NAKIT
Národní agentura pro komunikační a informační technologie, s. p.

Doporučená nastavení koncového zařízení OVS pro připojení ke službám v prostředí CMS

Autoři	Michal Brož, Martin Kulich
Datum vytvoření	19.11.2019
Datum aktualizace	15.06.2021
Verze	1.12
Počet stran	13
Název dokumentu	Doporučená nastavení koncového zařízení OVS pro připojení ke službám v prostředí CMS

NAKIT
Národní agentura pro komunikační a informační technologie, s. p.

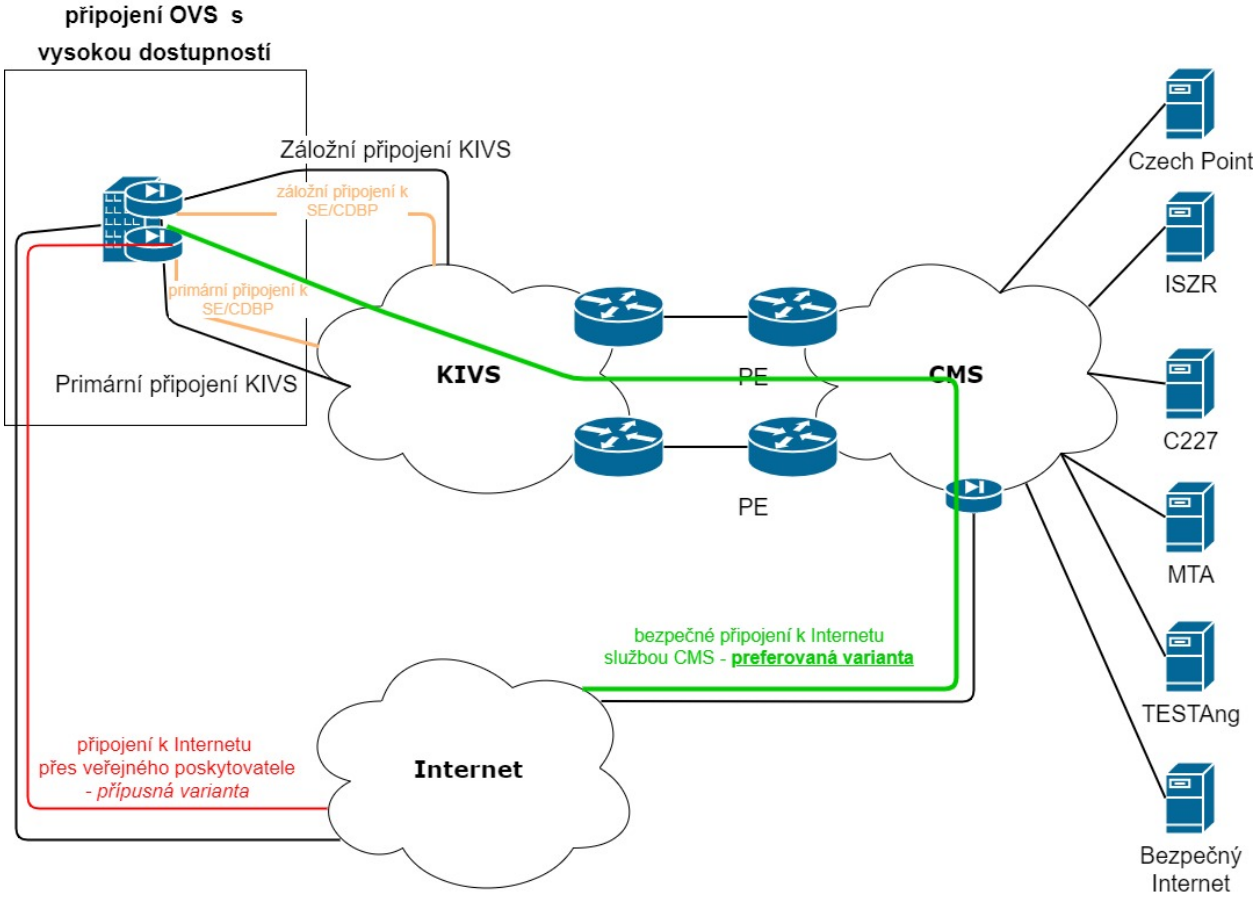
Obsah

1. Úvod

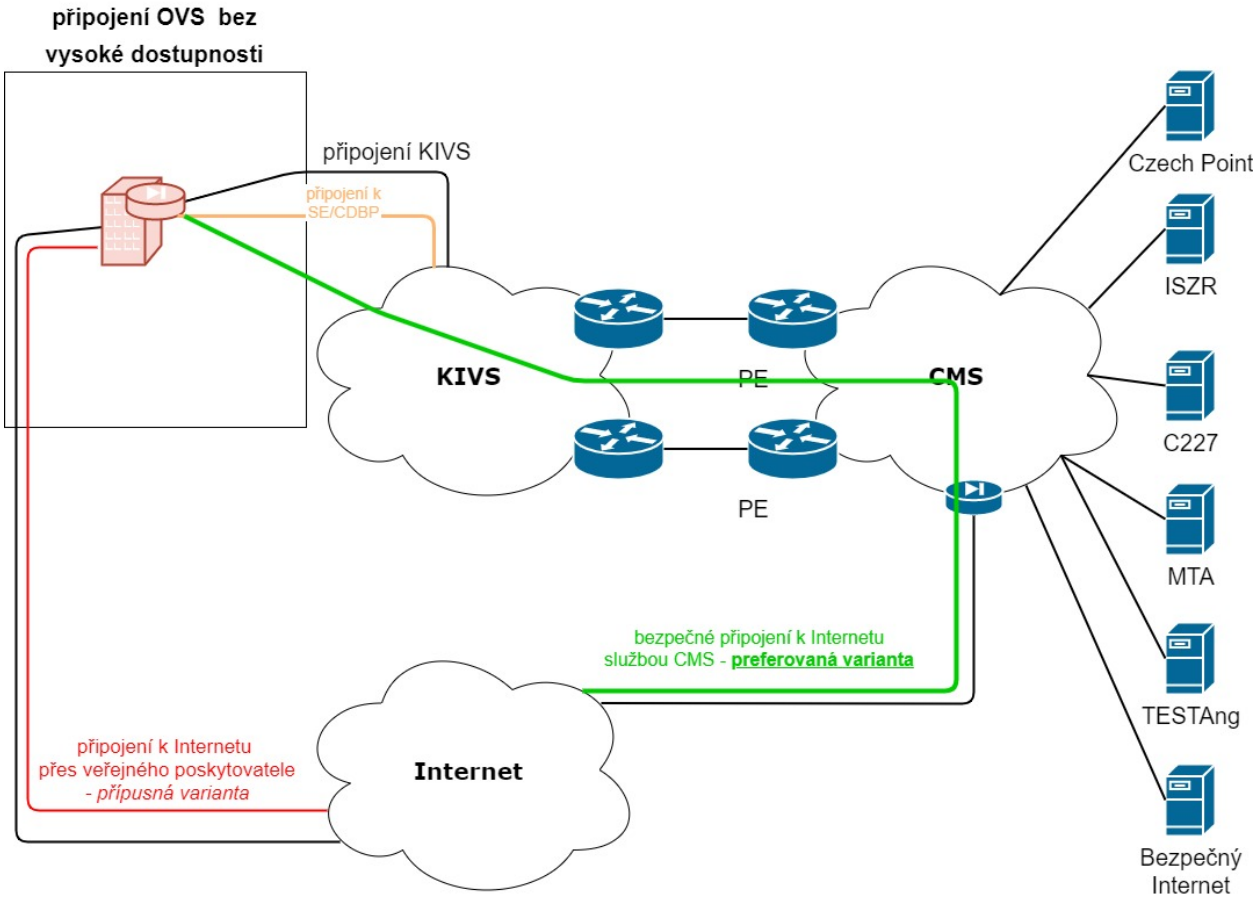
Účelem tohoto dokumentu je popsat bezpečnostní doporučení Ministerstva vnitra pro koncová zařízení pro připojení OVS ke službám v prostředí Centrálního místa služeb (CMS) přes Komunikační Infrastrukturu Veřejné Správy, dále jen KIVS a krajské konektory (KK).

Centrálním místem služeb (CMS) se rozumí soubor technického a programového vybavení, jehož prostřednictvím jsou poskytovány služby informačních systémů veřejné správy a jehož prostřednictvím jsou využívány a propojovány sítě elektronických komunikací. Kromě jiného zajišťuje vzájemné, řízené a bezpečné propojování orgánů veřejné správy pro výměnu dat a služeb, dále též komunikaci subjektů veřejné a státní správy s jinými subjekty ve vnějších sítích, jakými jsou Internet nebo komunikační infrastruktura EU. CMS tak vytváří základní stavební prvek celé komunikační infrastruktury veřejné správy a zabezpečuje služby pro výměnu dat a služeb mezi jednotlivými informačními systémy veřejné správy.

Ke službám v prostředí Centrálního místa služeb (CMS) se lze přes KIVS připojit i s vysokou dostupností (redundantním připojením). Podrobnější popis připojení s vysokou dostupností popisuje obrázek č.1 a kapitola 2.1.7.



Obrázek 1: Příklad připojení OVS k CMS přes KIVS s vysokou dostupností a v kombinaci s přípojkou k veřejné síti Internet



Obrázek 2: Příklad připojení OVS k CMS přes KIVS bez vysoké dostupností a v kombinaci s přípojkou k veřejné síti Internet

2. Doporučená nastavení koncového zařízení a infrastruktury OVS pro přístup ke službám v prostředí CMS

Subjekt, OVS, pro přístup ke službám v prostředí CMS musí splňovat podmínky uvedené v zákoně o kybernetické bezpečnosti – zákon číslo 181/2014 Sb. Pro informační systémy (IS) provozované OVS doporučujeme řídit se dokumentem Minimální bezpečnostní standard informačních systémů MV (zejména kapitola 3, 4.2, 4.3, 4.5.6, a 4.5.7), aby bylo minimalizováno riziko přístupu neoprávněné osoby do sítě OVS.

2.1. Seznam doporučovaných bezpečnostních vlastností koncového zařízení OVS pro připojení ke službám v prostředí CMS.

Níže jsou vyjmenována jednotlivá doporučená bezpečnostní nastavení, která by bylo vhodné zapracovat do infrastruktury OVS, protože Subjekt OVS je podle přístupové smlouvy k CMS (služba CMS2-01-1) zodpovědný za případné zneužití svého připojení útočníkem. V jednotlivých kapitolách je vysvětlen důvod konkrétního opatření a doporučené nastavení.

2.1.1 Fyzická bezpečnost

Je důležité zamezit fyzickému přístupu ke koncovému zařízení neoprávněnou osobou (minimalizace rizika neoprávněného přístupu do zařízení, např. obejitím autentizačního a autorizačního mechanismu, restartem koncového zařízení do nouzového režimu a tím pádem způsobení znepřístupnění služeb v CMS).

2.1.2 IDS a IPS

IDS – Nástroj pro detekci škodlivých a nebezpečných kódů s pravidelnou aktualizací databáze vzorků nejméně 1x týdně.

IPS – Nástroj pro prevenci před škodlivým kódem s pravidelnou aktualizací databáze vzorků nejméně 1x týdně.

IDS a IPS je doporučováno jako bezpečnostní nástroj pro zvýšení bezpečnosti

2.1.3 AntiDDoS

Ochrana hraničního zařízení proti DDoS útokům, které mohou znemožnit dostupnost služeb v CMS pro dané OVS (doporučené doplnění k IDS resp. IPS).

2.1.4 Antimalware

Nasadit SW pro ochranu koncových stanic příjemců elektronické pošty před napadením škodlivým kódem.

2.1.5 Firewall

Nástroj pro limitaci povolených a nepovolených síťových spojení na základě IP adresy, portu a protokolů, k aplikacím v CMS ze sítě OVS na základě zdrojové i cílové IP adresy a cílového portu. Základní prvek řízení komunikačních toků na hranicích infrastruktur.

2.1.6 Filtrování URL adres

Ochrana koncových stanic před napadením škodlivým kódem z www stránek, který tento kód mohou obsahovat. Limitace uživatelů z pohledu konzumovaných stránek ve veřejném internetu a jejich kategorií (Zakázání pornografie, nesnášenlivost apod.) Monitoring objemu konzumovaných dat uživatelů jednotlivých služeb veřejného internetu. Jedná se o další stupeň zabezpečení. Nastavení je nutné provádět vždy centrálně na přístupovém firewallu OVS.

2.1.7 Vysoká dostupnost (redundantní připojení do CMS)

Umožní přístup k aplikacím v CMS přes záložní hraniční zařízení a záložního okruhu v případě poruchy primárního hraničního zařízení anebo primárního okruhu. Soubor technických konfiguračních a organizačních opatření, které chrání proti výpadku jednotlivých komponent celého řešení a umožnují nepřerušený provoz, nebo provoz s minimálním výpadkem. Primární a záložní připojení k CMS zajistí vysokou dostupnost aplikací v prostředí CMS pro OVS.

2.1.8 Virtuální směrovací tabulka

Virtuální oddělení směrovacích tabulek je nezbytné pro oddělení provozu z důvodů bezpečnosti od ostatního provozu do a z CMS, např. CDBP, Internetového provozu a popř. vlastního provozu sítě OVS.

2.1.9 Log management a SIEM

Nástroj na zaznamenávání (logování) a vyhodnocování činnosti systémů administrátorů a uživatelů prvků infrastruktury atd. Tento nástroj je nezbytný pro zaznamenávání a identifikaci aktivit pro případné řešení problémů a incidentů ve spolupráci nadřízeným orgánem.

2.1.10 Synchronizace času

Synchronizace času s řádným zdrojem času (NTP servery) pro jednotnou časovou synchronizaci všech systémů a jimi zaznamenanými událostí a logů. Pro stanovení přesného data a času události je nutné veškeré prvky sítě mít synchronizovány jedním centrálním časovým zdrojem (natavení NTP serveru pro celou síť). Bez centrální synchronizace času napříč všemi součástmi není možné jednoznačně identifikovat skutečný (reálný) čas vzniku události/záznamu.

2.1.11 Nástroj pro ověřování uživatelské identity a řízení přístupových oprávnění

Ověřování uživatelské identity a řízení přístupových oprávnění pro přístupy a zajištění jejich jednoznačnosti centrální správy, řízení práv, oprávnění a autentičnosti. Tímto nástrojem snižujeme bezpečnostní riziko neoprávněného přístupu do síťe OVS, respektive i všech napojených systémů.

2.1.12 Management zařízení

Management všech zařízení v síti OVS musí být prováděn prostřednictvím bezpečných protokolů, kde seznam doporučovaných úrovní je pravidelně vydáván organizací NÚKIB. V rámci managmentu musí být možná jednoznačná identifikace jednotlivých administrátorů (tzv. jmenné účty). Nepojmenované účty mohou sloužit pouze jako emergency záloha. Administrace nesmí probíhat pod běžnými uživatelskými účty, které jsou administrátorům přiděleny.

2.1.13 Vypnutí nepoužívaných služeb

Vypnout nepoužívané defaultně zapnuté služby na všech zařízeních v síti OVS (např. telnet, ssh v1, dhcp, dns server/resolver aj.). Provádění pravidelné periodické kontroly na spuštěné služby a aplikace. Identifikace jejich potřebnosti pro provoz a služby. Validace úrovně nastavení šifrování a šifrovacích standardů, jejich verzí a odstraňování nepotřebných služeb a protokolů.

2.1.14 Filtrování nežádoucího a nepotřebného provozu

Na vstupním portu od koncové stanice na L2/L4 přepínači filtrovat nežádoucí provoz (např. non – IP data). Minimálně na úrovni přestupů mezi jednotlivými sítěmi musí docházet k limitaci provozu na pouze provoz žádoucí. Toto opatření snižuje zátěže (distribuce broadcastů za hranice sítě) a zvyšuje úroveň bezpečnosti omezením možnosti působení škodlivých kódů, které zneužívají otevřené komunikace pro identifikace dalších potencionálních cílů nákazy.

2.1.15 Omezení počtu mac adres

Omezení počtu mac adres na přepínači na portech pro koncové stanice a servery jako ochrana proti vyčerpání CAM tabulky přepínače a vyčerpání DHCP adresních bloků. Zapnutí funkcionality 802.1x na klientských portech pro limitaci připojení pouze schválených zařízení.

2.1.16 DHCP snooping

Ochrana proti falešnému DHCP serveru v síti.

2.1.17 Inspekce ARP paketů

Zabránění falešných ARP odpovědí na ARP dotazy.

2.1.18 Zamezení podvrhování zdrojových IP adres (IP source guard)

Zabránění falšování zdrojové IP adresy.

2.1.19 802.1Q

Vypnutí dynamic trunking protocol – nastavení módu portu staticky (přístupový port, trunk port). Přesné dedikování portu, jeho konkrétní činnost. Port určený pro přístup koncového zařízení. Zabránění nežádoucímu slučování portů.

2.1.20 Spanning – tree protokol

Zakázání nepoužívaných portů na přepínači a přiřazení do nepoužívané VLAN.

Nepoužívat VLAN číslo 1 pro infrastruktury, kde je využíván spanning tree protokol, doporučujeme případně na portech s koncovými stanicemi, servery zapnout BPDU guard a Root guard.

2.1.21 Segmentace sítě

Oddělení koncových stanic, serverů a jejich skupin do samostatných VLAN (např. dle odborů, přístupů do aplikací, nebo například dle poskytovaných služeb: IP telefonie, video konference, klientské stanice, Wifi sítě, aplikační servery, databázové servery, management sítě atd.).

2.1.22 WiFi

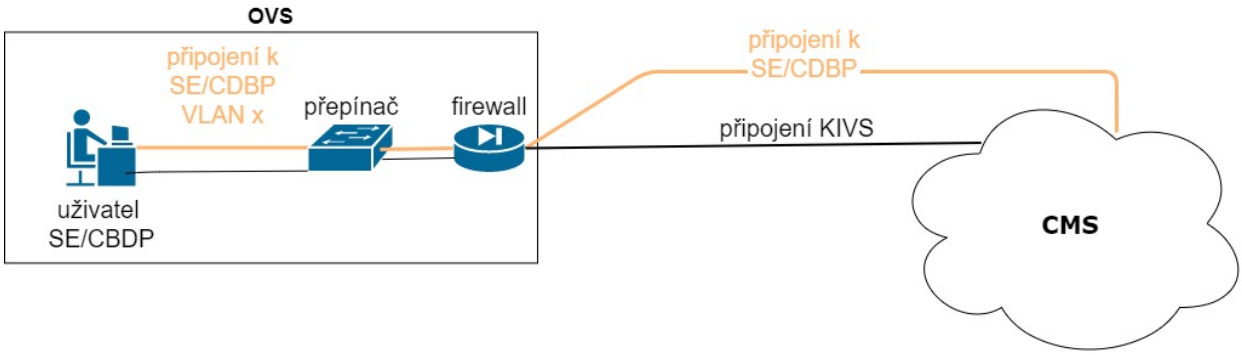
Veřejná WiFi síť by měla být oddělena od neveřejné sítě minimálně pomocí VLAN, guest VLAN, private VLAN, 802.1x apod. Privátní WiFi síť by měla obsahovat řízení přístupu a

verifikace oprávněnosti přístupu, například formou digitálního certifikátu. Využití pouze textového hesla není považováno za dostatečnou úroveň zabezpečení privátní WiFi sítě. Další variantou doplnění vhodné úrovně zabezpečení privátní WiFi sítě může být nutnost sestavení klientské VPN pro přístup k vnitřním systémům úřadu.

2.2. Přístup k aplikaci CDBP

Přístup k aplikaci CDBP je oddělen v samostatné privátní síti nazývané Síť správních evidencí (síť SE). Adresace těchto sítí je určena centrálním adresním plánem sítě SE (MV). Na hraničním zařízení aplikace CDBP je povolen pouze přístup k definovaným aplikacím CDBP z přidělených adresních rozsahů sítě SE pro OVS. V této síti je zároveň umožněn vzdálený management pracovních stanic z centra sítě SE (wake on LAN). V této nové síti budou provozovány pouze pracoviště CDBP (kabinky) a bude v ní umožněn přístup pouze k aplikaci CDBP.

Nevyužité počítače v LAN síti SE mohou být převedeny do LAN sítě OVS, ze které bude přístup k aplikacím vystaveným v CMS. Tyto počítače budou moci být využívány i pro ostatní agendy přenesené působnosti, pro které to dnes není možné. Aplikace sítě SE, vyjma CDBP, jsou dostupné jako aplikace v CMS.



Obrázek 3: Příklad připojení OVS k síti CDBP přes KIVS, kdy provoz uživatele sítě CDBP je virtuálně oddělen od ostatního provozu - uživatel má přístup pouze do sítě CDBP

2.3. Přístup ke službám v prostředí CMS

V rámci přístupu ke službám CMS jsou pro OVS dostupné aplikace k výkonu přenesené působnosti, vyjma CDBP, pro kterou je realizována zcela samostatná síť pro přístup k aplikaci CDBP, služby s otevřeným přístupem CMS a centrální služby CMS. Jejich seznam je uveden na Portálu CMS.

Každý OVS má v rámci CMS vlastní oddělenou VPN, zakončenou na virtuálním firewallu v CMS. Komunikace mezi jednotlivými OVS je řízena bezpečnostními politikami na

virtuálních firewallech v CMS, které reflektují ISMS resortu MV. V základním nastavení OVS nemohou mezi sebou napřímo komunikovat. V případě potřeby lze vzájemnou komunikaci povolit v rámci žádosti o publikační a přístupové služby CMS.

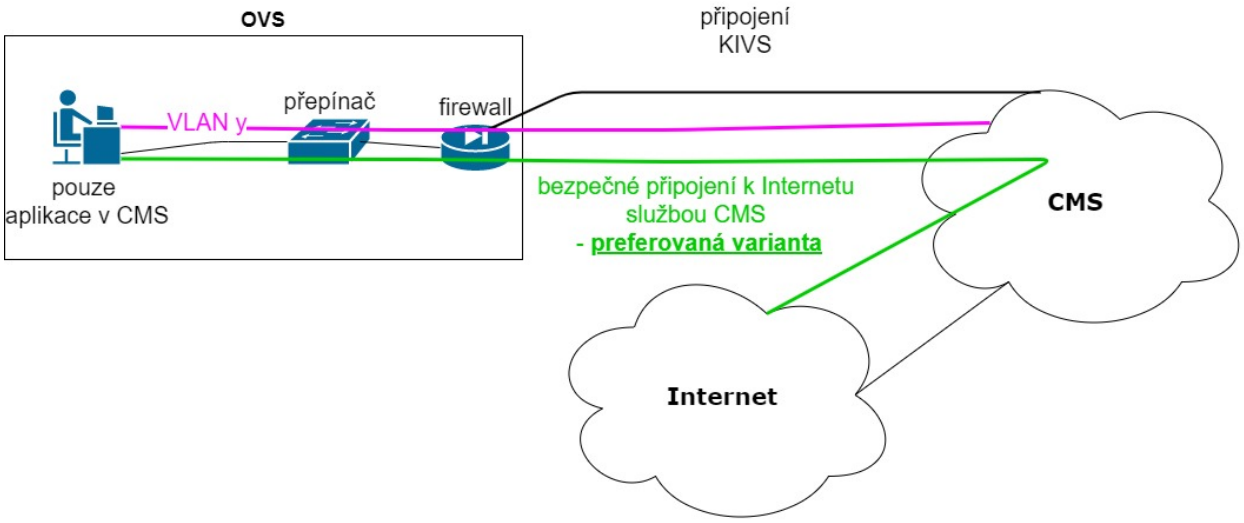
Pro přístup ke službám CMS je využito samostatné VPN pro každý OVS. Na směrovači, ve správě OVS, je potřeba nasměrovat adresní prostor 10.240.0.0/12 do k tomuto účelu zřízené VPN (KIVS, KK, ITS, …) a nastavit pravidla ve firewallu tak, aby byla povolena pouze IP komunikace z příslušných koncových stanic v síti OVS do sítě CMS na služby v CMS. Adresy, protokoly a porty služeb v CMS jsou uvedeny na Portálu CMS. Ostatní provoz je v CMS blokován.

Pro správné fungování služeb CMS je nutné odebírat DNS službu z CMS, minimálně pro domény, hostované v CMS. Jejich seznam je uveden na Portálu CMS. Popis správného nastavení DNS serveru subjektu je uveden v dokumentu „Popis nastavení DNS serveru subjektu CMS“.

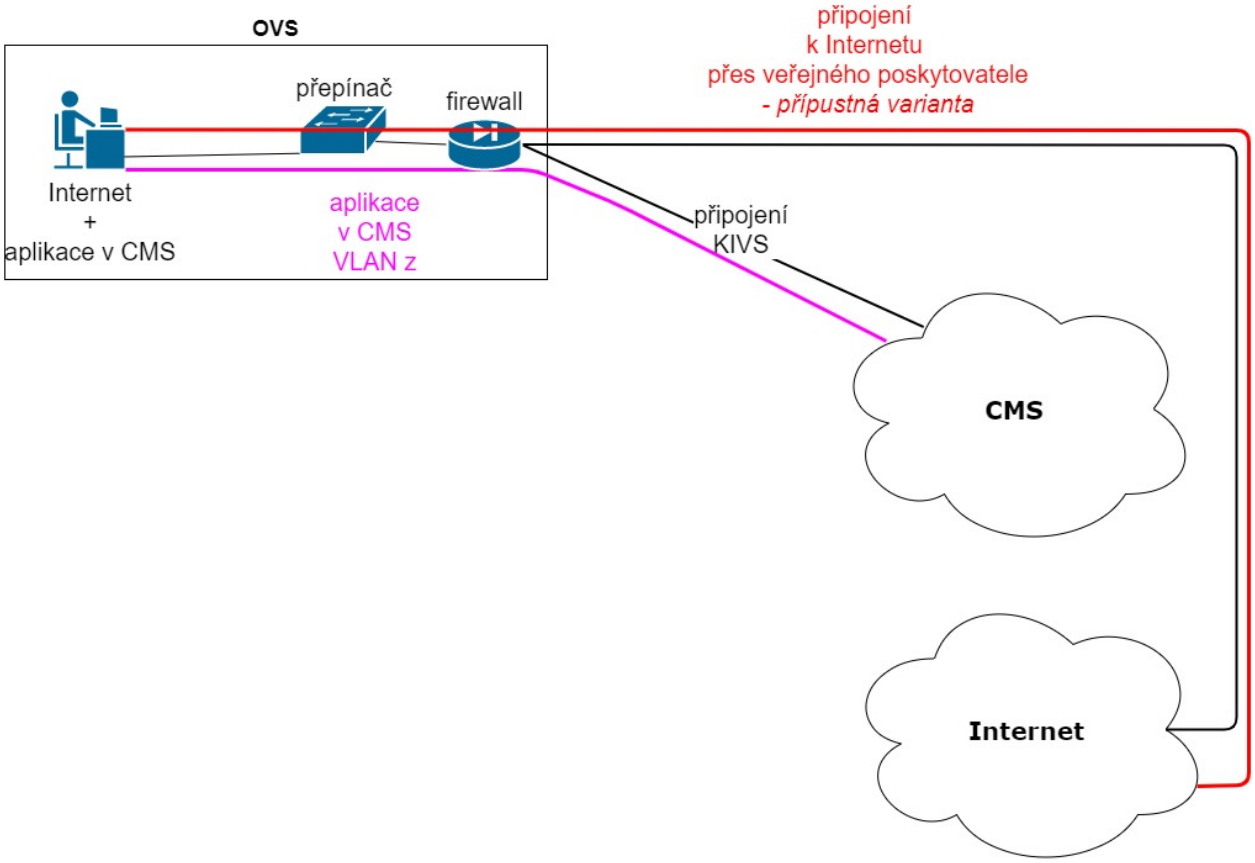
2.3.1 Připojení k Internetu

Z pohledu připojení OVS k internetu je preferována varianta, kdy OVS nemá vlastní připojení do internetu a k internetu připojuje prostřednictvím CMS, služby CMS2-9-2 - Bezpečný přístup do Internetu, viz obrázek č. 4.

Vlastní linka pro připojení k Internetu je přípustná (připojení k Internetu přes veřejného poskytovatele) viz obrázek č. 5, kde připojení k Internetu vlastní linkou musí být bezpodmínečně zakončeno na přístupovém firewallu OVS s nastavením bezpečnostních pravidel. Jiné připojení k Internetu než připojení přes přístupový firewall není z hlediska bezpečnosti přípustné.



Obrázek 4: Příklad připojení OVS ke službám CMS přes KIVS, kdy provoz uživatele je virtuálně oddělen od ostatního provozu – tento uživatel má přístup pouze ke službám publikovaným v CMS včetně bezpečného Internetu – preferovaná varianta připojení k Internetu



Obrázek 5: Příklad připojení OVS ke službám CMS přes KIVS, kdy provoz uživatele je virtuálně oddělen od ostatního provozu – tento uživatel má zároveň přístup i k Internetu – přípustná varianta připojení k Internetu

2.4. Dodatečná bezpečnostní doporučení

V rámci zvýšení zabezpečení systémů a sítě doporučujeme využít dalších služeb CMS. Například pro emailovou komunikaci lze využít službu MTA v CMS, aktualizační službu WSUS, Bezpečný přístup k internetu a podobně.

Služba MTA zajišťuje předávání zpráv elektronické pošty, jak mezi jednotlivými Subjekty KIVS, tak mezi Subjekty KIVS a uživateli sítě Internet a zároveň plní bezpečnostní funkce antiviru a antispamu.

Seznam služeb v CMS je dostupný v Přehledu služeb CMS viz kapitola 3.2.

3. Zkratky a související dokumenty

3.1. Slovník použitých zkratek

Termín	Definice
CDBP	Cestovní doklady s biometrickými prvky
CMS	Centrální místo služeb
DNS	Domain Name systém
IDS	Intrusion detection systém
IPS	Intrusion prevension systém
OVS	Orgán veřejné správy
URL	Uniform Resource Locator
VLAN	Virtual local area network
VPN	Virtual Private Network
VRF	Virtual routing and forwarding
NTP	Network time protocol (protokol pro synchronizaci času)
DHCP	Dynamic host configuration protocol (protokol pro přidělení IP adresy, brány, DNS, NTP serverů a dalších parametrů koncové stanice, serveru apod.)
KIVS	Komunikační infrastruktura veřejné správy

3.2. Související dokumenty a odkazy

Další podpůrné dokumenty: https://www.cms2.cz (dostupné z internetu)

Portál CMS – https://www.cms2.cz (dostupný jen z vnitřních sítí, připojených do CMS).

Minimální bezpečnostní standard informačních systémů vydaným NÚKIB - https://www.nukib.cz/download/publikace/podpurne_materialy/2020-07-17_Minimalni-bezpecnostni-standard_v1.0.pdf

Přehled služeb CMS – https://www.mvcr.cz/soubor/prehled-sluzeb-cms.aspx

Provozní podmínky CMS – https://www.mvcr.cz/soubor/provozni-podminky-cms-2.aspx