Sieť Govnet – informácia pre uzly

Upozornenie: Dokument obsahuje aktuálne informácie ku dňu vydania. Pravidlá a informácie môže prevádzkovateľ siete Govnet kedykoľvek jednostranne zmeniť. Aktuálne znenie dokumentu je dostupné v sieti Govnet na adrese https://govnet.gov.sk/. Táto adresa nie je publikovaná do Internetu.

verzia	dátum	popis
9.6	5.5. 2020	aktualizované adresy serverov , všeobecné požiadavky na uzol a doplnené sieťové služby
9.5	24.9. 2018	odmazané odkazy na sieť 172.16.0.0/12, pridaná informácia o novom proxy serveri newproxy.gov.sk, doplnené bezpečnostné požiadavky na uzol
9.4	8.3. 2017	doplnené verzionovanie, čísla strán, drobné upresnenia
9.3	20.2. 2017	zmenená IP adresa na SPAM karanténu (prístup je sprostredkovaný cez WAF)

Obsah

Obsah 1
Technické požiadavky na uzol 1
Všeobecné požiadavky 2
Pravidlá pre IPv4 adresáciu 2
Pravidlá pre IPv6 adresáciu 2
Konfigurácia proxy 2
Konfigurácia mailov 2
Konfigurácia DNS 3
Integrácia do UPVS, e-kolkov 3
Bezpečnostné požiadavky na uzol 3
Kontakty 5
Úvod do siete Govnet - informácia pre uzly 5
Typický spôsob využitia siete Govnet 7
Štandartné nastavenia 7
Webová stránka 8
Iná komunikácia mimo siete Govnet 8

Technické požiadavky na uzol

Uzlu siete Govnet pri pripájaní prideľujeme IP adresy z rôznych rozsahov, najmä z rozsahu Govnet-internet (/25 IPv4 adries a typicky /48 IPv6 adries)

Všeobecné požiadavky

- Pre zriadenie nového Govnet uzla je potrebné zo strany žiadateľa o pripojenie zabezpečiť housing vo svojej technologickej miestnosti. Presná špecifikácia parametrov housingu závisí od požiadaviek žiadateľa. Jedná sa predovšetkým o zabezpečenie:
    - asistovaného vstupu do technologickej miestnosti s dostatočným voľným miestom v RACKu
    - zálohovaného napájania s potrebným príkonom
    - vykáblovanie pripojenia smerom na infraštruktúru žiadateľa
- uzol musí mať vlastný e-mailový server
- uzol musí používať DNS servery, proxy servery, e-mailové servery siete Govnet
- Uzol musí mať vlastný DNS server pre Govnet
- webové sídlo uzla musí patriť do domény .gov.sk
- uzol musí mať zriadenú e-mailovú adresu govnet@menouzla.gov.sk, nasmerovanú na relevantný technický kontakt
- uzol musí NASES-u oznámiť aktuálne technické, administratívne a bezpečnostné kontakty a priebežne ich aktualizovať

Pravidlá pre IPv4 adresáciu

- 0-7 infraštruktúra (routre Govnet, routre uzol)
- 8-15 DNS servery
- 16-23 mail servery
- 24-31 VPN koncentrátory

- uzol musí do siete Govnet routovať celý rozsah 100.64.0.0/10
- uzlu odporúčame udržiavať informácie o pridelených IP adresách v aplikácii https://ipv6.gov.sk

Pravidlá pre IPv6 adresáciu

- uzol musí do siete Govnet routovať celý IPv6 adresný rozsah, ktorý je pridelený pre sieť Govnet
- uzlu odporúčame udržiavať pridelené sieťové alokácie v aplikácii https://ipv6.gov.sk

Konfigurácia proxy

- Povoliť komunikaciu:
    - wsa.gov.sk port 3128 - použiť doménové meno, súčasná adresa 100.64.16.190:3128 sa môže v budúcnosti zmeniť
    - newproxy.gov.sk port 3128 – použiť doménové meno, súčasná adresa 100.64.16.55:3128 sa môže v budúcnosti zmeniť

Konfigurácia mailov

- Povoliť prijímanie mailov z centrálnych mailových severov v sieti Govnet 2
    - ng2inmail.gov.sk - 100.64.16.30
    - 100.112.0.16 s bitovou maskou (nie sieťová maska) 0.15.255.7 - mailové servery uzlov v Govnet 2

- Povoliť odosielanie mailov na poštové servery podľa individuálneho plánu pre uzol - niektoré z uvedených:
    - ng2inmail.gov.sk (mail.gov.sk) - 100.64.16.30
    - 100.112.0.16 s bitovou maskou (nie sieťová maska) 0.15.255.7 - mailové servery uzlov v Govnet 2

- Povoliť HTTPS komunikaciu cez port 443 do SPAM karantény:
    - ng2karantena1.gov.sk, ng2karantena2.gov.sk - 100.112.0.126

Konfigurácia DNS

- DNS server na uzle musí robiť iteratívny lookup v rámci siete Govnet a rekurzívny lookup do internetu cez nadradené DNS servery Govnetu:
    - g2nsg1.gov.sk - 100.64.16.8
    - g2nsg2.gov.sk - 100.64.16.9

- MX záznamy pre uzol:
    - s vyššou prioritou - uzlový mailový server
    - s nižšou prioritou - g2inmail.gov.sk, ako záložná cesta v prípade nedostupnosti niektorého uzlového servera

Integrácia do UPVS, e-kolkov

- nevyhnutné podmienky:
    - IPSec VPN tunel do UPVS, e-kolkov
        - uzol používa na komunikáciu VPN koncentrátor z rozsahu 100.112.X.0/25. Tento rozsah sa nepoužíva na priamy prístup k poskytovaným službám.
        - každá organizácia má vyhradený tunelový koordinovaný adresný rozsah, ktorý sa používa iba vo VPN tuneloch a nie je v Govnet-e routovaný. Tento rozsah sa používa na prístup k poskytovaným službám.

Bezpečnostné požiadavky na uzol

- Webové aplikácie v sieti Govnet
    - Webové aplikácie by mali byť realizované rovnakým spôsobom, ako v prípade nasadenia webovej stránky do serverovej farmy NASES - statickým exportom hostovaným v NASES, typicky štrukturovaným pomocou dynamického webu aj s manažmentom a statickou kópiou webu.

        - ***Dynamický web*** je preferovane hostovaný na samotnom uzle, ale voliteľne tiež v NASES vedľa statického webu. Je hostovaný na samostatnom URL, odlišnom od publikovaného verejného URL.
        - Dynamický web generuje stránku obvyklým “dynamickým spôsobom”
        - Všetky lokálne URL sú “SEO friendly” a relatívne. Nikdy nie absolútne. URL neobsahuje otázniky.
        - Jazyk je kódovaný v URL.
        - Vyhľadávanie je vyriešené cez browser-side knižnicu a JSON index stránky (dynamicky generovaný podľa aktuálneho obsahu redakčného systému na statickom URL).

- Štatistika je riešená cez externú službu.
- Dynamický web je prístupný len z vybraných IP adries, hostovaný buď u zákazníka na Govnet uzle (preferované), alebo v NASES. Dynamický web nie je viditeľný z Internetu.

- ***Statický web*** je vytvorený automaticky rekurzívnym sťahovaním z dynamického webu, napríklad každých 15 minút. Táto statická kópia je prekopírovaná na webhosting NASES.
- Statický web neobsahuje manažment a ani žiadne dynamické skripty.
- V prípade, že je potrebné riešiť kontaktný formulár, rieši sa buď vnorením externej služby, alebo pridaním jedného dobre zauditovaného dynamického skriptu, na ktorý sa odkazuje web.

- Pre obmedzenie a zníženie rizika je potrebné vykonávať penetračné testy na webové aplikácie v sieti Govnet. Tieto penetračné testy môžu byť vykonávané:
  - Treťou stranou - v tomto prípade je potrebné dodržiavať formát oznamovania penetračných testov.
  - Službu penetračných testov vykonáva aj GOV CERT SK (https://www.cert.gov.sk)
  - V oboch prípadoch je potrebné zaslať požiadavku oficiálnou cestou na GOV CERT SK.

- V záujme najrýchlejšiej reakcie na bezpečnostný incident si GOV CERT SK vyhradzuje právo na testovanie zraniteľností zo zachytených incidentov na cieli v sieti Govnet. Týmto spôsobom zabezpečuje GOV CERT SK aktívnu kontrolu nad cieľom a jeho potenciálnou kompromitáciou.
- Uzol je povinný nahlasovať bezpečnostné incidenty a proaktívne kooperovať pri jeho riešení na nasledujúce kontakty:
  - web: **cert.gov.sk**
  - email: **incident@cert.gov.sk**
  - tel.číslo:

Kontakty

Uzol môže kontaktovať prevádzkovateľa siete Govnet niektorým z týchto spôsobov:

- tiketovým systémom na adrese https://servicedesk.gov.sk/ (povinný spôsob pre zadávanie nových požiadaviek a change requestov)
- e-mailom na govnet@nases.gov.sk (všeobecné informácie, havarijné stavy a podobne)
- telefonicky na čísle je +421 (0)2 3278 0780 (urgentné hlásenie havarijných stavov)

Úvod do siete Govnet - informácia pre uzly

Sieť Govnet, ktorá je budovaná už od roku 1993, prepája desiatky uzlov štátnej správy (medzi inými ministerstvá, Úrad Vlády, Kanceláriu Prezidenta a ďalšie) a poskytuje im širokú škálu služieb vrátane privátneho - od internetu nezávislého - vzájomného prepojenia, verejného pripojenia k internetu, služieb web hostingu, server housingu, antivírusovú a antispamovú ochranu.

Jedným z hlavných dizajnových motívov siete Govnet je umožniť využitie sieťových služieb bez závislosti od akejkoľvek externej infraštruktúry, čo umožňuje garantovať spojenie v akejkoľvek situácii a nastoľuje jednoduchý spôsob identifikácie a odstraňovania problémov. Z tohto pohľadu sa Govnet nechápe ako poskytovateľ pripojenia do Internetu, ale ako poskytovateľ prepojovacej sieťovej infraštruktúry, ktorý:

- definuje jednotný adresný plán (evidovaný v aplikácii https://ipv6.gov.sk/),
- definuje pravidlá využívania častí adresného plánu jednotlivými uzlami a sprostredkúva ich vzájomné prepojenie,
- prevádzkuje technické zariadenia nevyhnutné pre plnohodnotné fungovanie, ako napr. vnútorné servery DNS (g2nsg1, g2nsg2),
- prevádzkuje pridané služby siete Govnet,
- vykonáva pokročilý prevádzkový a bezpečnostný monitoring siete, jej údržbu. Spolupracuje s uzlami pri využívaní a rozvoji siete a pri riešení bezpečnostných incidentov

Ďalším z dizajnových motívov siete Govnet je bezpečnosť a spoľahlivosť, ktorá je zahrnutá v návrhu siete, a tiež v procesoch a postupoch jej využívania. Za časť týchto procesov je zodpovedný prevádzkovateľ siete Govnet, za ďalšiu časť sú zodpovedné jednotlivé uzly. Za tým účelom uzly môžu využívať a/alebo musia dodržiavať:

- tiketový a dohľadový systém
- telefonické a e-mailové kontakty
- pravidlá pre správne využitie komunikačnej siete, z ktorých časť je formalizovaná v priebežne aktualizovanom verejnom dokumente "Požiadavky na uzol" (napr. rozdelenie rozsahu pre routre, VPN koncentrátory, mail servery, ostatné servery, kvôli jednotným firewallovým pravidlám naprieč sieťou Govnet), časť je súčasťou interných postupov a s uzlom sa komunikujú v rámci riešenia jednotlivých tiketov (napr. nepovoľujú sa priame spojenia zo siete Internet a podobne)
- komunikácia medzi uzlami musí byť realizovaná prostredníctvom siete Govnet

Sieť Govnet poskytuje tiež centrálne služby s pridanou hodnotou ako napríklad:

- bezpečnú e-mailovú komunikáciu
- bezpečný prístup na web
- IP telefóniu
- prepojenie do Internetu
- NTP
- Vytváranie Virtual Private Netvork

Keďže sieť govnet „G2“ je stavaná už s ohľadom na podporu MPLS, je možne pri požiadavke zákazníka o vytvorenie VPN siete v rámci prostredia Govnet tuto požiadavku zrealizovať. V súčasnosti je celá produkčná komunikácia vygenerovaná Govnet uzlami smerovaná do týchto VPN: govnet, inet, iptv, voice, testa, wifi. Každá jedna požiadavka govnet uzla o vytvorenie VPN bude samostatne posudzovaná.

- Poskytnutie IPv6 adresného rozsahu

  Prevádzkovateľovi siete Govnet - NASES-u boli spoločnosťou RIPE prenajaté IPv6 adresne rozsahy, z ktorých je možne poskytnúť Govnet uzlu ucelený adresný rozsah.

- Služby IPTV

  Pri poskytovaní služieb IPTV je NASES len v pozícii sprostredkovateľa IP konektivity medzi koncovými stanicami (Set-top Box) a poskytovateľom programovej ponuky (kontentu) spoločnosti SWAN.

- Hosťovský internet

  Pri potrebe Govnet uzla mat k dispozícii (napr. pre svojich zamestnancov a klientov v priestoroch uzla) prístup čisto len do internetu, ktorý je oddelený od produkčných privátnych dát, je možne poskytnúť takúto konektivitu do internetu. Jedna sa o neobmedzenú konektivitu čo do objemu sťahovaných dát i čo do rýchlosti (tá však závisí od rýchlosti Govnet linky, ktorou je uzol pripojený do Govnet-u).

- Vzdialené pripojenie do siete Govnet cez FortiVPN pripojenie:
  Vzhľadom k prísnej bezpečnostnej politike v prostredí siete Govnet, jediným riešením zabezpečenia prístupu pre externých dodávateľov a správcov k informačným systémov na jednotlivých OVM je zriadiť VPN pripojenie. Prístup je generovaný na konkrétneho človeka. Nie je možný súčasný viacnásobný prístup cez jeden účet.

- Sledovanie štatistík vyťaženia Govnet linky
  Pre potreby mať informácie o vyťažení pripojenia do govnetu je možné zriadiť prístup do monitorovacieho systému. Štatistiky je možné prezerať v takmer ľubovoľne zvolenom časovom rozsahu.

Služby sú poskytované centrálne. To výrazne zvyšuje efektivitu prevádzky týchto služieb v prostredí verejnej správy. Napríklad prevádzkovaním jedného AV/AS riešenia namiesto viacerých, prípadne jednotným obstaraním spoločného pripojenia do siete Internet.

Pripojenie siete Govnet do Internetu a do iných sietí je redundantne realizované v prepojovacích bodoch prostredníctvom sady DMZ sietí GOVNET Edge, ktoré obsahujú perimetrové ochranné prvky, aplikačné firewally a aplikačné proxy pre jednotlivé protokoly:

- webový proxy cluster: wsa.gov.sk, newproxy.gov.sk
- edge DNS severy: g2ns1.gov.sk, g2ns2.gov.sk (uzly ich využívajú sprostredkovane pomocou vnútorných DNS serverov g2nsg1.gov.sk a g2nsg2.gov.sk)
- webový aplikačný firewall F5 - ASM na spojenia z internetu do Govnet-u, ak uzol využíva službu ochrany prichádzajúcich spojení
- mailovú farmu: mail.gov.sk (uzly ju využívajú pomocou vnútorných adries)

Sieť Govnet má centrálny prevádzkový a bezpečnostný dohľad v podobe dohľadového pracoviska a ďalšieho automatizovaného softvéru.

Všetky prvky Govnet Edge, vrátane upstream liniek do SIX a do Internetu a tiež väčšina pripojení uzlov (podľa typu uzlu), sú budované redundantne s vylúčením single point of failure na fyzickej, sieťovej aj aplikačnej úrovni.

Typický spôsob využitia siete Govnet

Typické využitie siete Govnet uzlom je nasledovné (príklad je len pre ilustráciu, konkrétne a aktuálne pravidlá je možné nájsť v dokumente “Požiadavky na uzol”):

Štandartné nastavenia

- uzol dostane od Govnet-u adresný rozsah napr. 100.112.500.0/25 a subdoménu .gov.sk, typicky ministerstvoXYZ.gov.sk.

- uzol si na tomto rozsahu nastaví jednotlivé zariadenia, najmä DNS server a mail server

- DNS server poskytuje informácie o doméne ministerstvoXYZ.gov.sk pre ostatné uzly siete Govnet. Tento DNS server bude vždy oznamovať **adresy z Govnetového rozsahu** 100.112.500.0/25, napr.:
  - mail.ministerstvoXYZ.gov.sk IN A 100.112.500.16 ,
  - vpn1.ministerstvoXYZ.gov.sk IN A 100.112.500.24,
  - www.ministerstvoXYZ.gov.sk IN A 100.112.500.32.

  TENTO DNS SERVER NIKDY NEPOSKYTUJE VEREJNÉ INTERNETOVÉ ADRESY.

- uzol nastaví svoj DNS resolver tak, aby resolvoval domény v .gov.sk priamo a všetky ostatné dopyty posielal na nadradený server g2nsg1.gov.sk, g2nsg2.gov.sk. Až tieto DNS servery spracujú rekurzívny lookup do Internetu prostredníctvom dopytov na ďalšie servery v Govnet Edge.

- odchádzajúce webové spojenia z uzla sú sprostredkované cez proxy servery wsa.gov.sk alebo newproxy.gov.sk

Webová stránka

- uzol si môže vytvoriť webovú stránku www.ministerstvoXYZ.gov.sk. Táto stránka **nemôže byť prevádzkovaná mimo siete Govnet.** Musí byť prevádzkovaná v rámci interného IP adresného rozsahu siete Govnet. Napríklad na IP adrese 100.112.500.32. Dôvodom je, aby bola vždy dostupná pre ostatné uzly siete Govnet.

- Ak má byť stránka dostupná z verejného Internetu, uzol požiada o NAT cez tiketový systém. Zároveň prevádzkovateľ siete Govnet zavedie záznamy s verejnými adresami do verejného DNS pre doménu .gov.sk. Tento DNS spravuje prevádzkovateľ siete Govnet.

- Uzol si voliteľne vyžiada od prevádzkovateľa siete Govnet, aby dohľadové centrum siete Govnet zabezpečilo bezpečnostnú kontrolu prichádzajúcich spojení na uzlový web server prostredníctvom webového aplikačného firewallu (WAF), umiestneného v Govnet Edge. Táto ochrana vyžaduje, aby v sieti Govnet bol nainštalovaný TLS certifikát uzlovej webovej stránky (TLS certifikát LetsEncrypt na požiadanie zabezpečí NASES). To umožňuje bezpečnostnému prvku WAF nahliadnuť do obsahu komunikácie. Očistená komunikácia je na vnútorný server opäť smerovaná šifrovaným protokolom TLS.

Iná komunikácia mimo siete Govnet

- Ak chce uzol komunikovať s iným uzlom, alebo s adresou v Internete, požiada prevádzkovateľa siete Govnet cez tiketový systém o povolenie firewallových pravidiel s uvedením protokolu, konkrétnych zdrojových a cieľových IP adries a portov.
- Tieto žiadosti sa akceptujú len od poverených kontaktných osôb na uzloch, nie od ich subdodávateľov.
- Žiadosti podliehajú schvaľovaniu podľa internej metodiky. Typicky sú zamietnuté žiadosti o povolenie prichádzajúcej komunikácie z Internetu na port 25=smtp (pretože je potrebné využívať AV/AS farmu v Govnet Edge), 22=ssh (pretože uzol má pre svojich dodávateľov vybudovať VPN prístup), žiadosti s príliš širokými neopodstatnenými pravidlami, žiadosti podané za iný uzol (komunikácia medzi uzlami musí byť odsúhlasená kontaktnými osobami oboch strán).
- Prevádzkovateľ siete Govnet, ak to situácia vyžaduje, môže požiadať uzly o revíziu starých pravidiel a potvrdenie, že majú naďalej platiť. Ak uzol na požiadanie nedodá potvrdenie o platnosti pravidiel, NASES si vyhradzuje právo na ich zrušenie.
- Domény iné ako .gov.sk:

  Uzol môže mať voliteľne aj doménu ministerstvoXYZ.sk hostovanú v sieti Govnet. Môže ju prevádzkovať buď u seba, alebo využívať komplexné služby prevádzkovateľa siete Govnet vrátane registrácie domény.