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
9.7	15 1.2023	Zapracovanie zmien s ohľadom na Govnet 3
9.6	24 4 2020	Aktualizovane adresy serverov
9.5	24 9 2018	odmazané odkazy na sieť 172 16 0 0/12, pridaná informácia o novom proxy servery 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 (pred servery bol doplnený WAF)

Obsah

Technické požiadavky na uzol

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

Všeobecné požiadavky

- uzol musí mať vlastný e-mailový server
- uzol musí mať vlastný DNS server
- uzol musí používať DNS servery, proxy servery, e-mailové servery siete 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 NASESu 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 server
- 16-23 mail server
- 24-31 VPN koncentrátory

- uzol musí do siete Govnet smerovať celý rozsah 100.64.0.0/10

Pravidlá pre IPv6 adresáciu

- uzol musí do siete Govnet smerovať celý IPv6 adresný rozsah, ktorý je pridelený pre sieť Govnet

Konfigurácia proxy

- Povoliť komunikáciu na Govnet proxy.
  - newproxy.gov.sk port 3128 – použiť doménové meno, súčasná adresa 100.64.16.55:3128 sa môže v budúcnosti zmeniť
  - všetka odchádzajúca HTTP/HTTPS komunikácia z uzla musí smerovať na Govnet proxy
  - komunikácia do internetu mimo Govnet proxy nie je povolená
  - o výnimky je potrebné požiadať cez Govnet Helpdesk

Konfigurácia mailov

- Povoliť prijímanie mailov z centrálnych mailových severov v sieti Govnet
  - g2inmail.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
- Povoliť odosielanie mailov na poštové servery podľa individuálneho plánu pre uzol - niektoré z uvedených·
  - g2inmail.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 komunikáciu cez port 443 do SPAM karantény
  - g2karantena1.gov.sk, g2karantena2.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 - 100.64.16.8
    - G2NSG2 - 100.64.16.9

- DNS DNS server na uzle musí mať povolené sťahovanie zónových súborov pre G2NSG1.GOV.SK a G2NSG2.GOV.SK port TCP 53
- MX záznamy pre uzol:
    - s nižšou prioritou - uzlový mailový server ako záloha pre prípad nedostupnosti g2inmail.gov.sk

s vyššou prioritou - g2inmail.gov.skIntegrácia do UPVS, e-kolkov

- nevyhnutné podmienky:
    - IPSec VPN tunel do UPVS, e-kolkov
        - uzol používa na komunikáciu VPN koncentrátorov rozsah 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 GOVNETe smerovaný. 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. A to realizovaním statickým exportom hostovaným v NASES, typicky štrukturovaná 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, napr každých 15 minút Táto statická kópia je nasledovne nahrávaná na webhosting NASES.

- Statický web neobsahuje manažment 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.
  - V oboch prípadoch je potrebné zaslať požiadavku oficiálnou cestou na GOV CERT SK.
- V záujme najrýchlejšej 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 **+421 2 3278 0780**

SSL certifikáty vydávané externými vydavateľmi pre potreby uzlov:

Ak uzol požiada o vydanie SSL certifikácu externého vydavateľa, ten spravidla vyžaduje overenie vlastníctva domény. Overenie väčšinou prebieha dvoma spôsobmi:

1. overenie pomocou potvrdenia linku odoslanom v mailí registrátorovi domény. V takomto prípade je potrebné vytvoriť prostredníctvom servicedesku-u požiadavku na NASES, kde sú uvedené údaje.
- uzol, ktorý žiada o vydanie certifikátu
- vydavateľ certifikátu
- pokiaľ nie je oslovený priamo vydavateľ, tak firma, ktorá sprostredkuje vydanie certifikátu a od ktorej dôjde požiadavka na overenie vlastníctva domény
- kontaktná osoba, ktorá bude uvedená v mailí od vydavateľa certifikátu
- domény, pre ktoré má byť certifikát vydaný
- pri zadávaní požiadavky externému vydavateľovi certifikátu je potrebné uviesť maily, na ktoré má byť odoslaná požiadavka na overenie vlastníctva domény.
-- postmaster@gov.sk
-- webmaster@gov.sk
V prípade, ak dôjde mailová požiadavka od vydavateľa certifikátu na overenie vlastníctva domény bez toho, aby boli k dispozícii údaje uvedené vyššie, nebude požiadavka od vydavateľa z bezpečnostných dôvodov potvrdená.

2. prostredníctvom reťazca vloženého do autoritatívneho DNS servera pre doménu v internete. V žiadosti podanej cez servicedesk je potrebné uviesť:
- uzol, ktorý žiada o vydanie certifikátu
- domény, pre ktoré má byť certifikát vydaný
- textový reťazec, ktorý má byť zavedený do DNS
Po vydaní certifikátu je potrebné zaslať žiadosť o zrušenie záznamu v DNS.

Niektorí vydavatelia vyžadujú aj ďalšie spôsoby overenia, napríklad oficiálny WEB, kde sú uvedené údaje o žiadateľovi (adresa firmy, kontakt,), prípadne je požadované aj telefónne číslo, kde je možné telefonicky overiť údaje o žiadateľovi. Tieto a prípadne ďalšie požiadavky na overenie vybavuje žiadateľ po vlastnej línii.

Kontakty

Uzol môže kontaktovať prevádzkovateľa siete GOVNET niektorým z týchto spôsobov

- tiketovacím systémom na adrese https://helpdesk.gov.sk/ (povinný spôsob pre zadávanie nových požiadaviek alebo požiadaviek na zmenu)
- 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 sa buduje už od roku 1993, prepája desiatky uzlov štátnej správy (medzi inými všetky ministerstvá, Úrad vlády SR, Kanceláriu Prezidenta SR a ďalšie) Poskytuje im širokú škálu služieb vrátane privátneho - od internetu nezávislého prepojenia, verejného pripojenia k internetu, služieb web hostingu a server housingu, alebo 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 pravidlá využívania častí adresného plánu prideleného jednotlivým uzlom 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 monitoring siete a jej údržbu a spolupracuje s uzlami pri využívaní a rozvoji siete,
- vykonáva pokročilý bezpečnostný monitoring siete, prevádzkuje dohľadové centrum a spolupracuje s uzlami na riešení bezpečnostných incidentov

Ďalším z dizajnových motívov siete GOVNET je bezpečnosť a spoľahlivosť, ktorá je zahrnutá v návrhu siete, ako aj 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

- tiketovací 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 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 tiež centrálne poskytuje služby s pridanou hodnotou ako napríklad

- bezpečnú e-mailovú komunikáciu
- bezpečný prístup na web
- IP telefóniu
- prepojenie do Internetu
- VPN pripojenia
- NTP
- DNS
- IPTV

a mnohé ďalšie

To, že služby sú poskytované centrálne, výrazne zvyšuje efektivitu prevádzky týchto služieb v prostredí verejnej správy, napríklad prevádzkovaním jedného AV/AS riešenia, miesto viacerých, alebo 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, napr

- webový proxy cluster· newproxy.gov.sk
- edge DNS severy: g2ns1.gov.sk, g2ns2.gov.sk (uzly ich využívajú sprostredkovane pomocou vnútorných DNS serverov g2nsg1, g2nsg2)
- webový aplikačný firewall F5 - ASM na spojenia dovnútra, ak uzol využíva službu ochrany prichádzajúcich spojení
- mailovú farmu· mail.gov sk (uzly ju využívajú pomocou vnútorných adries g2mail.gov.sk)

Sieť GOVNET má centrálny prevádzkový a bezpečnostný dohľad pomocou dohľadového pracoviska a ďalšieho automatizovaného softvéru Všetky prvky samotnej prepojovacej siete GOVNET, 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")

Štandardne nastavenia

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

- uzol si na tomto rozsahu nastaví jednotlivé zariadenia, najma DNS server a mail server, s ohľadom na požiadavky uvedené v odseku „Pravidlá pre IPv4 adresáciu"

- DNS server poskytuje informácie o doméne ministerstvoXYZ.gov.sk pre ostatné uzly siete GOVNET. Tento DNS server bude vždy oznamovať **adresy z GOVNET 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 robia rekurzívny lookup do Internetu prostredníctvom dopytov na ďalšie servery v GOVNET Edge

- uzol robí odchádzajúce webové spojenia prostredníctvom Govnet proxy newproxy.gov.sk

Webová stránka

- uzol si urobí webovú stránku www.ministerstvoXYZ.gov.sk. Táto stránka **nemôže byť prevádzkovaná mimo siete GOVNET**, ale musí byť prevádzkovaná v rámci siete GOVNET napr. 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 tiketovací systém. Zároveň prevádzkovateľ siete GOVNET zavedie záznamy s verejnými adresami do verejného DNS pre doménu .gov.sk. Toto DNS spravuje prevádzkovateľ siete GOVNET.

- Uzol si voliteľne vyžiada od prevádzkovateľa siete GOVNET, aby dohľad siete GOVNET robil bezpečnostný dohľad prichádzajúcich spojení na web server prostredníctvom webového aplikačného firewallu (WAF), umiestneného v GOVNET Edge. Táto ochrana vyžaduje, aby v sieti GOVNET bol nainštalovaný TLS certifikát webovej stránky (TLS certifikát LetsEncrypt vie na požiadanie zabezpečiť GOVNET), čo umožňuje bezpečnostnému prvku WAF nahliadnuť do obsahu komunikácie. Očistená komunikácia je na vnútorný server opať 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 tiketovací systém o povolenie firewallových pravidiel s uvedením protokolu, konkrétnych zdrojových a cieľových IP adries a portov.
- Tieto žiadosti sa akceptujú len od vybraných 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, môže ak to situácia vyžaduje, zažiadať uzly o revíziu starých pravidiel a potvrdenie, že majú naďalej platiť.

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.