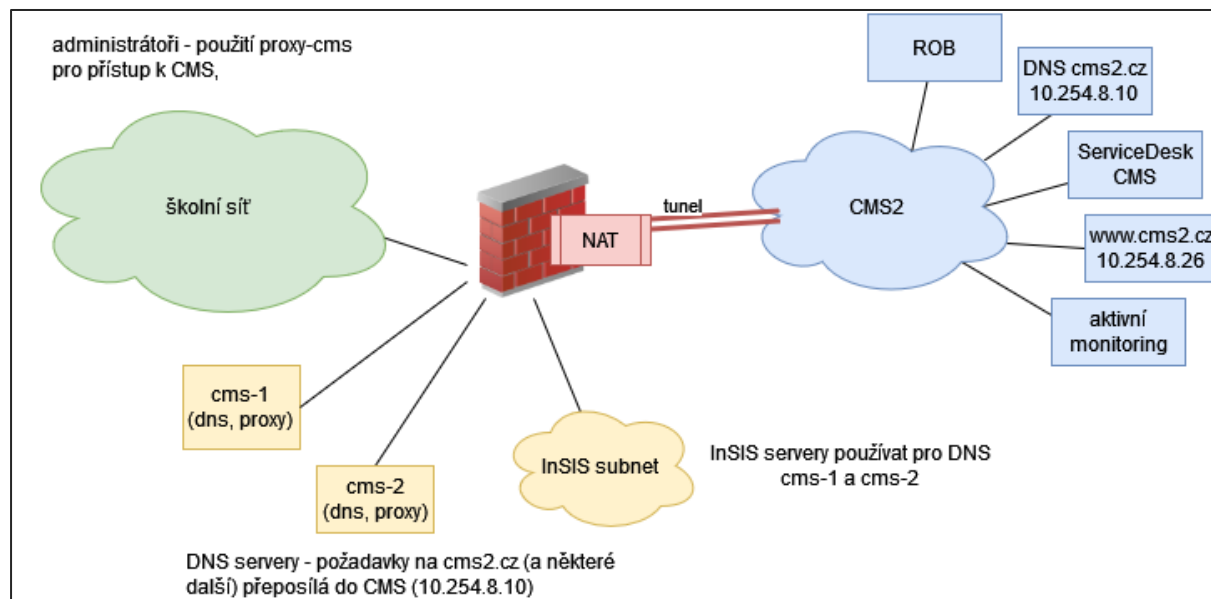




Připojení na CMS2 - VŠE

Uživatelský pohled

Síťové připojení z uživatelského pohledu je na následujícím diagramu:



Obrázek 1: Uživatelský pohled na připojení k CMS

Servery InSIS a servery cms-1.vse.cz a cms-2.vse.cz mají přístup do sítě CMS2.

Potřebné úpravy na serverech/stanicích pro přístup:

- servery InSIS – nastavit DNS resolver na 146.102.42.121 a 146.102.42.122.
- stanice administrátorů – nastavit proxy server, nejlépe pomocí skriptu z URL http://146.102.42.43/cms_proxy.pac (popis viz příloha).

Ověření připojení

- servery InSIS – ping na virtuální firewally 10.250.143.18 a 10.250.207.182; dns dotaz na 10.254.8.10 (např. dig www.cms2.cz @10.254.8.10),
- stanice administrátorů – zobrazit si www.cms2.cz, neměla by se zobrazit stránka z www.mvcr.cz, ale portál Centrální místo služeb.

Proxy servery lze použít jen z vybraných segmentů sítě (InSIS, zaměstnanci v SB, VPNka pro zaměstnance).

Síťový pohled

Připojovací síť si definuje škola sama – obvykle rozsah /24, musí být z 10.0.0.0/8, nesmí být z konce rozsahu (10.248-255.*.8). Na VŠE jsme zvolili 10.102.14.0/24.

[Sem zadejte text.]



Financováno
Evropskou unií
NextGenerationEU



Národní
plán
obnovy



Od CESNETu jsme získali VLAN 508 a přiřazené IP adresy spoje (záložní spoj zatím není, pravděpodobně bude potřeba zprovoznit BGP):

- IP 10.0.172.45/31 (na vaší straně)
- GW 10.0.172.44/31

VLAN je ukončen na firewallu (FortiGate), do VLANu se směřuje s cílovou adresou 10.240.0.0/12. Tento rozsah se propaguje ve vnitřní síti.

Na firewallu je nakonfigurován NAT, který převádí IP adresy ze 146.102.14.0-63 na 10.102.14.0-63. A dale převádí IP adresy 146.102.42.121 a 146.102.42.122 na 10.102.14.121 a 10.102.14.122.

Další překlad adres je možná u CESNETu, ale určitě i v rámci CMS2. Vůči službám v CMS2 vystupuje naše připojení pod IP adresami 10.252.39.33 a 10.252.39.35.

Nastavení a monitorování serverů cms-1 a cms-2

Servery cms-1.vse.cz a cms-2.vse.cz jsou totožné s výjimkou IP adres a jmen.

- 2x vCPU, 4GB RAM, 32GB HDD
- operační systém: Debian 11
- resolvující nameserver: unbound,
- proxy server: tinyproxy na portu 8888/tcp, v konfiguraci je omezení přístupu na vybrané sítě,
- firewall: v nftables se povoluje přístup jen ze školních sítí ke všem službám (ssh, dns, proxy)

Monitorování v Xymon:

- DNS včetně odpovědi pro www.cms2.cz,
- proxy server (cílová adresa je <http://nms.vse.cz/>)

Správa DNS serverů a konfigurace proxy

Nameserver v CMS2 pro některé domény slučuje veřejná jména z domény a jména dostupná jen v CMS2, popř. pro některá doménová jména vrací interní IP adresy z CMS2 (např. pro www.czechpoint.cz vrací IP 10.254.17.88). Seznam domén lze zobrazit po přihlášení na www.cms2.cz¹.

V blízké době pravděpodobně nebudeme potřebovat služby z jiných zón než je cms2.cz, v doporučeních ale je přebírat všechny zóny v seznamu z nameserveru v CMS2.

Pokud se přidá další zóna do seznamu CMS, je potřeba:

- a) upravit konfigurace pro nameserver na cms-1 a cms-2 (konfigurace se spravuje přes ansible)
- b) upravit konfiguraci proxy pro stanice

Konfigurace proxy je na nms.vse.cz v souboru `/var/www/4243/cms_proxy.pac`. Při změně DNS zón v CMS je potřeba upravit konfiguraci. Následuje obsah souboru k 31.5.

```
function FindProxyForURL(url, host) {
```

¹ V seznamu na www.cms2.cz chybí zóna cms2.cz. Doufám, že je to jediná zóna, která tam chybí.

[Sem zadejte text.]



**Financováno
Evropskou unií**
NextGenerationEU



**Národní
plán
obnovy**

MŠMT
MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY

```
var cmsdomains = new Array(  
    ".cms2.cz",  
    ".cuzk.cz",  
    ".czechpoint.cz",  
    ".e-legislative.cz",  
    ".e-sbirka.cz",  
    ".edalnice.cz",  
    ".ekis.mv.cz",  
    ".erop.cz",  
    ".eselpoint.cz",  
    ".isoss.cz",  
    ".mdcr.cz",  
    ".mojedatovaschranka.cz",  
    ".moneyweb.cz",  
    ".mze.cz",  
    ".mzem.net",  
    ".narodni-ca.cz",  
    ".postsignum.cz",  
    ".statnipokladna.cz"  
);  
for (i = 0; i < cmsdomains.length; i++) {  
    if (dnsDomainIs(host, cmsdomains[i])) {  
        return "PROXY cms-1.vse.cz:8888; PROXY cms-2.vse.cz:8888";  
    }  
}  
return "DIRECT";  
}
```

Příloha 1 – nastavení proxy na stanici

Ve Windows

[Sem zadejte text.]



**Financováno
Evropskou unií**
NextGenerationEU



**Národní
plán
obnovy**

MŠMT
MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY

Proxy server

Pro připojení k Ethernetu nebo Wi-Fi používat proxy server. Toto nastavení neplatí pro připojení VPN.

Automaticky zjišťovat nastavení

☐ Vypnuto

Používat skript pro nastavení

☒ Zapnuto

Adresa skriptu

Uložit

[Sem zadejte text.]



Financováno
Evropskou unií
NextGenerationEU



Národní
plán
obnovy

MŠMT
MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY

Ve Firefoxu

Nastavení připojení

Nastavení proxy serverů pro přístup k internetu

☐ Bez proxy serveru

☐ Automatické zjištění konfigurace proxy serverů

☐ Použít nastavení proxy serverů v systému

☐ Ruční konfigurace proxy serverů

HTTP proxy

Port

0

☐ Použít tento proxy server také pro HTTPS

HTTPS proxy

Port

0

SOCKS server

localhost

Port

10001

☐ SOCKS v4

☒ SOCKS v5

☒ URL adresa pro automatickou konfiguraci proxy serverů

http://146.102.42.43/cms_proxy.pac

Znovu načíst