Modernizace aktivních prvků společného bezpečnostního perimetru pro sítě LAN KÚZK a 21Net podporující ochranu proti „pokročilým hrozbám“ 3

1.1.1 NGFW 4

1.1.2 SandBox 5

1.1.3 Požadovaná implementace a integrace NGFW a SandBox 7

1.2 Modernizace aktivních prvků sítě LAN KÚZK pro možnost „adaptivního řízení“ přístupu do komunikační infrastruktury 7

1.2.1 Přístupový přepínač – 48p 7

1.2.2 Agregační přepínač 8

1.2.3 CORE přepínač 8

1.2.4 WIFI AP 9

1.2.5 Virtuální WLC 9

1.2.6 Centrální správa aktivních prvků LAN KÚZK 10

1.2.7 Cílový stav topologie a příslušenství 11

1.2.8 Požadovaná implementace a integrace 12

1.3 Modernizace aktivních prvků sítě 21Net podporující kryptaci provozu na L2 vrstvě ISO/OSI modelu 12

1.3.1 CORE router 12

1.3.2 PE MPLS přepínač 21NET 13

1.3.3 Firewally uzlových bodů 21NET 13

1.3.4 Cílový stav topologie a příslušenství 14

1.3.5 Požadovaná implementace a integrace 15

2. Nasazení mailové brány (MailGW) pro zajištění podpory ochrany příchozí i odchozí mailové komunikace KU proti pokročilým hrozbám 15

2.1 MailGW – základní funkce a vlastnosti 16

2.2 Ochrana proti spamu 17

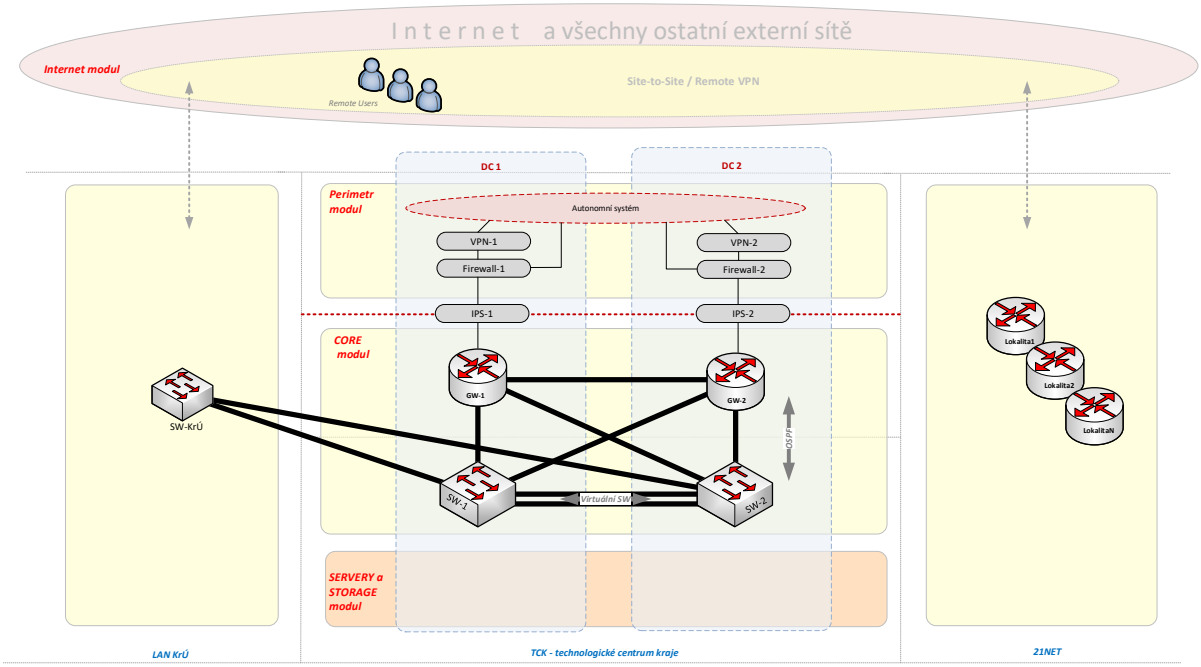
2.3 Minimální výkonnostní a systémové požadavky řešení 17

2.4 Požadovaná implementace a integrace 18

3. Modernizace SW ochrany "operačních systémů klientských a serverových zařízení" pro zajištění podpory ochrany proti pokročilým hrozbám 18
3.1 SW ochrana – základní funkce a vlastnosti 18
3.2 Požadovaná implementace a integrace 20
4. Zavedení dynamického, adaptivního řízení přístupu uživatelů a zařízení ke komunikačnímu systému lokální počítačové sítě LAN KÚZK 21
4.1 Security Enforcer – základní funkce a vlastnosti 21
4.2 Požadovaná implementace a integrace: 22
5. Požadované služby 23
5.1 Služby v rámci dodávky 23
5.2 Dokumentace 23
6. Seznam zkratek a pojmů 23

Popis současného prostředí

Základní schema aktuálního stavu



Poskytnutá virtualizační platforma

Pokud je u jednotlivých bodů nabízena možnost řešení v podobě virtualizované appliance (VApp) nebo virtual machine (VM), je možné v rámci technologického centra Objednatele (TC KÚZK, TCK) nabídnout prostředí VMWare VSphere 6.0 a OS MS Windows Server 2012/2016 DataCenter Edition. Pro chod řešení může být také poskytnuta databáze na stávajícím MS SQL 2014/2016 řešení TC KÚZK.

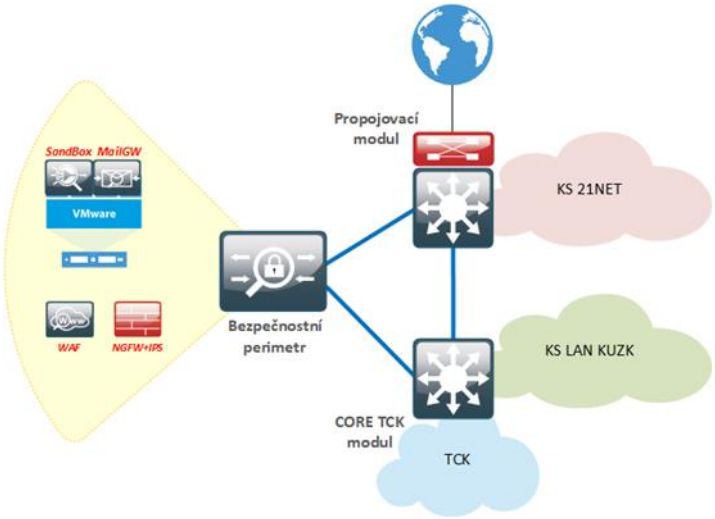
Podrobné kapacitní možnosti pro jednotlivé VApp/VM a SQL (počet vCPU, velikost operační paměti, úložiště…) jsou specifikovány níže.

1. Modernizace aktivních prvků komunikační sítě

1.1 Modernizace aktivních prvků společného bezpečnostního perimetru pro sítě LAN KÚZK a 21Net podporující ochranu proti „pokročilým hrozbám“

V rámci této části je požadována dodávka a implementace řešení NGFW a SandBoxu a vytvoření bezpečnostního ekosystému dle níže uvedené specifikace.

Jedná se o modernizaci společného bezpečnostního perimetru, která dodáním klíčového prvku NGFW sjednotí HW platformy dnes samostatných FW a IPS, umožní zde na požadovaný provoz nasazení UTM funkcí jako je WebFiltering, aplikační kontrola, antimalware kontrola s dynamickým využitím inteligenční a reputační báze výrobce. Druhým krokem je pořízení bezpečnostního prvku SandBox, který umožňuje hloubkovou kontrolu podezřelých fragmentů komunikace, včetně zazipovaných souborů, www odkazů apod. Sandbox bude integrován s HW plaformou NGFW a také s bezpečnostní Mailbránou, která je popsána v kapitole 2.



Minimální požadované funkce a vlastnosti řešení

1.1.1 NGFW

- HW platforma
- řízení bezpečného přístupu mezi vnější a vnitřní sítí
- segmentaci zejména použitím demilitarizovaných zón
- zajištění bezpečného vzdáleného přístupu pro uživatele (SSL VNP)
- zajištění blokování přenášených dat, které neodpovídají požadavkům
- podpora WAN load balancing
- IPSec VPN – propojení lokalit formou LAN-to-LAN
- podpora NGFW/UTM (AV, IPS, application control, WebFiltering)
- možnost centrálního sběru logů s následnou analýzou
- podpora Syslog pro zasílání logů
- zabezpečený management (GUI / CLI) - SSH, HTTPS přístup
- podpora IPv6
- podpora záložního připojení do internetu
- podpora dynamických směrovacích protokolů RIP, BGP, OSPF
- podpora HA nasazení v režimech Active/Pasive a Active/Active
- podpora min. 20 virtuálních instancí
- duální napájecí zdroje
- integrace s technologií SandBoxu (kapitola 1.1.2)

Minimální výkonnostní a systémové požadavky řešení

NGFW – HW platforma	
lokální úložiště	240 GB
porty	8x 10GB SFP+, 16x GE SFP, 16x GE RJ45

min. propustnost FW pro 512 byte UDP paket	60 Gbps
počet současných připojení	12 Mil
nové session/sec	300 000
propustnost IPSEC VPN	40 Gbps
Propustnost SSL inspekce	10 Gbps
propustnost application control	15 Gbps
propustnost při současně zapnutých funkcích FW, IPS, APP Control a Malware protection = threat protection	5 Gbps

1.1.2 SandBox

- HW platforma nebo vApp/VM do prostředí TC KÚZK
- webové uživatelské rozhraní a příkazová řádka
- možnost vytvořit více účtů správců
- zálohování a obnova nastavení
- upozorňování na odhalené škodlivé soubory e-mailem
- možnost reportingu
- centralizovaná stránka pro vyhledávání umožňující nastavit vlastní podmínky vyhledávání
- automatické aktualizace signatur
- automatické kontroly a stahování nových obrazů virtuálního stroje
- monitorování stavu virtuálního stroje
- ověřování správců pomocí serveru Radius nebo LDAP/AD
- podpora statického směrování
- vstup souborů od integrovaných zařízení (NGFW a MailGW)
- možnost vytvořit pro zkoumaný soubor simulované uzavřené síťové prostředí
- podpora klastrování pro vysokou dostupnost
- dynamické aktualizace databáze hrozeb a periodické předávání dynamické databáze registrovaným entitám
- databáze kontrolních součtů souborů a škodlivých URL
- vzdálený záznam událostí na syslog server
- možnost nastavení podporovaných typů souborů u virtuálních strojů
- detekce síťových hrozeb v režimu odposlechu
- identifikace aktivity botnetu a síťových útoků, návštěvy škodlivých URL
- plánovatelné prohledávání síťových úložišť sdílených přes SMB/NFS a karanténa podezřelých souborů
- kontrola URL adres vložených v dokumentech
- widgety pro monitorování v reálném čase (zobrazení podle zdroje a časového období)
- podrobný prohlížeč událostí: dynamická tabulka s detaily o akcích, názvy škodlivého softwaru, hodnocením, typem, zdrojem, destinací, časem detekce a cestou ke stažení
- záznam událostí — grafické uživatelské rozhraní, stažení protokolu ve formátu RAW

- generování reportů o škodlivých souborech: podrobné zprávy o charakteristice a chování souboru – modifikace souboru, související procesy, zásahy do registrů, chování v síti, snímek virtuálního stroje, chronologický přehled chování
- další analýza: stáhnutelné soubory — vzorek souboru, protokoly událostí v sandboxu, PCAP Capture a indikátory ve formátu STIX
- stažitelné zachycené balíčky, originální soubory, tracer logy a screenshoty
- aktivní část řešení vybavena grafickým komunikačním rozhraním v podobě HTTPS aplikace

Minimální výkonnostní a systémové požadavky řešení

Sandbox HW nebo VM platforma	
Počet podporovaných VM v ceně / maximálně	4/50
Požadované licencování OS v ceně řešení	4x Win10
Požadované licencování MS Office v ceně řešení	4x MS Office
Kapacita VM sandboxu (souborů/h)	160
Antivirová kontrola (souborů/h)	6000
Podporované OS VM	Windows 7, Windows 10, macOS, Android
podporované soubory	.7z, .ace, .apk, .arj, .bat, .bz2, .cab, .cmd, .dll, .doc, .docm, .docx, .dot, .dotm, .dotx, .exe,. gz, .htm, html, .jar, .js, .kgb, .lnk, .lzh, Mach-O, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt,.pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, url, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip
podporované protokoly v integrovaném nasazení	HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM a jejich SSL kryptované verze

Pro chod VApp/VM v prostředí TCK KÚZK bude možnost vyhrazení HW prostředků s následující charakteristikou:

Technická specifikace poskytnutého prostředí – maximální hodnoty	
počet podporovaných vCPU	8
počet virtuálních NIC	6
velikost úložiště virtuálního stroje	1 TB
velikost operační paměti virtuálního stroje	16 GB

1.1.3 Požadovaná implementace a integrace NGFW a SandBox

- integrace do provozovaného SIEM řešení
- vzájemná integrace NGFW a Sandboxu
- integrace s technologií MailGW (kapitola 2)
- migrace FW pravidel ze současného řešení a jejich profilaxe
- instalace a konfigurace dle Prováděcího projektu včetně návrhu řešení
- kvalifikované seznámení obsluhy v rozsahu min. 2 MD

1.2 Modernizace aktivních prvků sítě LAN KÚZK pro možnost „adaptivního řízení" přístupu do komunikační infrastruktury

Předmětem této části je změna topologie KS LAN KÚZK a následné sjednocení HW platformy KS, včetně bezdrátové přístupové technologie do jednotného prostředí se společným management nástrojem. Jde o dodávku a implementaci HW prvků a SW centrálního managementu. Celý tento ekosystém je nutné dále provázat s technologií adaptivního řízení přístupu (kapitola 4) a s technologií HW platformy NGFW (kapitola NGFW1.1.1).

Proti stávajícímu stavu dojde k implementaci agregační vrstvy do přístupové sítě KÚZK a to v podobě 2 ks nových „agregačních přepínačů". Dalším krokem je nasazení SW pro centrální správu prvků sítě LAN KÚZK, jak core, přístupových a agregačních přepínačů tak WiFi prvků.

Minimální požadované funkce a vlastnosti řešení

1.2.1 Přístupový přepínač – 48p

- základní L3 přepínač
- zabezpečený management (GUI / CLI)-SSH, HTTPS přístup
- podpora linkové agregace (LACP/statická)
- možnost diagnostiky a troubleshooting
- provedení do RACK -1U
- podpora VLAN
- Podpora dynamických VLAN
- Podpora ověřování 801.X
- statické routování, RIP
- podpora IPv6
- ACL pro přístup k prvku, definice ACL na úrovni VLAN
- 48x 10/100/1000 Mbit RJ45 POE+ port
- 4x SFP+ 1/10GB port
- switching kapacita 170 Gbps
- propustnost 100 Mpps
- MAC tabulka min. 32 000 záznamů
- Routing tabulka IPv4/IPv6 – 10000/5000 záznamů
- napájení PoE+ (30W / port), celkově PoE kapacita 370W
- možnost stohování switchů přes min. 2x 10 Gbps port
- režimy portu: access, trunk a hybrid
- DHCP snooping, ARP protection, port security, loopback protection
- integrace s centrální správou aktivních prvků (kapitola 1.2.6)
- tzv. zero touch provisioning

- integrace s technologií policiy enforceru (kapitola 4)

1.2.2 Agregační přepínač

- modulární L3 přepínač
- zabezpečený management (GUI / CLI) - SSH, HTTPS přístup
- možnost N+1 redundance napájení AC240V
- možnost redundance logických management karet (modulů)
- 6× 40Gb QSFP+ port
- 24× 1/10Gb SFP+ port
- 12× 1GB SFP
- 24× 10/100/1000 Base-T POE+
- 2 volné sloty pro osazení budoucích linkových karet
- podpora linkové agregace (LACP/statická)
- podpora virtuálního chassi – až 4 prvky
- možnost diagnostiky a troubleshooting
- provedení do RACK
- podpora VLAN
- Podpora dynamických VLAN
- Podpora ověřování 801.X,statické routování, RIP, OSPF
- podpora IPv6
- ACL pro přístup k prvku, definice ACL na úrovni VLAN
- switching kapacita 1200 Gbps
- propustnost 1100 Mpps
- MAC tabulka min. 64 000 záznamů
- Routing tabulka IPv4/IPv6 – 10000/5000 záznamů
- DHCP snooping, ARP protection, port security, loopback protection
- integrace s centrální správou aktivních prvků (kapitola 1.2.6)
- integrace s technologií policiy enforceru (kapitola 4)

1.2.3 CORE přepínač

- modulární Advanced L3 přepínač
- zabezpečený management (GUI / CLI) - SSH, HTTPS přístup
- N+1 redundance napájení AC240V
- 20× 40Gb QSFP+ port
- 24× 1/10Gb SFP+ port
- 24× 1/10GBase-T
- podpora linkové agregace (LACP/statická)
- podpora virtuálního chassi – min 4 prvky
- možnost diagnostiky a troubleshooting
- provedení do RACK
- podpora VLAN
- Podpora dynamických VLAN
- Podpora ověřování 801.X
- podpora VXLAN, VTEP a OVSDB

- DCB protokol
- role-based access control (RBAC)
- podpora IPv6
- statické routování, RIP, OSPFv2/v3, BGP/BGP+, Policy routing
- ACL pro přístup k prvku, definice ACL na úrovni VLAN
- switching kapacita 3,2 Tbps
- propustnost 2790 Mpps
- MAC tabulka min. 130 000 záznamů
- Routing tabulka IPv4/IPv6 – 128000/64000 záznamů
- DHCP snooping, ARP protection, port security, loopback protection
- integrace s centrální správou aktívních prvků (kapitola 1.2.6)

1.2.4 WIFI AP

- současné vysílání dualband (2,4 / 5 GHz)
- podpora AC Wave2 - napájení přes PoE
- podpora RADIUS
- podpora min. 6 SSID na jednom rádiu
- podpora 802.11 a/b/g/n/ac wave2
- podpora MIMO 3x3:3
- podpora 802.3 af/at
- zabezpečený management
- decentralizovaný management
- AP pro enterprise použití
- integrovaná anténa
- správa prvků z jednoho místa
- oddělení sítí pro jednotlivé typy uživatelů
- nastavení bezpečnosti samostatně pro každou síť
- podpora zabezpečené Guest sítě
- integrace s centrální správou aktivních prvků (kapitola 1.2.6)
- integrace s technologií policiy enforceru (kapitola 4)

1.2.5 Virtuální WLC

- virtualizovaný kontroler
- možnost běhu i na HW vlastních AP
- podpora mechanismu izolace klientů
- centralizovaná architektura správy WiFi
- centrální řešení distribuce konfigurací s podporou automatického rozložení zátěže klientů, roamingu mezi spravované access pointy a automatickým laděním kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení
- Podpora protokolu IEEE 802.1X resp. ověřování uživatelů oproti databázi účtů přes protokol radius (např. LDAP, MS AD …)
- ACL pro filtrování provozu
- Rychlá instalace i rozšíření sítě, škálovatelnost
- RF optimalizace sítě

- Automatický QoS pro hlas a video
- Vysoká dostupnost
- Integrovaný Firewall, integrované wireless IPS/IDS

1.2.6 Centrální správa aktivních prvků LAN KÚZK

- Správa autonomních AP, "tenkých" AP, fyzických i virtuálních WiFi controlérů a přepínačů.
- Licence pro správu všech dodávaných přepínačů a bezdrátových prvků, možnost flexibilního rozšiřování až do 2500 zařízení.
- Software bude dodán ve formě VApp/VM bez nutnosti pořizovat další licence např. pro OS nebo databáze.
- Manuální a automatické discovery síťových zařízení pomocí SNMP, HTTP a CDP skenování.
- Monitorovací nebo plný-managed režim pro nově objevená zařízení jako ochrana před nechtěným přepsáním konfigurace.
- RBAC pro jednotlivé síťové operátory na úrovni síťových zařízení a jejich funkcí. Možnost plného oddělení tak aby se v rámci jednoho systému dalo spravovat více samostatných entit s vlastními procesy.
- Webové uživatelské rozhraní s podporou HTTPS.
- Možnost přizpůsobení prostředí ovládací obrazovky (webový dashboard), zvlášť pro každého síťového operátora.
- Vyhledávání koncových uživatelů na základě MAC adresy, IP adresy, uživatelského jména a LAN hostname.
- Real-time monitoring každého uživatele v síti včetně charakteristik jako jsou: kvalita RF signálu, utilizace pásma (in/out), autentizační status a čas, historie roamingu, délka trvání připojení, typ klientského zařízení, asociace s SSID, objem a seznam používaných L7 aplikací a navštívených webových kategorií.
- Real-time monitoring všech připojených a řízených fyzických a virtuálních zařízení a zasílání alarmů při změnách stavu.
- Podpora sběru flow z každého připojeného zařízení
- Podpora alarmování s možností nastavitelných prahů pro jednotlivé událostí. Podporované události: odchylka od baseline konfigurace, RF metrika, nově objevené zařízení, Radius autentizace, Rogue AP, nadměrné utilizace AP (bandwidth), počet připojených klientů, nadměrná utilizace klientem (bandwidth), Up/Down zařízení, Up/Down Radio, IDS událost
- Konfigurace formu politik aplikovatelných na všechna zařízení, jejich skupinu nebo jednotlivé zařízení.
- Možnost tvorby konfiguračních šablon, jak nových tak z běžících zařízení jako jsou AP nebo kontrolery.
- Podpora konfigurační změn a upgrade firmware pomocí jednorázových nebo opakujících se pracovních úloh (scheduled-job).
- Kontrola provedených konfiguračních změny, v případě nesouladu definice a runtime stavu konfiguračni rollback.
- Archivace konfiguraci.
- Audit konfigurace, porovnávní rozdílů proti přednastaveným politikám individuálně pro jednotlivá a hromadně proti skupině zařízení.

- Konfigurační management: zálohy a obnova konfigurace, srovnávání rozdílů, auditování podle přednastavených i vlastních pravidel.
- Možnost funkčního rozšíření o monitorování stability a odezvy ostatních síťových služeb pro jednotlivé klienty jako je průměrný čas odpovědi na DNS dotaz nebo průměrný čas zpracování RADIUS autentizace.
- Vytváření reportů v PDF formátů reportujících různé přehledové statistiky o využití sítě a jejím stavu. Autmatizované pravidelné zasílání reportů mailem.
- Vizualizace umístění prvků sítě ve fyzických mapách. Zobrazení bezdrátových klientů na mapě a jejich signálu a využívaných L7 aplikací.
- Možnost monitorování wireless IDS událostí z více samostatných systémů současně.
- Podpora systému pro automatizované bezzásahové zprovoznění připojeného zařízení.
- Monitoring a detekce síťových anomálií jako je např. nadměrné a neobvyklé navýšení objemu provozu a upozorňování na tyto stavy pomocí alarmů.

Pro chod VApp/VM v prostředí TCK KÚZK bude možnost vyhrazení HW prostředků s následující charakteristikou:

Technická specifikace poskytnutého prostředí – maximální hodnoty	
počet podporovaných vCPU	4
počet virtuálních NIC	6
velikost úložiště virtuálního stroje	500 GB
velikost operační paměti virtuálního stroje	16 GB

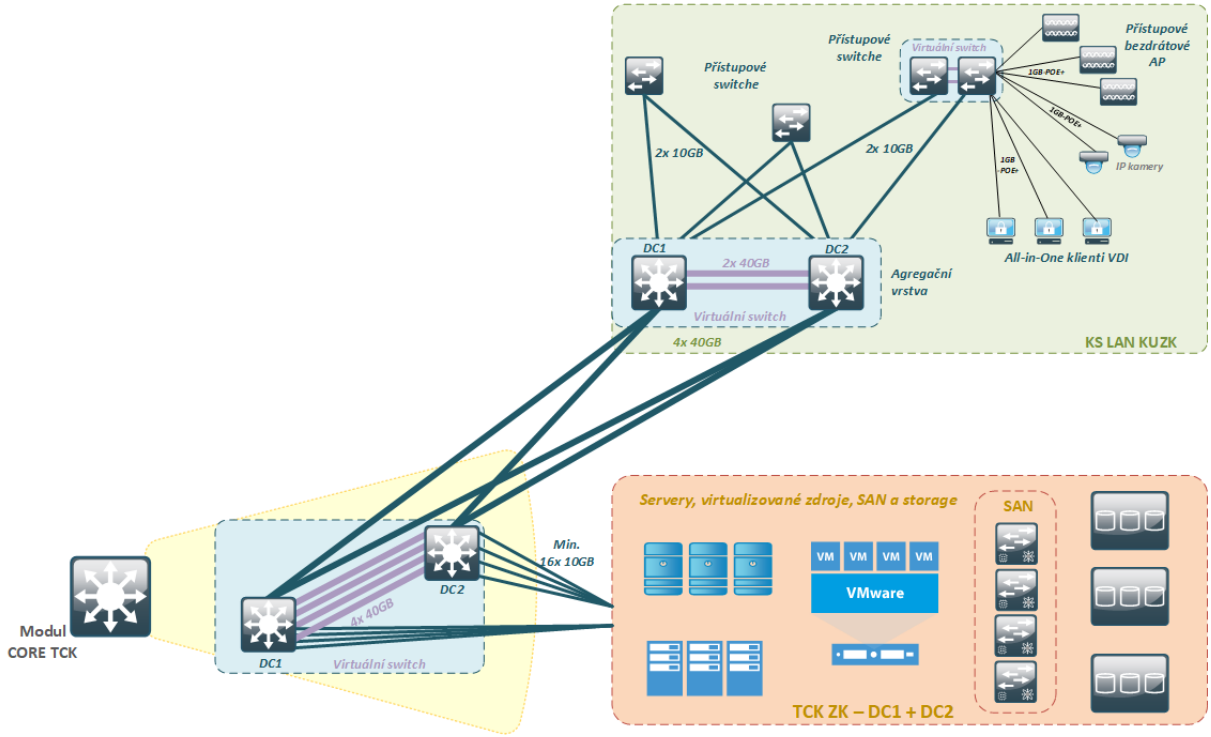
1.2.7 Cílový stav topologie a příslušenství

Součástí dodávky je vybudování nových optických rozvodů v sídle Objednatele mezi serverovnou (2. patro) a jednotlivými patrovými rozvodnami (9., 10., 11., 12., 13., 14. a 15. patro) umístěnými horizontálně nad sebou. Optické trasy budou nataženy singlemódovým optickým kabelem 9/125 µm s minimálně 12 vlákny. Ukončení jednotlivých tras bude provedeno na obou stranách v optických vanách a ukončeno SC/PC nebo SC/APC konektory.

Útlum jednotlivých optických vláken bude proměřen přímou nebo nepřímou metodou a ke každému vláknu bude vyhotoven měřící protokol.

Montáž a instalace bude probíhat dle norem ČSN50173 a ČSN50174 – je připuštěna možnost nabídnutí jiného rovnocenného řešení.

Všechny dodávané a implementované prvky musí být vybaveny komunikačními transceivery, kabely a DAC kabely tak, aby bylo možné nasazené prostředí plně propojit dle následujícího cílového schématu.



1.2.8 Požadovaná implementace a integrace

- integrace do provozovaného SIEM řešení
- vzájemná integrace s technologií Policy Enforceru (kapitola 4)
- kvalifikované seznámení obsluhy v rozsahu min. 2 MD

1.3 Modernizace aktivních prvků sítě 21Net podporující kryptaci provozu na L2 vrstvě ISO/OSI modelu

Předmětem této části je zajistit integritu KS 21Net pomocí nasazení prvků podporujících šifrování provozu na L2 vrstvě v plných rychlostech komunikačních rozhraní. Jedná se o nasazení PE MPLS přepínačů do 13 lokalit ORP, z toho ve 4 ORP bude provoz přepínačů v režimu HA – celkem se tedy jedná o 17 ks PE MPLS přepínačů. Každá lokalita je připojena ke CORE routeru, umístěném v DC1 a v DC2 TCK ZK. Dále se jedná o dodávku 16 ks firewallů, které zabezpečují provozované služby v lokalitách ORP.

Minimální požadované funkce a vlastnosti řešení:

1.3.1 CORE router

- modulární Advanced L3 přepínač
- zabezpečený management (GUI / CLI) - SSH, HTTPS přístup
- N+1 redundance napájení AC240V
- 4x 40Gb QSFP+ port
- 20x 1/10Gb SFP+ port s podporou MACsec
- 24x 1/10GBase-T
- podpora linkové agregace (LACP/statická)
- podpora virtuálního chassi – min 4 prvky
- možnost diagnostiky a troubleshooting
- provedení do RACK

- podpora VLAN
- podpora VXLAN, VTEP a OVSDB
- DCB protokol
- role-based access control (RBAC)
- podpora IPv6
- statické routování, RIP, OSPFv2/v3, BGP/BGP+, Policy routing
- podpora MPLS a VPLS řešení VPN, VRF
- ACL pro přístup k prvku
- switching kapacita 3,2 Tbps
- propustnost 2790 Mpps
- MAC tabulka min. 130 000 záznamů
- Routing tabulka IPv4/IPv6 – 128000/64000 záznamů
- DHCP snooping, ARP protection
- integrace s centrální správou aktivních prvků (kapitola 1.2.6)

1.3.2 PE MPLS přepínač 21NET

- Advanced L3 přepínač
- zabezpečený management (GUI / CLI) - SSH, HTTPS přístup
- N+1 redundance napájení AC240V
- 2x 1/10Gb SFP+ port s podporou MACsec - uplink
- 4x 1/10Gb SFP+ port
- 16x 1GB SFP porty
- 8x 1GB Dual SFP/ RJ45 porty
- podpora linkové agregace (LACP/statická)
- možnost diagnostiky a troubleshooting
- podpora VLAN
- statické routování, RIP, OSPFv2/v3, BGP/BGP+
- podpora MPLS a VPLS řešení VPN
- podpora IPv6
- ACL pro přístup k prvku
- switching kapacita 280 Gbps
- propustnost 210 Mpps
- MAC tabulka min. 32 000 záznamů
- Routing tabulka IPv4/IPv6 – 32000/16000 záznamů
- možnost virtuálního chassi switchů přes min. 2x 10 Gbps
- DHCP snooping, ARP protection

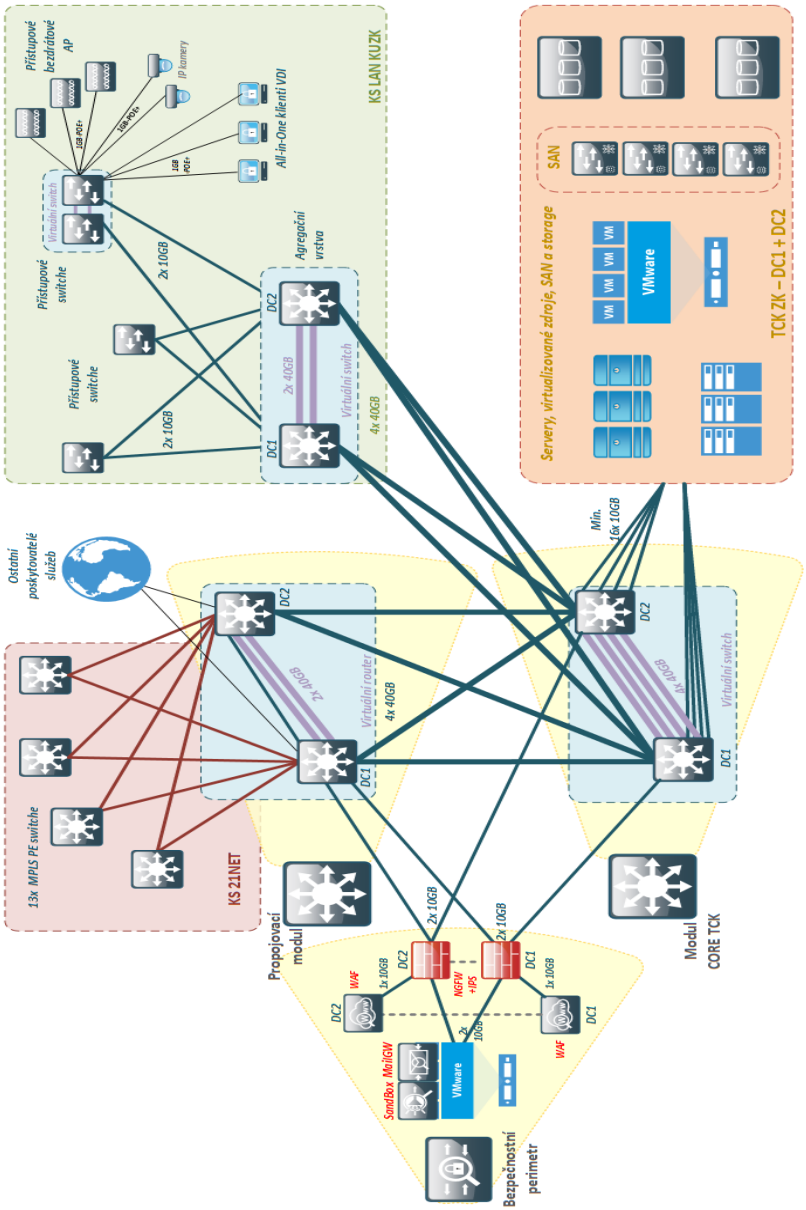
1.3.3 Firewally uzlových bodů 21NET

- HW platforma
- řízení bezpečného přístupu mezi vnější a vnitřní sítí
- segmentaci zejména použitím demilitarizovaných zón
- zajištění bezpečného vzdáleného přístupu pro uživatele (SSL VNP)
- zajištění blokování přenášených dat, které neodpovídají požadavkům
- IPSec VPN – propojení lokalit formou LAN-to-LAN

- podpora NGFW/UTM (AV, IPS, application control, WebFiltering)
- možnost centrálního sběru logů s následnou analýzou
- podpora Syslog pro zasílání logů
- zabezpečený management (GUI / CLI) - SSH, HTTPS přístup
- podpora IPv6
- podpora záložního připojení do internetu
- min 6x 1GB port Base-T
- min. propustnost FW pro 512 byte UDP paket – 3Gbps
- min. počet současných připojení – 1,3 Milionů
- min. počet nových session/sec – 30.000
- min. propustnost IPSEC VPN – 2 Gbps
- min. propustnost při současně zapnutých funkcích FW, IPS, APP Control a Malware protection = threat protection = 200 Mbps

1.3.4 Cílový stav topologie a příslušenství

Všechny dodávané a implementované prvky musí být vybaveny komunikačními transceivery, kabely a DAC kabely tak, aby bylo možné nasazené prostředí plně propojit dle následujícího cílového schématu.



1.3.5 Požadovaná implementace a integrace

- Integrace do provozovaného SIEM řešení.
- Vzájemná integrace s technologií Policy Enforceru (kapitola 4).
- Kvalifikované seznámení obsluhy v rozsahu min. 1 MD.

2. Nasazení mailové brány (MailGW) pro zajištění podpory ochrany příchozí i odchozí mailové komunikace KU proti pokročilým hrozbám

Mail Gateway (MailGW) bude plnit potřebu kontroly a třídění příchozí a odchozí elektronické pošty proti SPAMU a virům. MailGW bude implementována jako vApp/VM do prostředí TC KÚZK. MailGW bude detekovat rozšířenými metodami spam nejen pro příchozí, ale i odchozí poštu. Každá z těchto

antispamových metod může mít nastavenou svou separátní akci, jak naložit s detekovaným spamem, v podstatě co má následně nastat po tomto vyhodnocení. Další požadovanou kontrolou na bráně je antivirová kontrola. Klíčovým přínosem řešení MailGW je schopnost integrace s izolovanou lokální technologií SandBoxingu popsanou v kapitole 1.1.2. Integrované antimalware řešení bude umožňovat kontrolu přílohy nejen na viry samotné, ale i na malware všeobecně (adware, grayware, spyware, fishing atd.) a má plnou integraci se Sandboxem.

Dodáná licence umožní provoz dvou MailGW vApp/VM instancí za účelem rozložení SMTP zátěže a failoveru. Funkcionalita SMTP load balancingu není součástí této dodávky a bude řešena externím prvkem kupujícího.

Minimální požadované funkce a vlastnosti řešení

2.1 MailGW – základní funkce a vlastnosti

- Implementace jako vApp/VM do prostředí TC KÚZK nebo součástí HW NGFW (kapitola 1.1.1).
- Dodáná licence umožní provoz dvou MailGW vApp/VM instancí za účelem rozložení SMTP zátěže a failoveru.
- Kontrola příchozí i odchozí emailové komunikace s nastavením separátních akcí pro oba směry zahrnující:
  - spam,
  - vir,
  - malware (adware, grayware, spyware, fishing atd.),
  - content filtering,
  - integrace se SandBoxem (kapitola 1.1.2).
- Aktivní část řešení pro uživatele a administrátory je přístupná přes grafické komunikační rozhraní v podobě HTTPS aplikace.
- Možnost více e-mailových domén.
- Podpora adresních prostorů IPv4 a IPv6.
- Podpora ověřování SMTP adres přes:
  - LDAPS nebo MS AD;
  - RADIUS;
  - volitelně POP3 a IMAP.
- Směrování a kontrola e-mailu pomocí LDAP.
- Řízení fronty zpráv.
- Plně kompatibilní podle RFC pro e-mail a MS Exchange server.
- Možnost vytvoření administrátorských účtů s definováním administrátorských rolí.
- Vestavěná funkce pro komplexní reporting (message queue size, system resouces, health monitoring, incidenty, atd.).
- Centralizovaná karanténa pro rozsáhlé implementace, zahrnující minimálně:
  - Možnost natavení časové retence zpráv v karanténě nebo po dosažení velikosti obsahu karanténní složky s automatickým promazáváním starých zpráv.
  - Automatická emailová notifikace uživatelům při zachycení emailové zprávy do karantény.

    - Možnost přístupu do karantény jednotlivým uživatelům po přihlášení přes SSO nebo unikátní HTTPS odkaz.
    - Možnost jednoduchých operací nad zachycenými zprávami v uživatelské karanténě (náhled, smazání, uvolnění).
- Možnost nahrání vlastního SSL certifikátu za účelem bezpečného HTTPS přístupu do Administrátorské nebo uživatelské konzole.
- Podpora SNMP s využitím standardních a privátních MIB se zasíláním trapů při dosažení hraničních úrovní.
- Podpora lokálního nebo externího ukládacího serveru včetně zařízení iSCSI.
- Podpora pro externí Syslog.
- Možnost komplexního vyhledávání v historii emailové komunikace minimálně na základě následujících parametrů: Odesílatel, Příjemce, Předmět, Čas.

2.2 Ochrana proti spamu

- Ochrana proti spamovým epidemiím v reálném čase.
- Identifikátory URI zdrojových e-mailových adres spamu a phishingu.
- Možnost využití nástroje pro filtrování URL.
- Dočasné blokování (greylisting) IPv4 a IPv6 adres a e-mailových účtů.
- Reputace lokálních odesílatelů (podle IPv4, IPv6 a ID koncového bodu).
- Hloubková inspekce hlaviček e-mailových zpráv, kde na základě specifické hodnoty hlavičky provedení akce, a to minimálně:
    - zadržení emailu v karanténě;
    - smazání emailů.
- Integrace s externími seznamy identifikátorů spamu (URI) a realtimovými seznamy nežádoucích entit (SURBL/RBL).
- Detekce newsletterů/marketing emailů.
- Administrátorem definovatelné seznamy nežádoucích a povolených entit:
    - globální – IPv4 a IPv6 adresy;
    - doménové – všechny adresy z dané domény;
    - uživatel / adresa – konkrétní adresa z dané domény.
- Podpora podnikových standardů pro identitu odesílatele:
    - validační systém Sender Policy Framework (SPF);
    - elektronický podpis hlaviček Domain Keys Identified Mail (DKIM);
    - validace pomocí Domain-Based Message Authentication (DMARC).
- Práce se spam e-maily v rámci centralizované karantény.
- Flexibilní profily akcí a upozornění.

2.3 Minimální výkonnostní a systémové požadavky řešení

Výkon (zpráv/h) bez řazení do fronty, zprávy o velikosti 100 KB	
Směrování e-mailu	3000

Antispam	2400
Antispam + Antivirus	2000
Systémové specifikace	
Konfigurované domény	5
Pravidla podle příjemců (na doménu / na systém) – příchozí nebo odchozí	60 / 300
Antispam, antivirus, ověřování a profily obsahu (na doménu / na systém	50 / 60

Pro chod VApp/VM v prostředí TCK KÚZK bude možnost vyhrazení HW prostředků s následující charakteristikou:

Technická specifikace poskytnutého prostředí – maximální hodnoty	
počet podporovaných vCPU	2
počet virtuálních NIC	2
velikost úložiště virtuálního stroje	500 GB
velikost operační paměti virtuálního stroje	6 GB

2.4 Požadovaná implementace a integrace

- Integrace s technologií SandBoxu (kapitola 1.1.2).
- Integrace do provozovaného SIEM řešení.
- Kvalifikované seznámení obsluhy v rozsahu min. 0,5 MD.

3. Modernizace SW ochrany "operačních systémů klientských a serverových zařízení" pro zajištění podpory ochrany proti pokročilým hrozbám

Předmětem této části je pořízení a implementace komplexního server a end-point security řešení.

Minimální požadované funkce a vlastnosti řešení

3.1 SW ochrana – základní funkce a vlastnosti

- Požadované množstevní pokrytí:
  - OS MS Windows Serverů (2008,2012,2016) – 120 ks;
  - OS NonWindows Serverů (linux, unix atd.) – 30 ks;
  - OS PC a notebooků (MS Win7, 10) – 493 ks;

- OS Mobilních platforem (Android, iOS…) – 250 ks.

- Centrální konzole pro správu AV řešení na stanicích a serverech.
- Centrální konzole pro správu AV řešení na mobilních zařízeních (android, iOS…).
- Zabezpečení koncových stanic a serverů:
  - Pokročilá ochrana stanic a serverů:
    - Intrusion Prevention na úrovni stanice;
    - ochrana před síťovými hrozbami – ochrana prohlížeče, ochrana před přístupem na škodlivé destinace, botnet ochrana a ochrana před vzdáleným napadnutím;
    - rootkit ochrana;
    - detekce a blokace podezřelého chování (heuristika) i neznámých verzí škodlivého kódu (zero hour/zero day) a ransomware.
  - Zakázání spuštění aplikací minimálně pomocí následujících parametrů:
    - file path;
    - názvu aplikace nebo aplikačního souboru.
  - Kontrola a blokace přístupu k periferiím:
    - zamezení používání USB flash disků mimo Objednatelem centrálně povolené výjimky;
    - zamezení používání CD-DVD mimo Objednatelem centrálně povolené výjimky;
    - zamezení používání neschválené třídy zařízení nebo konkrétního zařízení, např. rozeznávání Class i Device ID.
  - Kontrola a blokace přístupu na web - možnost vytvoření centrálních blacklistů webových stránek a serverů.
  - Karanténa:
    - možnost obnovy souboru do originální lokality;
    - automatické mazání souborů v karanténě starších než zadaná doba stáří.
  - Plánované skenování, možnost definování spouštění naplánovaného testu v časovém intervalu.
  - Modul Firewallu pro koncové stanice:
    - Možnost vytváření Firewallových pravidel na základě připojeného média (WiFi, kabel) nebo přiřazené adresy (subnet).
    - Možnost vypnutí Windows firewallu.
  - Funkcionalita „tiché“ vzdálené instalace na koncové stanice včetně bezobslužné konfigurace.
- Zabezpečení mobilních zařízení:
  - Podporované platformy:
    - Android Lollipop 5.1 a vyšší;
    - iOS 10 a vyšší.
  - Anti-Theft funkce:
    - Remote-Lock;
    - Remote-Wipe;
    - lokace;

        - ochrana programu heslem před změnou nastavení Anti-Theft a odinstalováním.
    - Detekce nejnovějších hrozeb v reálném čase.
    - Aplikace nesmí výrazně ovlivnit životnost baterie, nezpomalí systém a negeneruje moc velký síťový provoz.
- Automatická a efektivní aktualizace definic na koncových zařízeních.
- Implementace centrální části jako vApp/VM do prostředí TC KÚZK.

Pro chod VApp/VM v prostředí TCK KÚZK bude možnost vyhrazení HW prostředků s následující charakteristikou:

Technická specifikace poskytnutého prostředí – maximální hodnoty	
počet podporovaných vCPU	2
počet virtuálních NIC	2
velikost úložiště virtuálního stroje	300 GB
velikost operační paměti virtuálního stroje	8 GB
velikost databáze na sdíleném MS SQL 2014/2016 řešení KÚZK	10 GB

3.2 Požadovaná implementace a integrace

- Integrace do MS AD KÚZK.
- Integrace do provozovaného SIEMU KÚZK.
- Integrace do řešení Adaptivního řízení přístupu (kapitola 4).
- Instalace a konfigurace řídící konzole, serverů a centrálních komponent navrhovaného řešení dle Prováděcího projektu včetně návrhu řešení.
- Zpracování podrobného plánu nasazení nového AV do celého prostředí KÚZK (viz množstevní pokrytí) včetně komplexního nastavení funkčnosti v KÚZK.
- V rámci možností přichystání automatizované odinstalace stávajícího antivirového řešení z klientských stanic a serverů.
- Automatizovaná instalace navrhovaného řešení na 2 zařízení každého jmenovaného OS:
    - MS Windows 7 Enterprise CZ a Windows 10 Enterprise CZ;
    - MS Windows Server 2012 R2 a Windows Server 2016;
    - Android, iOS;
- Implementace metodik a pracovních postupů.
- Kvalifikované seznámení obsluhy v rozsahu min. 0,5 MD.
- V případě dodání stejného produktu používaného Objednatelem (bližší popis může být poskytnut na vyžádání):
    - nebude požadována reinstalace,
    - nebude požadována integrace do MS AD a SIEM KÚZK,
    - nebude požadováno zpracování plánu nasazení,
    - nebude požadována implementace metodik a pracovních postupů,
    - nebude požadováno kvalifikované seznámení obsluhy,

- bude požadována hloubková revize stávajících politik a současného nasazení,
- budou požadovány úpravy v návaznosti na Adaptivní řízení přístupu (kapitola 4).

4. Zavedení dynamického, adaptivního řízení přístupu uživatelů a zařízení ke komunikačnímu systému lokální počítačové sítě LAN KÚZK

Předmětem této části je implementace SW řešení typu Security Enforcer, které ve spolupráci s infrastrukturou KS LAN KÚZK a jeho bezpečnostního perimetru dokáže aplikovat řešení adaptivního řízení přístupu DRA (Dynamic Risk Assessment). Tzn. pomocí on-line sbíraných atributů s informacemi o kontextu infrastruktury a pomocí monitoringu chování a reputačních informací bude neustále vyhodnocováno připojení konkrétního uživatele a v případě že dojde ke změně nějakého monitorovaného fenoménu, bude dané připojení znovu prohnáno mechanismem ověření uživatele. Tímto bude zajištěna diferenciace přístupů k infrastruktuře pro různé typy uživatelů na základě jejich rolí v KÚZK. Bude možné rozlišovat aplikaci bezpečnostních nastavení například pro zaměstnance, hosty nebo externí pracovníky, a to i v kontextu přistupujícího zařízení.

Minimální požadované funkce a vlastnosti řešení

4.1 Security Enforcer – základní funkce a vlastnosti

- On premise řešení pro externí captive portál pro hosty a jejich rozšířenou autentizaci a pro BYOD.
- Implementace jako vApp/VM do prostředí TC KÚZK.
- 802.1X autentizace pro WiFi, Ethernet LAN sítě a VPN.
- Podpora minimálně pro 1500 autentizovaných zařízení (pomocí 802.1X) s možností navýšení počtu.
- Podpora klastrování pro vysokou dostupnost pro všechny funkcionality řešení.
- Podpora následujících metod autentizace: PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC autentizace.
- Podpora TACACS+ autentizace správců síťových zařízení.
- Podpora dalších možností autentizace a autorizace: LDAP, MS AD, Token, MAC auth, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On (minimálně SAML 2+ IdP a SP, OAuth, Shibboleth a Okta).
- Možnost provozovat více graficky i obsahově unikátních portálů v rámci jedné instalace.
- Redakční systém pro plnou grafickou a obsahovovou úpravu jednotlivých captive portálů:
  - Uprava barev, fontů, pozadí a loga.
  - Úprava registračních formulářů – přidávání a odebírání polí pro vstupní data formuláře včetně validace vkládaného obsahu.
  - Možnost vkládání animací a videí.
  - Vytváření specifických stránek pro různé typy zařízení a operačních systémů (např. pro efektivní navedení do specifického app store).
- Samoobslužný Captive portal pro řízení přístupu hostů:
  - Registrace a přihlášení s nutnostní zadání a ověření telefoního čísla (SMS).
  - Přístup zdarma pouze s akceptací podmínek užití.
  - Tarify lze omezit časově, z hlediska rychlosti připojení či objemu přenesených dat.
  - Vynucení odpojení zařízení ihned po naplnění jakéhokoliv z limitů.
  - Podpora autentizace lokálními účty v rámci portálu.

    - Podpora autentizace pomocí socialních sítí – Google, Google Plus, Facebook, Facebook WIFI, Twitter, LinkedIn, Microsoft.
    - Perzistence autentizace/registrace skrze MAC caching a zobrazení už jen uvítacích stránek s osobním oslovením hosta při dalších návštěvách.
    - Vytváření účtů samoobslužnou registrací.
    - Průměrný počet ověřených unikátních hostů/pracovní den = 1000.
- Sběr dodatečných informací o připojených zařízeních (“profiling”) jako jsou DHCP volby klienta, HTTP uživatelský agent či předvolba MAC adresy. Tyto informace musí být možné využít pro doplňkové ověření přístupu zařízení do sítě.
- Samoobslužný BYOD portal pro Onborading koncových zařízení:
    - Přihlášení s nutnostní zadání AD jmena hesla + následná registrace zařízení.
    - Portál umožňuje vydávat cerfifikáty, funguje jako certifikační autorita a jednoduchý způsob importu certifikátů do zařízení.
    - Automatické profilování zařízení.
    - Celkový počet unikátních onboardovaných zařízení = 1000.
- Podpora ochrany koncových zařízení formou posture assessments a health checks.
- Podpora software (NAC agenta) pro MS Windows 7 a vyšší, Mac OS X 10.7 a vyšší, RHEL 4 a vyšší, Ubuntu 12.x a vyšší.
- Kontrola stavu koncového zařízení na přítomnost aktuálního antiviru.
- NAC formou permanentního nebo dočasného SW agenta.
- NAC podporuje v návaznosti na autentizační proces kontrolu systémových procesů, aplikací, klíčů registru, použití USB zařízení, přítomnost anti-viru, firewallu.

Pro chod VApp/VM v prostředí TCK KÚZK bude možnost vyhrazení HW prostředků s následující charakteristikou:

Technická specifikace poskytnutého prostředí – maximální hodnoty	
počet podporovaných vCPU	4
počet virtuálních NIC	2
velikost úložiště virtuálního stroje	300 GB
velikost operační paměti virtuálního stroje	24 GB
velikost databáze na sdíleném MS SQL 2014/2016 řešení KÚZK	10 GB

4.2 Požadovaná implementace a integrace:

- Integrace do MS Active Directory KÚZK.
- Integrace do provozovaného SIEM KÚZK.
- Integrace do řešení KS LAN KÚZK (kapitola 1).
- Kvalifikované seznámení obsluhy v rozsahu min. 1 MD.

5. Požadované služby

5.1 Služby v rámci dodávky

V rámci dodávky budou požadovány následující služby:

- Projektové řízení dodávky řešení.
- Zpracování návrhu řešení implementace jednotlivých částí – Prováděcí projekt včetně návrhu řešení specifikovaný v Příloze č. 3 Povinná struktura Prováděcího projektu včetně návrhu řešení.
- Dodávka, implementace, instalace, zapojení a konfigurace všech částí dle Prováděcího projektu včetně návrhu řešení.
- Vytvoření a předání Objednateli zálohy konfigurace.
- Ověření funkčnosti dodaného řešení a jeho částí.
- Dodávka dokumentace dodaného vybavení a jeho částí.
- Kvalifikované seznámení uživatelů a administrátorů – seznámení s funkcionalitami, obsluhou dodávaného řešení a jeho budoucím provozem.
- Provedení zkušebního provozu.
- Podpora provozu dle Přílohy č. 4: Podmínky zajištění podpory provozu díla

5.2 Dokumentace

V rámci plnění bude dodána zhotovitelem kompletní dokumentace řešení (dokumentace může být jedním dokumentem, nicméně musí obsahovat všechny relevantní informace) obsahující minimálně:

- Podrobná systémová a bezpečnostní dokumentace (administrátorská dokumentace) v českém jazyce:
    - popis skutečného provedení řešení min. ve struktuře dle Prováděcího projektu včetně návrhu řešení;
    - princip aktualizace;
    - seznam licencí.
- Kompletní provozní dokumentace ke všem částem v českém nebo anglickém jazyce.

6. Seznam zkratek a pojmů

Zkratka	Význam, výklad
ACL	Access Control List
AD	Active Directory – autentikační a adresářový systém pro platformu Windows
AD/LDAP	Active Directory/Lightweight Directory Access Protocol
AP	Access Point – přístupový bod
ARP	Address Resolution Protocol
BYOD	Bring Your Own Device – zaměstnanec může k práci používat vlastní zařízení
CDP	Cisco Discovery Protocol

CLI	Command Line Interface – rozhraní formou příkazové řádky
CPU	Central Processing Unit – procesor počítače
CRR	Centrum pro regionální rozvoj
CSV	Comma Separated Value – formát dat (souboru)
ČR	Česká republika
DAC	Discretionary Access Control
DC	Data Center
DHCP	Dynamic Host Configuration Protocol – síťový protokol
DKIM	Domain Keys Identified Mail – metoda autentikace e-mailů
DMARC	Domain-Based Message Authentication, Reporting and Conformance – validační systém pro e-mail
DNS	Domain Name Server
DRA	Dynamic Risk Assessment
EAP-TLS	Metoda autentizace
EAP-TTLS	Metoda autentizace
FTP	File Transfer Protocol – síťový internetový protokol
FW	Firewall – síťový bezpečnostní prvek
GUI	Grahical User Infterface – grafické uživatelské rozhraní
HA	High Availability
HTML	Hypertext Markup Language – jazyk pro tvorbu webových stránek
HTTP	Hypertext Transfer Protocol – internetový komunikační protokol
HTTPS	Hypertext Transfer Protocol Secure – bezpečný internetový komunikační protokol
HW	Hardware
HZS	Hasičský záchranný systém
ID	Identifier – identifikátor
IDS	Intrusion Detection System
IDS/IPS	Intrusion Detection Systém / Intrusion Prevention System
IKT	Informační a komunikační technologie
IM	Instant Messaging – systém komunikace pomocí zpráv na internetu
IMAP	Internet Message Access Protocol – síťový protokol pro e-mail

IMC	Intelligent Management Center
IP	Internet Protocol – internetový komunikační protokol
IPS	Intrusion Prevention System
IPsec	Síťový autentikační a šifrovací protokol
IS	Informační systém
ISO	International Organization for Standards – mezinárodní standardizační organizace
ISO/OSI model	ISO Open Systems Interconnection model – model propojování počítačových systémů
IT	Informační technologie
KS	Komunikační systém
KÚZK	Krajský úřad Zlínského kraje
LACP	Link Aggregation Control Protocol – síťový internetový protokol
LAN	Local Area Network – lokální počítačová síť
LDAP	Lightweight Directory Access Protocol
MAC adresa	Media access control address – unikátní adresa elektronického zařízení v síti
MAPI	Messaging Application Programming Interface
MDM	Mobile Device Management – správa mobilních zařízení
MS	Microsoft
NAC	Network Access Control
NGFW	Next-Generation Firewall
ORP	Obec s rozšířenou působností
OS	Operační systém(y)
PC	Personal Computer – třída osobních počítačů
PDF	Portable Document Format – souborový formát pro textové dokumenty
POE	Power over Ethernet
POP3	Post Office Protocol 3 – síťový protokol pro elektronickou poštu
RBAC	Role-Based Access Control
RF	Radiofrekvenční
RJ-45	Standard konektoru síťové kabeláže
RTF	Rich Text Format – standard pro textový soubor

SC/PC nebo SC/APC	Konektory optických kabelů
SMTP	Simple Mail Transfer Protocol – síťový protokol pro elektronickou poštu
SNMP	Simple Network Management Protocol – síťový protokol pro správu sítě
SQL	Structured Query Language – jazyk pro práci s databázemi
SSH	Secure Shell – kryptografický síťový protokol
SSID	Service Set IDentifier – identifikátor Wi-Fi sítě vysílaný AP (viz)
SSL	Secure Sockets Layer - kryptografický síťový protokol
SW	Software – programové vybavení počítačů
SW/HW	Software/hardware
TACACS+	Terminal Access Controller Access-Control System Plus – autentikační, autorizační a účtovací síťový protokol
TC	Technologické centrum
TCK	Technologické centrum kraje
TCP/IP	Transmission Control Protocol/Internet Protocol – síťový komunikační protokol
UDP	User Datagram Protocol – síťový internetový protokol
URI	Uniform Resource Identifier – řetězec znaků identifikující zdroj
URL	Uniform Resource Locator – webová adresa zdroje (stránek)
USB	Universal Serial Bus – počítačová sběrnice pro připojení periferií k počítači
VLAN	Virtuální LAN (viz) - logicky nezávislá síť v rámci jednoho nebo několika zařízení
WAN	Wide Area Network – územně rozsáhlá počítačová síť
WHQL	Windows Hardware Quality Labs – testování kompatibility s Windows a její certifikace
WiFi	Bezdratová síť
XLS	Excel Binary File Format – původní formát aplikace Microsoft Excel
XML	eXtensible Markup Language - obecný značkovací jazyk
ZK	Zlínský kraj