Tehnična navodila za priklop

Navodila za upravitelje omrežnih naprav

Tip naloge: Tehnična navodila
Datum: N/A
Verzija: 2.0

Koda: Navodila za upravitelje omrežnih naprav

PODATKI O NALOGI

Naslov	Vzpostavitev komunikacijskega okolja
Investitor	Ministrstvo za zdravje
Predstavnik investitorja	Andrej Žlender
Naročnik	Ministrstvo za zdravje
Predstavnik naročnika	Andrej Žlender
Vodja	
Datum zaključka naloge	N/A

Verzije dokumenta

Datum	Različica	Opis sprememb	Avtor	Pregledal in odobril
5.1.2012	0.9	Začetni neuradni dokument	Martin Zemljič Astec d.o.o.	
14.1.2012	1.0	Dodani zahtevnejši scenariji	Martin Zemljič Astec d.o.o.	
2.2.2012	1.1	Brskalniki, DNS	Martin Zemljič Astec d.o.o.	
24.7.2014	1.2	Uskladitev s stanjem	Martin Zemljič Astec d.o.o.	
11.2.2015	1.3	Dopolnitve ob vzpostavitvi RDC	Miro Valjavec Astec d.o.o.	
7.3.2015	2.0	Dopolnitve	Miro Valjavec PRO.ASTEC d.o.o.	

Kazalo

1.1.1.1.1 Namen dokumenta in ciljna publika

Dokument je namenjen uporabnikom lokalnih računalniških omrežij, ki so priklopljena ali bodo priklopljena v komunikacijsko hrbtenico »eZdravje« oziroma »zNET«. Ponudnik hrbtenice je Ministrstvo za zdravje.

Namenjen je osebam, ki so zadolžene za urejanje računalniških povezav pri subjektih z navedenim interesom. Od uporabnika dokumenta se pričakuje temeljno poznavanje delov komunikacijske opreme in osnovni pojmi IPv4 transportnega protokola.

Opisuje omrežne zahteve, ki jim mora uporabnik hrbtenice zadostiti, da jo lahko kakovostno uporablja. Za izpolnitev zahtev ponuja tudi nekaj scenarijev in navodil za posege na omrežni opremi subjekta.

Dokument **ne predpisuje** varnostnih mehanizmov. Zanje je odgovoren drug dokument, glej prilogo.

Dokument **nima normativne** narave. Upoštevanje dokumenta pomaga k uspešni rabi hrbtenice. Neupoštevanje dokumenta **lahko vodi k težavam** pri njeni uporabi, breme odprave težav nosi subjekt sam.

2 Povzetek navodil

2.1 Uporabniki brez posebnih pooblastil

Za uspešno uporabo običajnih storitev v omrežju, ki so predvsem spletne, mora omrežje subjekta usmeriti proti hrbteničnemu usmerjevalniku IPv4 naslovne prostore 172.24.0.0/15 in 172.29.0.0/16. Poskrbeti mora, da se domene znet.si, ezdrav.si in sigov.si razrešujejo na notranjih DNS strežnikih. Na dan pisanja dokumenta je mogoče uporabiti strežnike 172.29.192.8 in 172.29.192.16.

2.2 Uporabniki z višjimi pooblastili

Poleg nastavitev morajo upoštevati zahteve za delovne postaje in revizijski sled. Poleg ustrezne varnostne programske opreme na delovnih postajah (protivohunska in protivirusna) morajo zagotoviti sledljivost lastništva omrežnega naslova za 6 mesecev.

2.3 Uporabniki elektronske pošte v hrbtenici ali dostopa do interneta

Uporabniki elektronske pošte morajo ne glede na raven pooblastil poskrbeti za MX zapise za lastne poštne domene. Te kažejo na mail1.znet.si, mail2.znet.si ali na drug par strežnikov, ki velja za omrežje.

Uporabniki dostopa do interneta lahko do tega dostopajo le prek zastopniškega (proxy) strežnika, ki ga naslovijo z »proxy.znet.si« ali »proxy.is.ezdrav.si«, vrata 8080. Domene znet.si, ezdrav.si in sigov.si (lahko tudi druge) morajo biti za delovanje vpisane kot izjeme. Na voljo je »proxy.pac« datoteka na naslovu »proxypac.is.znet.si«. Slednjo je mogoče pripraviti za vsak subjekt posebej (se oblikuje dinamično glede na odjemalca).

2.4 Ponudniki storitev v hrbtenici

Storitve, namenjene več kot lastnemu subjektu, je potrebno umestiti v segment znotraj naslovnega prostora 172.29.224.0/19. Tipično je segment dosegljiv vsem uporabnikom hrbtenice. Imenovanje storitev mora zadoščati nekaterim zahtevam glede poimenovanja.

3 Slovar

- IPv4: Protokol za prenos podatkov po računalniškem omrežju. Podatki potujejo v obliki paketov, ki imajo med drugim izvorni naslov, ponorni naslov in podatke o vsebini višjih ravni
- Lokalno omrežje: nekoliko ohlapen pojem; po navadi si pod njim prestavljamo logične in fizične povezave med napravami, ki za medsebojno komunikacijo ne potrebujejo omrežnih prehodov (gateway, router).
- Hrbtenica: Logična povezava več različnih računalniških omrežij. Običajno združuje subjekte s podobnimi interesi in omogoča dostope do računalniških storitev, ki nečlanom niso preprosto dostopni.
- DNS: **D**omain **N**ame **S**erver, temeljna storitev na računalniškem omrežju ali hrbtenici, ki pretvarja imena storitev v njihove omrežne naslove ali obratno. Potrebna je za to, da odjemalec (brskalnik v računalniku) lahko izve, kam mora usmeriti zahtevek za (na primer) dosego strani »vesti.is.ezdrav.si«.
- Domena: V splošnem območje upravljanja. Običajno uporabljeno za območje upravljanja imen storitev v DNS. V urejenih omrežjih storitve naslavljamo z imeni, ki vsebujejo vsaj eno piko; ta razločuje komponente domene.
- DHCP: Temeljna storitev na računalniškem omrežju ali hrbtenici, ki računalnikom v določenih primerih dodeli omrežni naslov in nekatere druge podatke, potrebne za delovanje v izbranem okolju.
- Usmerjevalnik: Naprava v lokalnem omrežju, ki zna in zmore preposlati prejeti paket iz enega omrežja v drugo omrežje.
- Stikalo: Switch, omrežna naprava z več omrežnimi vmesniki. Obvlada prepošiljanje omrežnih paketov znotraj omrežja. Pogosto izvedena kot del druge naprave, na primer usmerjevalnika.
- DMZ: **D**e**m**ilitarized **z**one, splošna oznaka za namensko računalniško omrežje, namenjeno dostopu **drugih** subjektov do storitev, ki jih ponuja subjekt lastnik DMZ. DMZ je lahko internetni (je dosegljiv z interneta) ali drugače (dosegljiv na primer samo v hrbtenici eZdravja).
- Extranet: Splošna oznaka za računalniško omrežje, ki ni dosegljivo prek interneta, pač pa le pod določenimi pogoji. Običajno gre za povezavo med dvema različnima hrbtenicama, pri tem pojem »extranet« označuje tisti nabor storitev, ki jih ena hrbtenica dovoljuje dosegati drugi.
- VLAN: Posebna oblika paketa na računalniškem omrežju in konfiguracije naprave z ustrezno zmogljivostjo. Tako lahko po istem fizičnem vodniku (kablu) vodimo več različnih računalniških omrežij, ki se med seboj ne vidijo. Običajne delovne postaje

takih paketov ne prepoznajo, zato jih v običajne, npr. IPv4 pakete izluščimo na namenskih napravah, tipično stikalih.

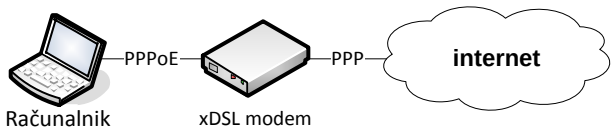
- Zastopnik: Proxy, proksi, posrednik. Aplikacija, ki sprejema ali prestreza omrežne zahtevke in jih na enak ali drugačen način posreduje proti končnemu cilju. Pogosto uporabljen za obvladovanje spletnega prometa iz notranjega omrežja v zunanjost.
- Požarna pregrada: Namenska naprava v omrežju, ki odloča o tem, ali je posamezen omrežni promet dovoljen ali ne. O tem se lahko odloča na podlagi vira, cilja in protokola (osnovne požarne pregrade), boljše pa zmorejo tudi pravila na podlagi uporabnika, aplikacije in drugih parametrov.
- IPS: **I**ntrusion **p**revention **s**ystem, sistem za preprečevanje vdorov je namenska naprava v omrežju, ki se posveča prepoznavanju škodljivega prometa, na primer prenosa virusov, napada spletnega strežnika, ipd.
- ISP: **I**nternet **s**ervice **p**rovider, ponudnik internetnih storitev. Pravna oseba, ki interesentu omogoča dostop do hrbtenice »internet« in s tem storitev, ki so drugod priklopljene na internet. Za to interesenta opremi z administrativnimi in tehničnimi podatki, ki omogočajo IPv4 promet, v novejšem času tudi IPv6.
- ADSL, xDSL: Način priklopa v omrežje in naprava za tak priklop. Običajno cenovno sprejemljiva različica priklopa v internet ali drugo hrbtenico. Običajno omogoča uporabo samo enega omrežnega naslova na strani uporabnika, poleg tega je za uporabnika hitrost oddajanja lahko le del hitrosti sprejemanja.

4 Navodila za prilagoditve lokalnega omrežja

4.1 Preprostejši scenariji

4.1.1 Scenarij »en računalnik in ADSL«

Logični načrt takega omrežja zgleda takole:



Slika »Računalnik + modem«

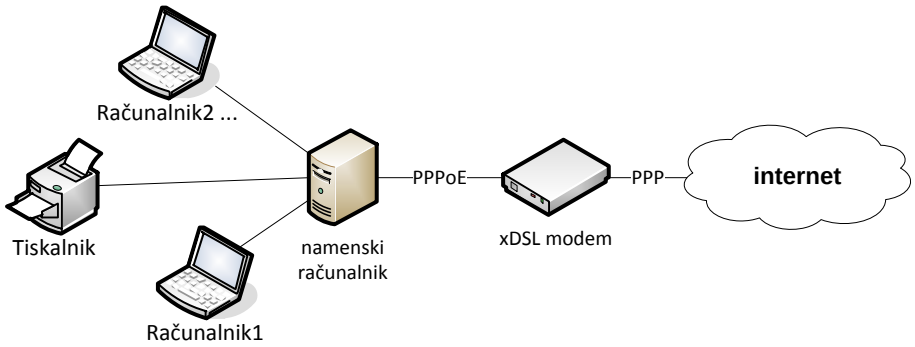
Računalnik je neposredno dosegljiv komur koli z interneta in lahko neomejeno dostopa na internet.

V tem primeru se bo med računalnik in modem vrinil usmerjevalnik. Brez dodatne investicije je mogoče priključiti toliko računalnikov, kot je prostih mest v stikalu, vgrajenem v usmerjevalnik (tipično 4 ali 8). Novo stanje je razvidno na sliki »Rešitev 1«.

Opozorilo: Dostop do interneta je bistveno spremenjen. Vpisati je potrebno nove DNS strežnike, računalniku dodeliti predpisano IPv4 številko in za dostop do interneta zastopniški strežnik.

4.1.2 Scenarij »računalnik z deljeno povezavo in ADSL«

Logični načrt takega omrežja izgleda takole:

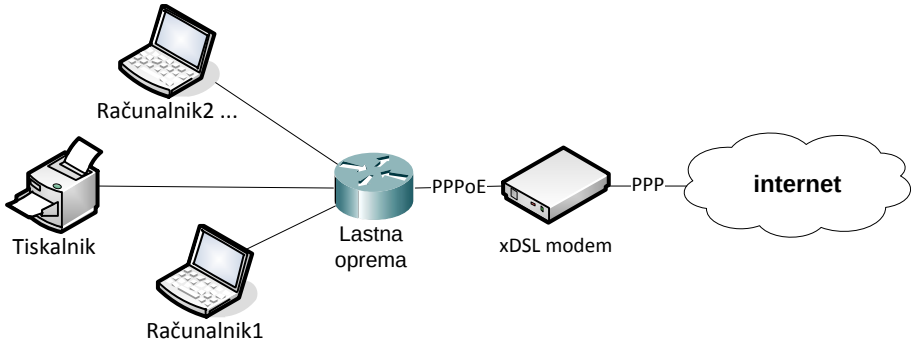


Slika »Računalnik z deljeno povezavo + modem«

V tem primeru se namenski računalnik nadomesti z usmerjevalnikom. Brez dodatne investicije je mogoče priključiti toliko računalnikov, kot je prostih mest v stikalu, vgrajenem v usmerjevalnik (tipično 4). Novo stanje je razvidno na sliki »Rešitev 1«.

Opozorilo: Namenski računalnik se umakne, lahko pa se uporabi kot navaden odjemalec v obstoječem omrežju. Preostale naprave pridobijo nove omrežne naslove in drugačen dostop do interneta.

4.1.3 Scenarij »lasten usmerjevalnik in ADSL«



Slika »Lasten usmerjevalnik + ADSL«

Ta scenarij je najpogostejši pri manjših organizacijah. Funkcionalno je enak scenariju »računalnik z deljeno povezavo + ADSL«, enaka je tudi rešitev.

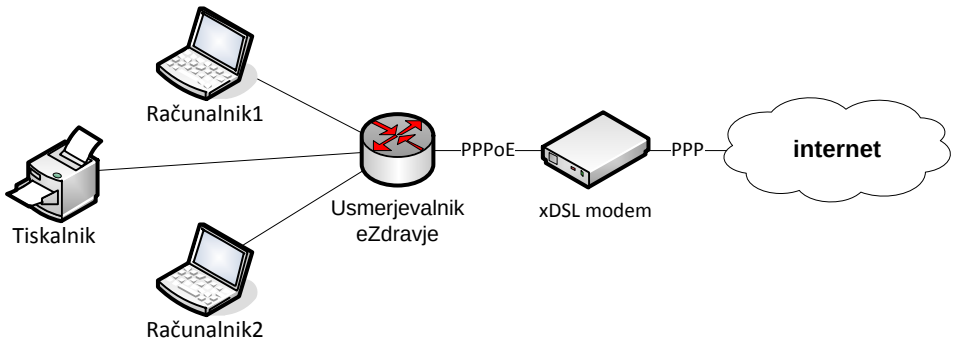
Če je »lastna oprema« imela tudi nalogo koncentriranja brezžičnega prometa, je funkcionalnost mogoče ohraniti ob upoštevanju varnostnih zahtev (glej ustrezni dokument).

Opozorilo: Dostop z interneta do naprav v notranji mreži po preklopu ni mogoč. Dostop do interneta se spremeni.

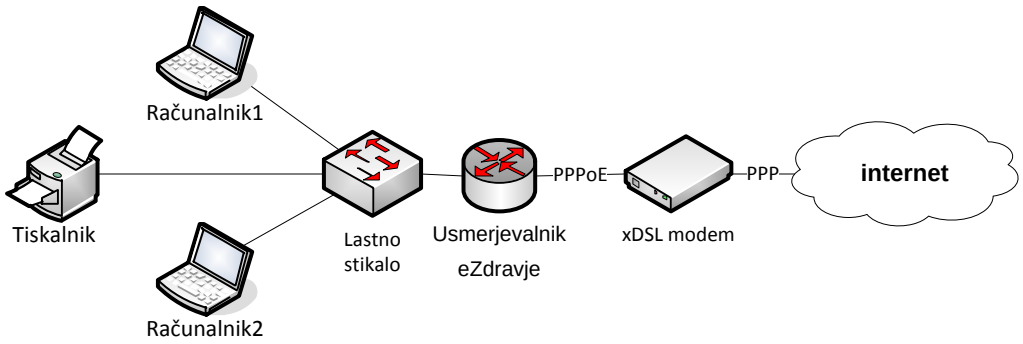
4.2 Rešitev preprostih scenarijev

Dosedanje scenarije je mogoče rešiti na način, da subjekt namesto trenutnega priklopa v internet uporabi napravo in infrastrukturo eZdravja. Dostavljena oprema lahko poskrbi za dodeljevanje omrežnih naslovov, vpisa DNS strežnikov in usmerjanja. Ne more poskrbeti za avtomatsko prekonfiguracijo elektronske pošte in dostopa do interneta. Ne omogoča

oddaljenega dostopa (npr. s potovanja, od doma) do naprav v omrežju. Ne omogoča internetne dostopnosti morebitnih javnih strežnikov, ki so bili izvedeni na takem omrežju.



Slika »Rešitev 1«, kjer je na usmerjevalniku dovolj vrat za vse naprave



Slika »Rešitev 1«, kjer je potrebno vključiti dodatno stikalo.

Tipično so v tej rešitvi dodeljeni naslovni prostori oblike 10.56…, 10.57…., 10.58…., 10.59…., in velikosti 8 do 256 naslovov. To na kratko imenujmo »mreža z masko 24 do 29 iz prostora 10.56.0.0/14«. Tipično je najnižja številka v taki mreži uporabljena za prehod.

Primer:

- Uporabnik ima omrežje 3 naprav, ki se zaključujejo na usmerjevalniku, najetem od internetnega ponudnika.
- Pri pregledu naprave je ugotovljeno, da imajo postaje dodeljene omrežne IPv4 naslove 192.168.0.3, 192.168.0,4, 192.168.0.5 z masko 255.255.255.0 (kar pomeni masko velikosti 24),
- DNS strežnikom 192.168.0.1 in
- prehodom 192.168.0.1.

Po novem bi lahko konfiguracija izgledala:

- Uporabnik ima omrežje 3 naprav, ki se zaključujejo na usmerjevalniku eZdravja.
- Obstoječi ADSL modem se ne spremeni in ostane v enaki vlogi.
- Napravam se dodelijo IPv4 omrežni naslovi 10.58.11.27, 10.58.11.28, 10.58.11.29 z masko velikosti 28 (kar zapišemo kot 255.255.255.240).
- Na usmerjevalniku eZdravja se lahko pripravi DHCP servis, ki ponudi računalnikom ustrezne omrežne nastavitve.
- Uporabi se DNS strežnike 172.29.192.8, 172.29.192.16, 172.29.64.8 (za aktualne vrednosti glej ustrezen dokument).

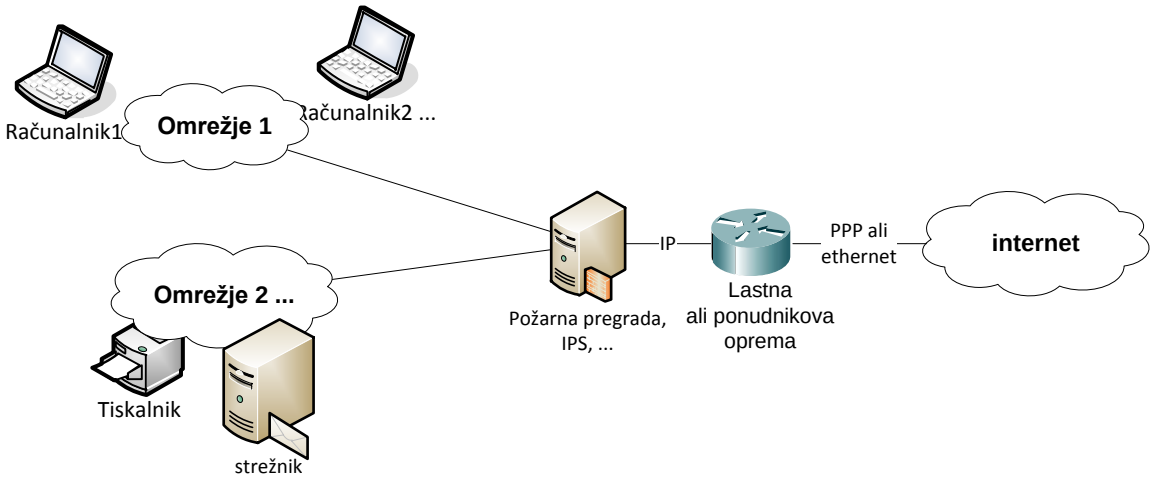
- Uporabi se prehod 10.58.11.25.

Za uporabo interneta je potrebno v brskalnik vpisati še: »proxy = proxy.znet.si, vrata 8080« ali »avtomatska konfiguracija je na naslovu http://proxypac.is.znet.si« (glej poglavje »Konfiguracija odjemalcev«).

4.3 Zahtevnejši scenariji

4.3.1 Odjemalec ima več lokalnih omrežij

Groba skica takega omrežja:



Označeni elementi »Požarna pregrada« in »Lastna ali ponudnikova oprema« niso nujno ločeni deli opreme. Dober del proizvajalcev združuje več funkcionalnosti v enem kosu opreme, zato je slika lahko preobsežna.

Uporabnik ima **samo en** zunanji omrežni naslov.

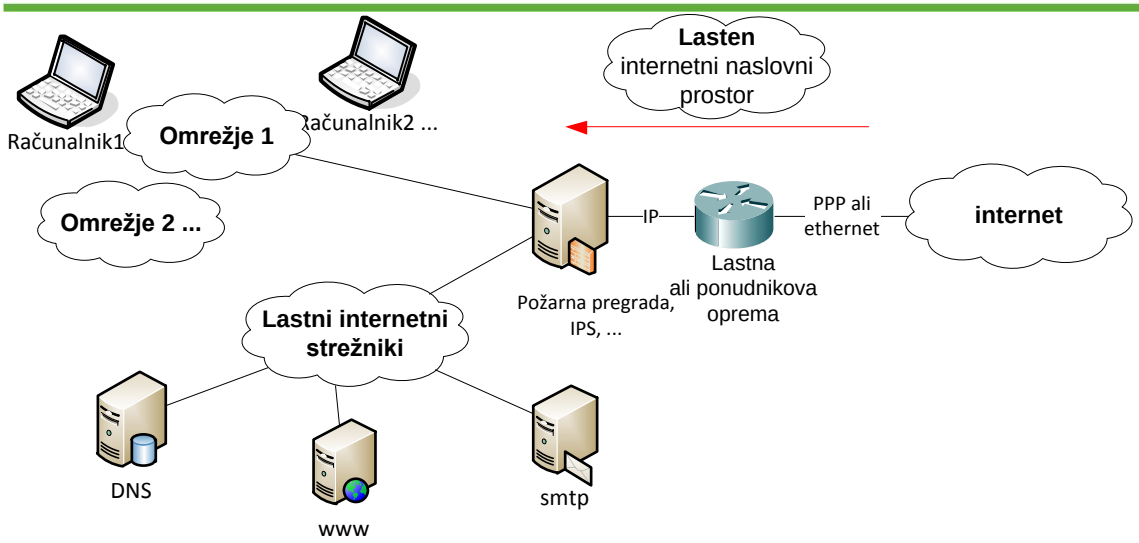
Načrt za izvedbo je na skici »Rešitev 2«.

Dodatne potrebne konfiguracije na strani odjemalca so enake kot pri preprostih scenarijih.

Uporabnik v tem scenariju prepusti internetno povezavo za potrebe naprave eZdravja. Če ta izbira ni sprejemljiva, se uporabi dodatna povezava internetnega ponudnika ali MPLS voda. Uporabi se »Rešitev 3«.

4.3.2 Odjemalec ima lasten internetni naslovni prostor, ki ga želi ohraniti

Groba skica takega omrežja:



Uporabnik ima v svojem omrežju internetne strežnike, na katerih bo morda stregel tudi storitve za hrbtenico eZdravja

Ima lahko eno ali več lokalnih omrežij.

ISP k njemu usmerja mednarodno prepoznaven naslovni prostor, ki ga uporabnik **ne želi ukiniti** ob prehodu v hrbtenico.

Rešitev je mogoča, če je izpolnjeno **vsaj eno** od naslednjega:

- subjekt pridobi še eno neodvisno povezavo v internet ali drugačno dogovorjeno omrežje (tipično MPLS predpisanega ponudnika); ali
- subjekt lahko izolira eno lastno javno IPv4 številko, ki jo za povezavo uporabi naprava eZdravja.

Uporabnik mora zadostiti tudi drugim zahtevam, ki jih postavlja hrbtenica eZdravja (glej ustrezno dokumentacijo).

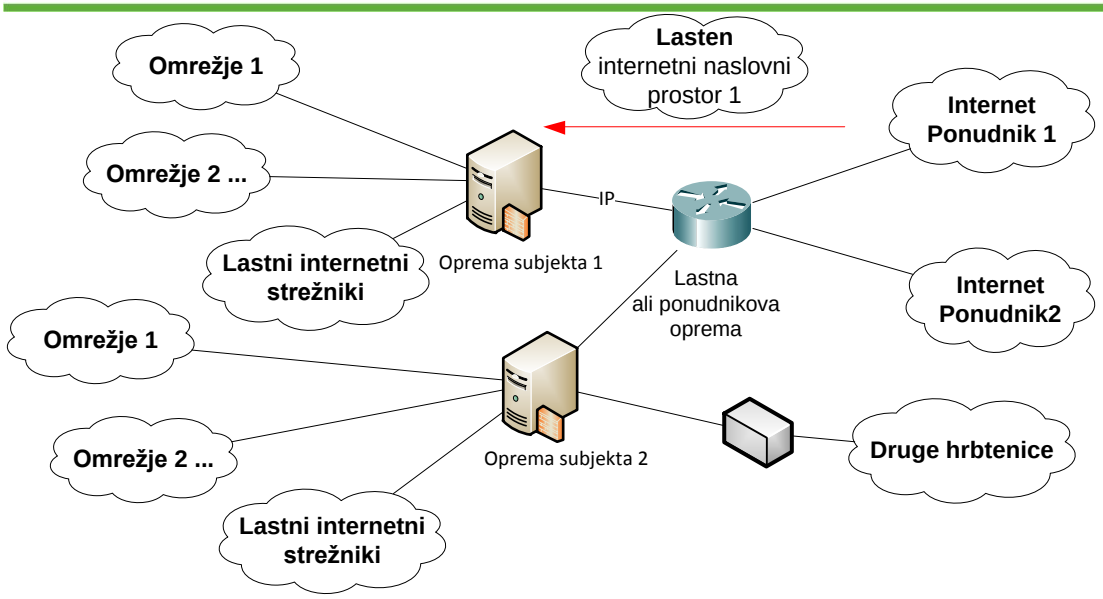
V primeru, da nadaljuje z uporabo lastnega DNS strežnika, ga mora pravilno konfigurirati (glej ustrezno shemo).

V primeru, da nadaljuje z uporabo lastnega poštnega strežnika, ga mora pravilno konfigurirati (glej ustrezno shemo).

Načrt za izvedbo je na skici »Rešitev 3«.

4.3.3 Odjemalec želi imeti več različnih omrežij v hrbtenici, želi ponujati storitve in ohraniti javni naslovni prostor, napravo pa uporablja vsaj ena pravna oseba z vsaj enim ISP

Posplošena skica takega omrežja:



V tem primeru je uporabnik omrežja udeleženec v obstoječem kompleksnem sistemu omrežij. Lahko gostuje v večjem sistemu ali je soudeležen pri njegovem upravljanju. Obstajajo storitve, ki bi jih subjekt lahko ponudil omrežju. Tvegano je, da bo ob priklopu okolja eZdravja prišlo do prekrivanja naslovnega prostora (IPv4).

V tem primeru je potrebno v hrbtenico izvesti vsaj dva logično ločena priklopa. Po enega za vsak subjekt, ki bo hrbtenico uporabljal in po enega za vsak sklop storitev, ki jih bo subjekt hrbtenici ponujal. Za priporočene izbire naslovnega prostora glej prilogo.

Načrt za izvedbo je na skici »Rešitev 3«.

4.4 Rešitev zahtevnejših scenarijev

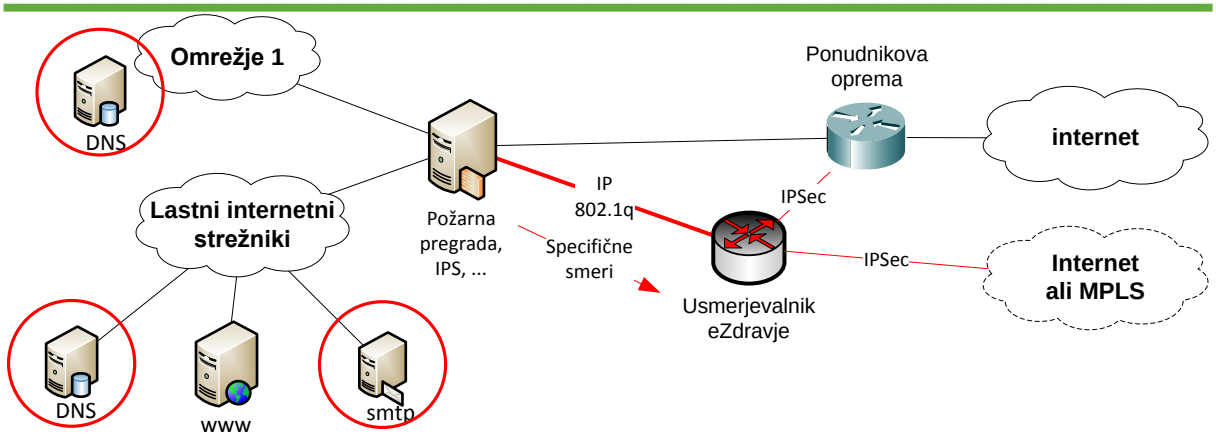
Rešitev omogoča, da subjekt v celoti spremeni dostop do drugih omrežij in interneta tako, da ga vodi prek infrastrukture eZdravje, **ali** pa skozi eZdravje vodi le tisti del prometa, ki ni na voljo drugje.

Za vzpostavitev povezljivosti v okolje eZdravja je potrebno zagotoviti

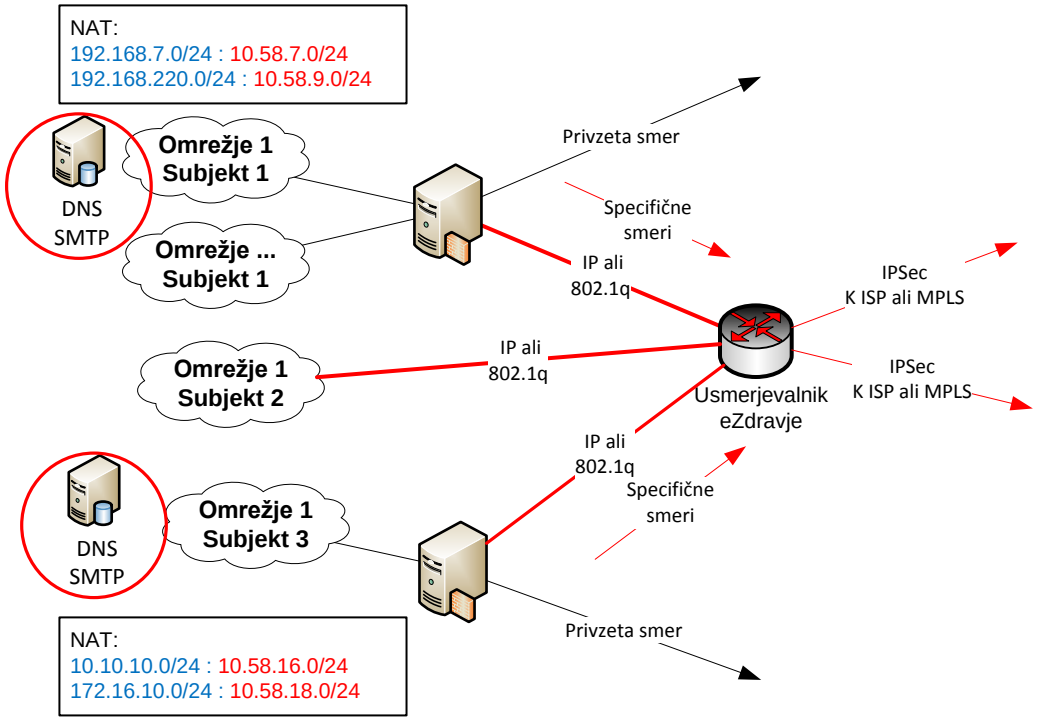
- eno namensko IPv4 številko na vsakem od ponudnikov transporta (internet, MPLS ali drug dogovorjen medij, za katerega ima Ministrstvo sklenjeno ustrezno pogodbo)
- en logični ali fizični vmesnik na strani odjemalcev
- en logični ali fizični vmesnik na strani interneta (lahko tudi v DMZ) ali drugega ponudnika transporta.

V okolji eZdravja je želen izvorni IPv4 naslovni prostor znotraj območja 10.56.0.0/14, kar glede na dogovor ob priklopu zagotovi oprema uporabnika ali oprema eZdravja.

Na slikah so upodobljene le bistvene komponente. Nastavitve odjemalcev so opisane v posebnem poglavju. Prilagoditi je potrebno vsaj še konfiguracijo označenih komponent.



Slika »Rešitev 2«



Slika »Rešitev 3«, kjer je več subjektov z več naslovnimi prostori.

Tipično so v tej rešitvi dodeljeni naslovni prostori oblike 10.56…, 10.57…., 10.58…., 10.59…., in velikosti 256 do 4096 naslovov. To na kratko imenujmo »mreža z masko 20 do 24 iz prostora 10.56.0.0/14«. Tipično so 4 najnižje številke v taki mreži uporabljene za prehod proti okolju eZdravje. V primerih, ko uporabnik okolja posreduje promet lokalnih omrežij prek lastne naprave (usmerjevalnik, požarna pregrada), se med obe napravi vrine *tranzitni segment* iz naslovnega prostora 10.159.0.0/16. Uporabljena maska je običajno 28-bitna.

Za odjemalce je prevajanje IPv4 naslovov mogoče izvesti na opremi uporabnika **ali** na opremi eZdravje.

Kjer je ponujena storitev za večje število subjektov (DMZ), prevajanje IPv4 naslovov ni želeno. Število različnih IPv4 naslovnih prostorov, ki jih je mogoče logično priklopiti na usmerjevalnik eZdravje je dovolj visoko.

Primer:

- Subjekt1 ima hrbtenico 4 oddelkov. Uporabljajo naslovne prostore 10.10.14.0/24, 10.10.18.0/22, 192.168.55.0/24, 192.168.18.0/23.
- Subjekt2 ima hrbtenico 2 oddelkov. Naslovni prostori so 192.168.55.0/24 (prekrivanje!), 10.10.0.0/23.
- Subjekt2 ponuja skupno storitev »storitev-subjekt2.ss.ezdrav.si«.
- Upravitelj omrežja ne želi, da je IPSec vmesnik usmerjevalnika eZdravje neposredno na internetu

Po novem bi lahko konfiguracija izgledala:

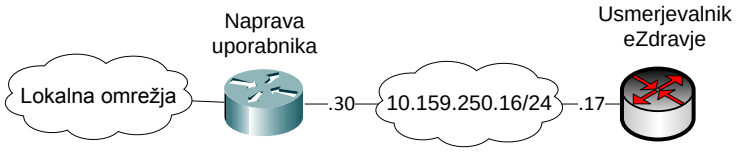
- Subjekt1 se v okolju eZdravje predstavlja z blokom naslovnega prostora 10.58.16.0/20. IPv4 naslove prevaja na svoji opremi. Do okolja eZdravje se promet usmerja prek tranzitnega segmenta 10.159.250.16/28: v eZdravje vodi naslov 10.159.250.17, do subjekta pa 10.159.250.30.
- Subjekt2 se v okolju eZdravje se predstavlja z blokom naslovnega prostora 10.58.32.0/22. Prevajanje zagotavlja usmerjevalnik eZdravje.
- Subjekt2 ponuja skupno storitev »storitev-subjekt2.ss.ezdrav.si« na naslovnem prostoru 172.29.253.211, ki se zaključuje na ločenem VLAN in na ločenem fizičnem vmesniku usmerjevalnika eZdravje.
- Upravitelj omrežja zagotovi javno IPv4 številko v internetnem DMZ. Na svoji požarni pregradi lahko omejuje promet na obeh straneh usmerjevalnika eZdravje

Ne glede na število subjektov in priklopljenih lokalnih omrežij usmerjevalnik eZdravja omogoča popolno logično ločitev vseh naslovnih prostorov, ki so do usmerjevalnika pripeljani po različnih VLAN.

4.5 Konfiguracija infrastrukture subjekta

4.5.1 Usmerjanje

Če subjekt ni konfiguriral omrežja na način »Rešitev 1« in torej prek okolja eZdravje vodi le izbran del izhodnega prometa, mora prilagoditi usmerjevalne tabele na napravi, ki je sosednja k usmerjevalniku eZdravje, ter na drugih ustreznih napravah.



Minimalni poseg, ki omogoča ustrezno rabo okolja eZdravje, je usmeritev naslovnih prostorov 172.24.128.0/17 in 172.29.0.0/16 proti usmerjevalniku eZdravje.

Konfiguracija na napravah na podlagi Unix ali Linux operacijskih sistemov:

```
$ ip route add 172.24.0.0/16 via 10.159.250.17
$ ip route add 172.29.0.0/16 via 10.159.250.17
```

Konfiguracija za Cisco IOS, GateD in sorodne:

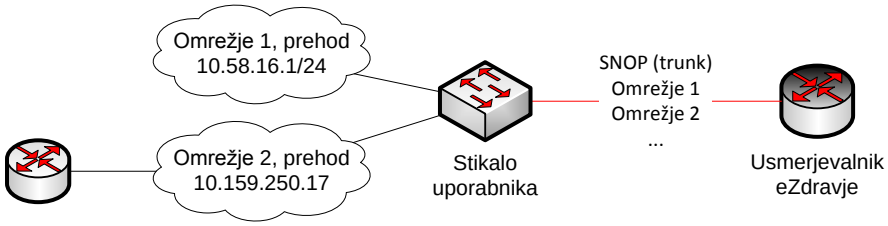
```
host(config)# ip route 172.24.0.0 255.255.0.0 10.159.250.17
host(config)# ip route 172.29.0.0 255.255.0.0 10.159.250.17
```

4.5.2 Stikanje

Zaradi usmerjevalnika eZdravja **ni potrebno spreminjati** stikal ali VLAN nastavitev pri uporabniku. Če ni drugače določeno, so fizična vrata na usmerjevalniku nastavljena v dostopovni način z lastno IPv4 številko, to je, privzetim prehodom v okolje eZdravje.

Če nastane potreba, da je skozi fizični vmesnik potrebno pripeljati več ločenih mrež (delitev fizičnega vodnika z drugim subjektom ali dostopom do ISP), si okolje eZdravje pridržuje pravico zahtevati ustrezno razporeditev VLAN znotraj snopa (trunk).

Scenarij:



Podprti način snopa je 802.1q.

Priklop odjemalcev in DMZ ima številko VLAN med 800 in 830.
Priklop ISP ima VLAN številko med 900 in 930.
Priklop VoIP ima VLAN številko med 100 in 130.

Konfiguracija na napravah na podlagi Unix ali Linux operacijskih sistemov:

```
$ ifconfig eth1 up # trunk do eZdravje
$ ifconfig eth1.801 10.58.16.3 netmask 255.255.255.0 up # lokalna mreža 1
$ ifconfig eth1.802 10.159.250.30 netmask 255.255.255.0 up # mreža 2
```

Konfiguracija za Cisco IOS in sorodne (VLAN):

```
host(config)# interface GigabitEthernet X
host(config-if)# description povezava do eZdravje
host(config-if)# switchport trunk encapsulation dot1q
host(config-if)# switchport trunk allowed vlan 801
host(config-if)# switchport trunk allowed vlan add 802
host(config-if)# switchport mode trunk
```

4.5.3 Filtriranje prometa in privzeta politika

Okolje eZdravje na centralni opremi poskrbi, da proti omrežjem uporabnika ne usmerja škodljivega prometa. Dopušča možnost, da je proti lokalnemu omrežju sprožen promet

- iz naslovnih prostorov drugih subjektov v okolju eZdravje, če je bila taka povezljivost naročena
- iz naslovnega prostora 172.29.192.0/19 (centralne storitve)

- iz naslovnega prostora 172.29.128.0/19 (storitve RDC)
- iz naslovnega prostora oddaljenih uporabnikov, ki vstopajo skozi testno okolje **in** je bil tak dostop naročen (trenutno 172.24.0.0/18).

Subjekt **lahko** promet dodatno filtrira na lastnih napravah in / ali v **razumnem obsegu in za razumno obdobje** zahteva poročilo o izvedenih dostopih do njegovega omrežja.

Storitve, ki jih subjekt objavi v intranetnem DMZ (172.29.x.y), so privzeto vsem subjektom v hrbtenici dosegljivi prek https/443. Dodatne zaostritve izvaja subjekt. Preostali dostopi so mogoči le, če so naročeni.

4.5.4 Dodeljevanje in prevajanje IPv4 naslovov vira

Vse vrednosti za IPv4 naslovni prostor, ki jih predpisuje okolje eZdravje, izvirajo iz tehničnih omejitev. Ob vstopu v okolje se tehnični kontakti na strani uporabnika in ponudnika dogovorijo o obsegu, količini in vrsti naslovnih prostorov. Če je potrebno prevajanje, se dogovorijo o točki, ki naslove prevaja.

Okolje eZdravje zahteva sledljivost uporabe omrežnega naslova v obsegu, ki ga zahtevajo splošni predpisi. To pomeni, da je v primeru sproženega preiskovalnega postopka zahtevano poročilo o lastništvu omrežnega naslova vsaj 6 mesecev od trenutka uporabe.

4.5.5 Prevajanje IPv4 naslovov cilja

Izrecno odsvetujemo, da skrbnik infrastrukture na uporabniški strani prevaja IPv4 naslove cilja v okolju eZdravja. S tem onemogoči delovanje DNS infrastrukture in uvaja druge težko premostljive težave v omrežje.

V primeru, da je izjemno zahtevno ali nemogoče v večjih omrežjih zagotoviti usmerjanje naslovnih prostorov 172.24.0.0/16 in 172.29.0.0/16 proti okolju eZdravje, bo na podlagi odobritve Ministrstva ponujen nov naslovni prostor 172.18.0.0/16 in ustrezen DNS strežnik, ki bo preslikoval vse naslove.

4.5.6 Razreševanje DNS

Za delovanje odjemalcev trenutno zadostuje, da lokalni DNS strežniki razrešujejo imena na običajen način, za uporabo storitev v testnem okolju eZdravje pa je potrebno nekatere domene razreševati na **namenskih** DNS strežnikih.

4.5.6.1 Ves promet skozi eZdravje

Če odjemalec ves promet vodi skozi okolje eZdravje, je delovanje zagotovljeno z DNS strežniki, ki jih pridobi skozi DHCP na usmerjevalniku eZdravje.

Če so DNS strežniki nastavljeni ročno, morajo biti vpisani 172.29.192.8, 172.29.192.16, 172.29.64.8 (ne nujno vsi).

4.5.6.2 Del prometa skozi eZdravje

Upravitelj lokalnega DNS mora poskrbeti, da se vsaj naslednja področja (domene) razrešujejo na specifičnih DNS strežnikih 172.29.192.8, 172.29.192.16, 172.29.64.8:

- ezdrav.si
- znet.si
- sigov.si

Če je odjemalec tudi administrator katerega od strežnikov v okolju eZdravje, poskrbi še za

- ezdrav
- znet

Primer konfiguracije za programsko opremo »ISC bind« (named.conf)

```
…
zone "ezdrav.si" IN {
      type forward;
            forwarders { 172.29.192.8; 172.29.192.16; 172.29.64.8; };
};
zone "sigov.si" IN {
      type forward;
      forwarders { 172.29.192.8; 172.29.192.16; 172.29.64.8;  };
};
zone "znet.si" IN {
      type forward;
      forwarders { 172.29.192.8; 172.29.192.16; 172.29.64.8;  };
};
…
```

Upravitelj DNS procesa na Microsoft programski opremi konfigurira »Conditional forward« funkcionalnost na DNS procesu z enakimi nastavitvami.

4.5.6.3 Lastni imenski prostori (DNS cone)

Subjekt, ki želi sam skrbeti za objavo imen lastnih storitev, zanje uvede imenski prostor, **dogovorjen** z Ministrstvom. Tipično je ta znotraj »ss.ezdrav.si« ali »ss.znet.si«. S skrbnikom okolja se dogovori za točko upravljanja cone (uporabnikov DNS) in pravice prenosa cone. Podatke do preklica prenaša primarni DNS strežnik z naslovom 172.29.192.8.

4.5.7 Spletni zastopnik (proxy)

4.5.7.1 Zastopnika ni

4.5.8 Potrebne niso nobene spremembe. Vsi uporabniki spletnih storitev iz okolja eZdravje morajo imeti zagotovljen omrežni dostop do DNS strežnika iz točke »Filtriranje prometa in privzeta politika

Okolje eZdravje na centralni opremi poskrbi, da proti omrežjem uporabnika ne usmerja škodljivega prometa. Dopušča možnost, da je proti lokalnemu omrežju sprožen promet

- iz naslovnih prostorov drugih subjektov v okolju eZdravje, če je bila taka povezljivost naročena
- iz naslovnega prostora 172.29.192.0/19 (centralne storitve)
- iz naslovnega prostora 172.29.128.0/19 (storitve RDC)
- iz naslovnega prostora oddaljenih uporabnikov, ki vstopajo skozi testno okolje **in** je bil tak dostop naročen (trenutno 172.24.0.0/18).

Subjekt **lahko** promet dodatno filtrira na lastnih napravah in / ali v **razumnem obsegu in za razumno obdobje** zahteva poročilo o izvedenih dostopih do njegovega omrežja.

Storitve, ki jih subjekt objavi v intranetnem DMZ (172.29.x.y), so privzeto vsem subjektom v hrbtenici dosegljivi prek https/443. Dodatne zaostritve izvaja subjekt. Preostali dostopi so mogoči le, če so naročeni.

4.5.9 Dodeljevanje in prevajanje IPv4 naslovov vira

Vse vrednosti za IPv4 naslovni prostor, ki jih predpisuje okolje eZdravje, izvirajo iz tehničnih omejitev. Ob vstopu v okolje se tehnični kontakti na strani uporabnika in ponudnika dogovorijo o obsegu, količini in vrsti naslovnih prostorov. Če je potrebno prevajanje, se dogovorijo o točki, ki naslove prevaja.

Okolje eZdravje zahteva sledljivost uporabe omrežnega naslova v obsegu, ki ga zahtevajo splošni predpisi. To pomeni, da je v primeru sproženega preiskovalnega postopka zahtevano poročilo o lastništvu omrežnega naslova vsaj 6 mesecev od trenutka uporabe.

4.5.10 Prevajanje IPv4 naslovov cilja

Izrecno odsvetujemo, da skrbnik infrastrukture na uporabniški strani prevaja IPv4 naslove cilja v okolju eZdravja. S tem onemogoči delovanje DNS infrastrukture in uvaja druge težko premostljive težave v omrežje.

V primeru, da je izjemno zahtevno ali nemogoče v večjih omrežjih zagotoviti usmerjanje naslovnih prostorov 172.24.0.0/16 in 172.29.0.0/16 proti okolju eZdravje, bo na podlagi odobritve Ministrstva ponujen nov naslovni prostor 172.18.0.0/16 in ustrezen DNS strežnik, ki bo preslikoval vse naslove.

Razreševanje DNS« in omrežni dostop do okolja eZdravje.

Če subjekt **ves promet** vodi skozi okolje eZdravje, s tako konfiguracijo **nima dostopa do interneta**.

4.5.10.1 Lasten zastopnik

Če subjekt uporablja lasten zastopniški strežnik za dostop do interneta, mora poskrbeti za eno od naslednjega:

4.5.11 spletni zastopnik uporablja DNS, konfiguriran na način, opisan v razdelku »Filtriranje prometa in privzeta politika

Okolje eZdravje na centralni opremi poskrbi, da proti omrežjem uporabnika ne usmerja škodljivega prometa. Dopušča možnost, da je proti lokalnemu omrežju sprožen promet

- iz naslovnih prostorov drugih subjektov v okolju eZdravje, če je bila taka povezljivost naročena
- iz naslovnega prostora 172.29.192.0/19 (centralne storitve)
- iz naslovnega prostora 172.29.128.0/19 (storitve RDC)
- iz naslovnega prostora oddaljenih uporabnikov, ki vstopajo skozi testno okolje **in** je bil tak dostop naročen (trenutno 172.24.0.0/18).

Subjekt **lahko** promet dodatno filtrira na lastnih napravah in / ali v **razumnem obsegu in za razumno obdobje** zahteva poročilo o izvedenih dostopih do njegovega omrežja.

Storitve, ki jih subjekt objavi v intranetnem DMZ (172.29.x.y), so privzeto vsem subjektom v hrbtenici dosegljivi prek https/443. Dodatne zaostritve izvaja subjekt. Preostali dostopi so mogoči le, če so naročeni.

4.5.12 Dodeljevanje in prevajanje IPv4 naslovov vira

Vse vrednosti za IPv4 naslovni prostor, ki jih predpisuje okolje eZdravje, izvirajo iz tehničnih omejitev. Ob vstopu v okolje se tehnični kontakti na strani uporabnika in ponudnika dogovorijo o obsegu, količini in vrsti naslovnih prostorov. Če je potrebno prevajanje, se dogovorijo o točki, ki naslove prevaja.

Okolje eZdravje zahteva sledljivost uporabe omrežnega naslova v obsegu, ki ga zahtevajo splošni predpisi. To pomeni, da je v primeru sproženega preiskovalnega postopka zahtevano poročilo o lastništvu omrežnega naslova vsaj 6 mesecev od trenutka uporabe.

4.5.13 Prevajanje IPv4 naslovov cilja

Izrecno odsvetujemo, da skrbnik infrastrukture na uporabniški strani prevaja IPv4 naslove cilja v okolju eZdravja. S tem onemogoči delovanje DNS infrastrukture in uvaja druge težko premostljive težave v omrežje.

V primeru, da je izjemno zahtevno ali nemogoče v večjih omrežjih zagotoviti usmerjanje naslovnih prostorov 172.24.0.0/16 in 172.29.0.0/16 proti okolju eZdravje, bo na podlagi odobritve Ministrstva ponujen nov naslovni prostor 172.18.0.0/16 in ustrezen DNS strežnik, ki bo preslikoval vse naslove.

- Razreševanje DNS« **in** spletni zastopnik mora biti v delu omrežja, ki ima dostop do okolja eZdravje
- uporabniki se izogibajo spletnemu zastopniku za zgoraj navedene domene **in** uporabniki imajo dostop do okolja eZdravje

4.5.13.1 Uporaba zastopnika v okolju eZdravje

Subjekt se lahko odloči, da uporablja internetni spletni zastopnik v okolju eZdravje.

Konfiguracija se ročno ali z ustreznimi administratorskimi orodji (group policy, ZENworks, …) izvede na odjemalcu (glej spodaj).

Zaradi varnosti in arhitekture je dostop do **notranjih** delov omrežja prek internetnega zastopnika striktno **onemogočen**.

4.5.14 Elektronska pošta

4.5.14.1 Ves promet skozi eZdravje

Trenutno je podprt scenarij, kjer ima subjekt poštni strežnik s SMTP dostavo pošte in je ta umeščen v omrežju subjekta. **Konfiguracija se do nadaljnjega rešuje individualno**.

Če subjekt uporablja elektronsko pošto internetnega ponudnika, ni potrebna nobena sprememba. Pri POP, IMAP in SMTP dostopu v tem primeru **ponudnik elektronske pošte lahko postavi dodatne omejitve**.

4.5.14.2 Del prometa skozi eZdravje

Spremembe trenutno niso potrebne. Primerno je, da ima poštni strežnik dostop do DNS strežnika, ki pozna okolje eZdravje.

4.6 Konfiguracija odjemalcev

Okolje je zastavljeno tako, da poleg zgoraj navedenih posegov na infrastrukturi ni potrebno dodatno konfigurirati odjemalcev.

4.6.1 Varnostna politika

Dokument se ne ukvarja z varnostno politiko odjemalcev ali omrežja. Ministrstvo je za te namene izdalo druge dokumente in vprašalnike o skladnosti.

4.6.2 Podprti in dovoljeni operacijski sistemi

Priklop odjemalca v okolje eZdravje **ni pogojen** z vrsto operacijskega sistema. Odjemalec mora biti sposoben IPv4 povezljivosti, za dostop do vstopne točke v okolje (usmerjevalnik eZdravje) poskrbi skrbnik lokalnega omrežja. **Lahko obstajajo omejitve**, ki jih glede operacijskega sistema ali nameščene programske opreme postavljajo **uporabljene aplikacije**. **Dodatne omejitve** lahko postavlja varnostna politika.

4.6.3 Razreševanje DNS

4.6.4 Če pri subjektu za DNS razreševanje ni poskrbljeno na infrastrukturni ravni, se smiselno upoštevajo navodila iz razdelka »Filtriranje prometa in privzeta politika

Okolje eZdravje na centralni opremi poskrbi, da proti omrežjem uporabnika ne usmerja škodljivega prometa. Dopušča možnost, da je proti lokalnemu omrežju sprožen promet

- iz naslovnih prostorov drugih subjektov v okolju eZdravje, če je bila taka povezljivost naročena
- iz naslovnega prostora 172.29.192.0/19 (centralne storitve)
- iz naslovnega prostora 172.29.128.0/19 (storitve RDC)
- iz naslovnega prostora oddaljenih uporabnikov, ki vstopajo skozi testno okolje **in** je bil tak dostop naročen (trenutno 172.24.0.0/18).

Subjekt **lahko** promet dodatno filtrira na lastnih napravah in / ali v **razumnem obsegu in za razumno obdobje** zahteva poročilo o izvedenih dostopih do njegovega omrežja.

Storitve, ki jih subjekt objavi v intranetnem DMZ (172.29.x.y), so privzeto vsem subjektom v hrbtenici dosegljivi prek https/443. Dodatne zaostritve izvaja subjekt. Preostali dostopi so mogoči le, če so naročeni.

4.6.5 Dodeljevanje in prevajanje IPv4 naslovov vira

Vse vrednosti za IPv4 naslovni prostor, ki jih predpisuje okolje eZdravje, izvirajo iz tehničnih omejitev. Ob vstopu v okolje se tehnični kontakti na strani uporabnika in ponudnika dogovorijo o obsegu, količini in vrsti naslovnih prostorov. Če je potrebno prevajanje, se dogovorijo o točki, ki naslove prevaja.

Okolje eZdravje zahteva sledljivost uporabe omrežnega naslova v obsegu, ki ga zahtevajo splošni predpisi. To pomeni, da je v primeru sproženega preiskovalnega postopka zahtevano poročilo o lastništvu omrežnega naslova vsaj 6 mesecev od trenutka uporabe.

4.6.6 Prevajanje IPv4 naslovov cilja

Izrecno odsvetujemo, da skrbnik infrastrukture na uporabniški strani prevaja IPv4 naslove cilja v okolju eZdravja. S tem onemogoči delovanje DNS infrastrukture in uvaja druge težko premostljive težave v omrežje.

V primeru, da je izjemno zahtevno ali nemogoče v večjih omrežjih zagotoviti usmerjanje naslovnih prostorov 172.24.0.0/16 in 172.29.0.0/16 proti okolju eZdravje, bo na podlagi odobritve Ministrstva ponujen nov naslovni prostor 172.18.0.0/16 in ustrezen DNS strežnik, ki bo preslikoval vse naslove.

Razreševanje DNS« predhodnega poglavja. Izrecno odsvetujemo uporabo »goljufanja s *hosts* datoteko«.

Odjemalec vpiše med DNS strežnike še 172.29.192.8, 172.29.192.16, 172.29.64.8 .

4.6.7 Spletni zastopnik (proxy)

Če se odjemalec **odloči** uporabljati spletni zastopnik okolja eZdravje in za to ni poskrbljeno na infrastrukturi, ga lahko konfigurira individualno (ročno ali s skrbniškimi orodji).

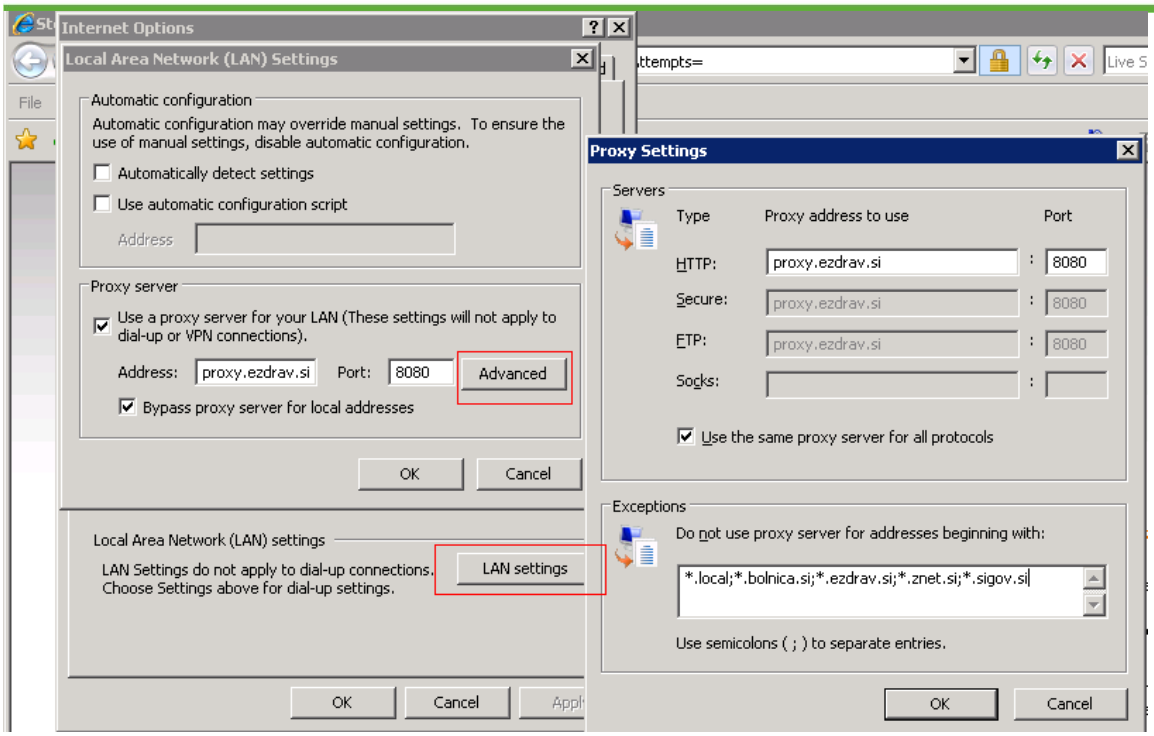
4.6.7.1 Ročna nastavitev

Naslov strežnika je »proxy.znet.si« ali »proxy.ezdrav.si«, uporablja vrata 8080.

Med izjeme za uporabo zastopnika je potrebno vnesti vse imenske prostore, ki jih uporabnik želi dosegati lokalno ali v okolju eZdravje. Tipično so to vsi lokalni naslovi pri uporabniku in naslovi intranetnih aplikacij:

- *.local
- *imeustanove*.si
- *.ezdrav.si
- *.znet.si
- *.sigov.si

Posnetek prikazuje nastavitev zastopniškega strežnika pri brskalniku Internet Explorer (Tools / internet options oziroma Orodja / Internetne možnosti).

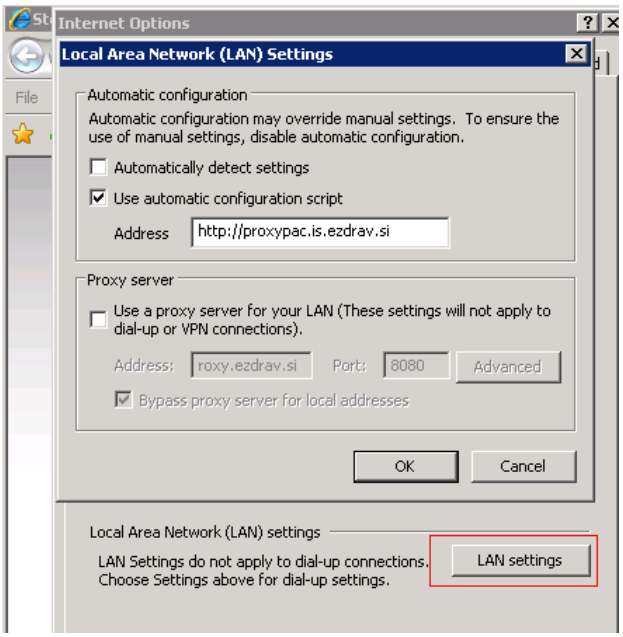


4.6.7.2 Samokonfiguracija z uporabo »proxypac« datoteke

Na omrežju je na voljo storitev »proxypac.is.znet.si« ali »proxypac.is.ezdrav.si«,

Z uporabo te storitve se izognemo tipkarskim napakam v konfiguraciji izjem, hkrati lahko precej razširimo fleksibilnost konfiguracije.

Konfiguracija *Tools / Internet options* za ta primer:



Konfiguracija na ta način omogoča vsakemu subjektu drugačno konfiguracijo oziroma politiko. Spremembe se izvajajo po naročilu.

4.6.7.3 Samokonfiguracija z uporabo »WPAD« zapisa

V domenah ezdrav.si in znet.si sa na voljo WPAD (Web Proxy Auto Discovery) zapisa. Protokol je namenjen predvsem odjemalcem, ki se pogosto selijo med različnimi omrežji.