Operativni program
KONKURENTNOST
I KOHEZIJA

EUROPSKI STRUKTURNI
I INVESTICIJSKI FONDOVI

Projekt je sufinancirala Europska unija iz Europskog fonda za regionalni razvoj.
Sadržaj dokumenta isključiva je odgovornost Ministarstva uprave.

Referentna arhitektura servisa u IaaS modelu

Javno
V 2.3

Vlasnik dokumenta:	CDU
Autor:	Mr.Sc. Mladen Goršeta, dipl.ing. elektrotehnike
Oznaka dokumenta:	CDU-RA
Verzija:	2.2
Datum kreiranja:	

1 Obilježje dokumenta

1.1 Povijest dokumenta

Datum revizije	**Verzija**	**Razlog promjene**	**Vlasnik promjene**
8.7.2019.	1.0	Inicijalni dokument	Mladen Goršeta
3.12.2019.	2.0	Ažurirano	Mladen Goršeta
3.3.2020.	2.2	Ažurirano	Mladen Goršeta

1.2 Povezani dokumenti

Ovaj dokument je povezan s dokumentima:

Oznaka dokumenta	**verzija**
Podržani sustavi	1.1
LLD template	

1.3 Odobrenja

Ovaj dokument mora odobriti:

Ime	**Potpis**	**Titula**	**Datum**	**Verzija**

1.4 Distribucija

Dokument može na uvid svim potencijalnim i trenutnim korisnicima CDU platforme.

Contents:

2 Uvod

2.1 Obuhvat dokumenta

IT infrastrukturni standard se primjenjuje na sve sustave hostane na CDU platformi.

2.2 Cilj dokumenta

Cilj ovog dokumenta je definiranje referentne arhitekture informatičkih servisa na CDU infrastrukturi u IaaS modelu. Standard definiran u ovom dokumentu se koristi kao referentni dizajn prilikom izrade arhitekture servisa koji će biti udomljen na CDU platformi u IaaS modelu.

2.3 Vlasništvo dokumenta

Vlasništvo ovog dokumenta je CDU.

3 Management summary

CDU kao pružatelj usluga ovisi o pouzdanim IT operacijama i pripadajućoj infrastrukturi kako bi podržao temeljne poslovne procese korisnika:

-pružanje usluga
-osiguranje usluge

Stoga je potrebna odgovarajuća IT infrastrukturna arhitektura i standardi kako bi se omogućili postupci koji su visoko dostupni i geo redundantni sposobni za rad u načinu 24 x 7 x 365. Osim dostupnosti, ona također mora biti prilagodljiva budućim rješenjima i procesima koji nude najviše standarde izvedbe, kvalitete i pouzdanosti.

Ovaj dokument opisuje referentnu arhitekturu servisa udomljenog u IaaS modelu.

Implementacija servisa prema referentom dizajnu doprinosi:

- učinkovitom upravljanju i boljem planiranju
- učinkovitosti i kvaliteti usluge
- smanjenju rizika za pružanje IT usluga
- smanjenju ukupnih troškova vlasništva nad IT infrastrukturom što u konačnici doprinosi smanjenju cijene usluge za krajnjeg korisnika,
- povećanju sigurnosti udomljenih sustava.

Osim toga, dodatne pogodnosti proizlaze iz optimizacije IT resursa i koncentraciji stručnosti upravljačkog osoblja koja je dostupna svim korisnicima CDU usluga.

4 Načela koja se koriste za definiranje referentne arhitekture aplikacije

IT sustavi se implementiraju kao troslojne ili dvoslojne aplikacije. Troslojne aplikacije se sastoje od sloja web poslužitelja, sloja aplikacijskih poslužitelja i sloja baza podataka. Kod dvoslojne aplikacije web i aplikacijski sloj čine jedinstveni sloj dok su baze podataka odvojene u zasebni sloj. U ovom dokumentu je prikazan referentni dizajn za dvoslojne i troslojne aplikacije. Dizajn aplikacije ovisi o ciljanoj raspoloživosti usluge, količini konkurentnih sesija i transakcija u jedinci vremena te o procjeni veličine baze podataka.

4.1 Raspoloživost servisa

CDU platforma je visoko dostupna i visoko skalabilna cloud platforma koja je rastegnuta preko dvije fizičke lokacije što osigurava visoku dostupnost servisa i ugrađenu DR funkcionalnost. Infrastruktura bazirana na cloud computingu osigurava visoku dostupnost na nivou virtualnih poslužitelja (VM). Svaki VM je zaštićen od ispada bilo koje komponente unutar podatkovnog centra i ispada cjelokupnog podatkovnog centra. Aplikacija se ne mora brinuti za DR funkcionalnost jer je ista ugrađena u dizajn platforme. Tablica ispod prikazuje ciljanu raspoloživost ovisno o dizajnu servisa:

Ciljana raspoloživost	Broj VM-ova za Web/App sloj	Broj VM-ova za DB sloj	Potreban Load balancer za servis	Ugrađena DR funkcionalnost
99% (3,65 dana kumulativna nedostupnost servisa)	1	1	NE (u slučaju ako nije javno dostupan servis)	DA
99,9% (8,77 sati kumulativna nedostupnost)	2	1	DA	DA
99,99%(62,60 minuta kumulativna nedostupnost)	2	2 (replikacija na nivou baze)	DA	DA

Osnovna garantirana dostupnost servisa instaliranog na jednom VM-u za Web/App sloj i jednom VM-u za DB sloj je na nivou 99% (3,65 dana nedostupnosti godišnje).

4.2 Mrežna dostupnost servisa

Svaki servis udomljen na CDU infrastrukturi može biti dostupan putem minimalno jednog ili više tipova mrežnog pristupa:

- Javna Internet mreža- Servis ima javnu IP adresu i dostupan je s javne mreže bez ograničenja ili s ograničenjem na nivou IP adrese korisnika servisa. Moguće je ograničiti pistup servisu na nivou teritorije (npr. samo javne adrese iz Republije Hrvatske mogu pristupiti servisu)
- Privatne mreže Hitronet,
- Privatne mreže operatera- u ovom slučaju korisnik plaća link i pristupnu točku na strani CDU platforme
- Putem kriptiranog tunela kroz javnu Internet mrežu (IP Sec site to site). U tom slučaju korisnik mora osigurati uređaj na svojoj strani za termininranje kriptiranog tunela. CDU platforma osigurava na svojoj strani termininranje tunela,
- Putem klijentskog kriptiranog pristupa putem javne Internet mreže. Korisnik na svom uređaju mora instalirati Palo Alto networks klijenta za pristup putem SSL tunela.

Svi mrežni pristupi su visoko dostupni i DR zaštićeni.
Korisnik sam odlučuje putem koje mreže će oglasiti svoj servis te svaki servis može biti oglašen putem više pristupnih mreža.

5 Referentna arhitektura CDU IaaS usluge

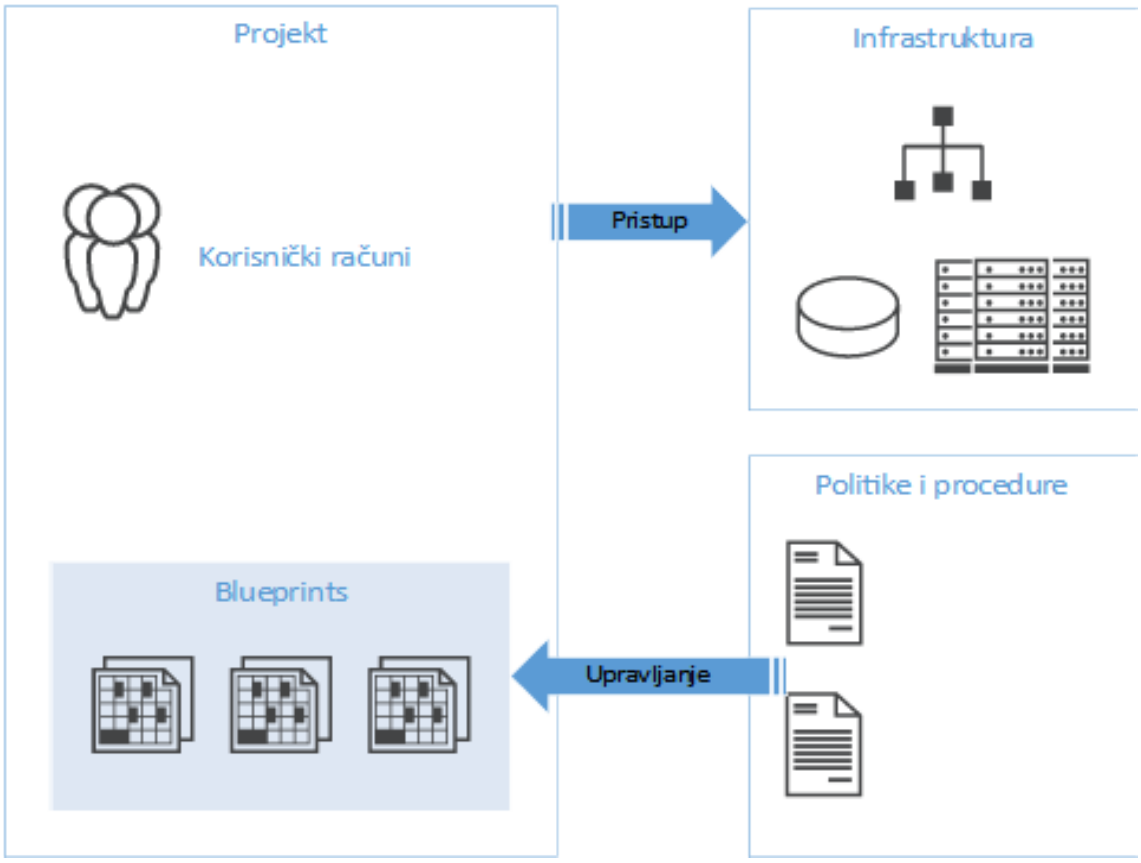
5.1 Projekti

IaaS usluga je organizirana u projekte koji predstavljaju sigurnosne i resursne kontejnere.
Projekt ima slijedeće karakteristike:

- Pravo pristupa korisničkih računa za administraciju projekta,
- Dodijeljene resurse na Infrastrukturi,
- Katalog servisa koje može koristiti,
- Mrežni segmenti s predefinirani sigurnosnim pravilima.

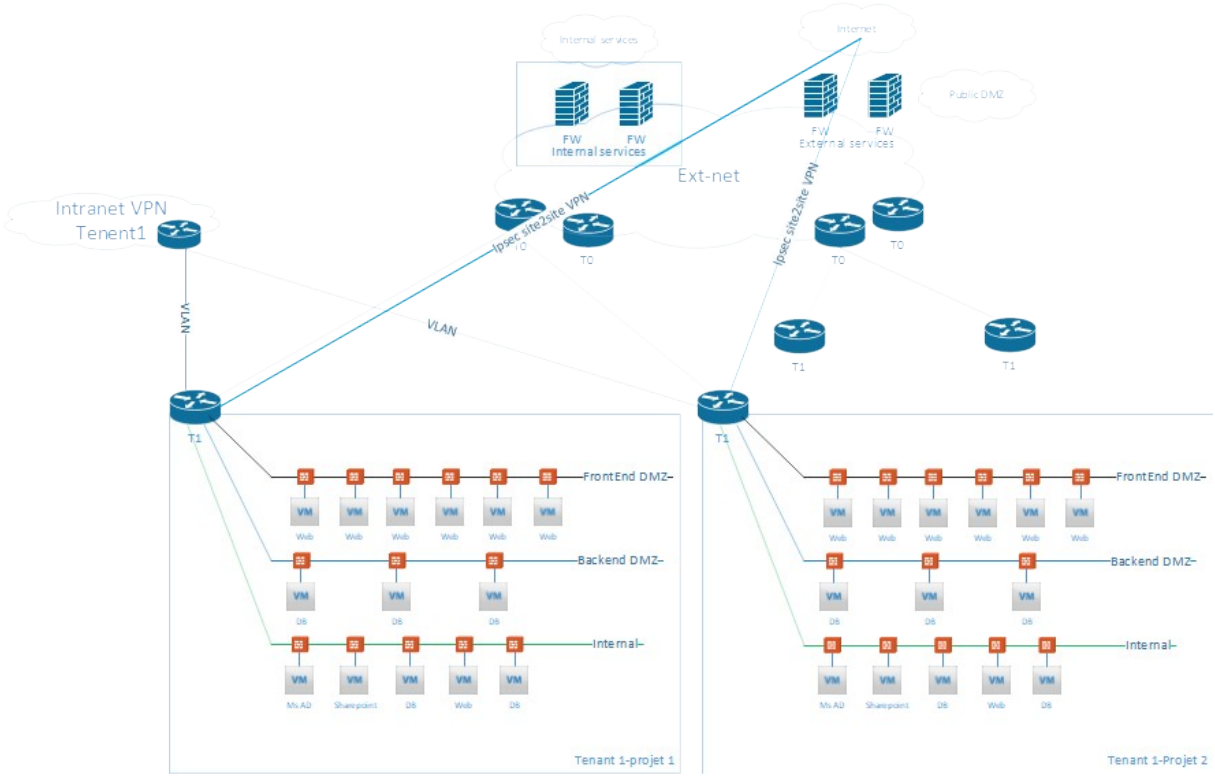
Svaki korisnik IaaS usluge može imati jedan ili više projekata. Projekt je sigurnosna zona na koju imaju pristup određeni korisnički računi i prijedlog je da se za jedan projekt odredi jedan cjelokupan servis. Na primjer jedan registar je jedan projekt i slično.

Shematski prikaz projekta se nalazi na slici ispod.



5.2 Mrežna arhitektura

Mrežna arhitektura je vezana uz organizaciju projekata. Svaki projekt predstavlja posebni virtualni podatkovni centar s jednim dediciranim virtualnim mrežnim usmjeriteljem (virtualni router). Projekti su međusobno mrežno izolirani što osigurava visok nivo sigurnosti cjelokupne CDU platforme. Servisi udomljeni u različite projekte međusobno mogu komunicirati isključivo putem regularnog načina komunikacije: Internet/Hitronet/GSB.
Slika Ispod prikazuje arhitekturu mreže IaaS usluge ovisno o projektima.



6 Gradivni blokovi za servise

Gradnja servisa se vrši putem gradivnih blokova iz servisnog kataloga.

6.1 Virtualni poslužitelj

Virtualni poslužitelj je osnovni gradini blok koji je definiran slijedećim parametrima:

- Broj virtualnih jezgri
- Količina RAM-a u GB
- VSAN disk veličine 100 GB namijenjen smještanju operacijskog sustava i aplikacije

VM na sebi ima preinstaliran operacijski sustav u skladu s CDU infrastrukturnim standardom.

6.1.1 Virtualni diskovi

Virtualni diskovi se dodaju virtualnom poslužitelju kao dodatni diskovni prostor ovisno o potrebama aplikacija. Tablica ispod definira tri osnovna dostupna virtualna diska s garantiranim performansama i primjerima namjene.

Tier diska	Minimalni gradivni blok	Garantirane performanse na minimalnom bloku	DR funkcionalnost	Primjer namjene
Tier 1	100 GB	500 IOPS (25 MBps)	DA (sinkrona replikacija)	Baze podataka visokih performansi preko 100.000 transakcija u sekundi
Tier 2	100 GB	150 IOPS	DA (sinnkrona replikacija)	Baze podataka svih vrsta i aplikacijski serveri svih vrsta
Tier 3	100 GB	N/A	DA (asinkrona replikacija)	Arhive/skladišta podataka/dijeljeni diskovi …

Objektni diskovni prostor

CDU platforma omogućuje korištenje objektnog diskovnog polja za pohranu nestrukturiranih podataka prema slijedećim protokolima:

- S3 protokol,
- HDFS,
- CAS

Objektno diskovno polje osigurava DR funkcionalnost kroz asinkronu replikaciju podataka na pričuvnu lokaciju. Namjena objektnog diskovnog sustava je izgradnja aplikacija nove generacije za upravljanje dokumentima/slikama/video sadržajima i arhiviranje podataka.

6.1.2 Mrežni diskovi

6.1.2.1 NFS mrežni disk

Virtualni poslužitelji mogu imati pristup dijeljenom mrežnim diskovima putem NFS protokola. Dijeljeni diskovni prostori se dodjeljuju na zahtjev s centralnog diskovnog polja baziranog na Tier 3 disku. NFS disk može biti dijeljen između više virtualnih poslužitelja i različitih projekta.

6.1.2.2 SMB mrežni disk

Virtualni poslužitelji mogu imati pristup dijeljenom mrežnim diskovima putem SMB protokola. Dijeljeni diskovni prostori se dodjeljuju na zahtjev s centralnog diskovnog polja baziranog na Tier 3 disku. SMB disk može biti dijeljen između više virtualnih poslužitelja i različitih projekta.

6.2 Virtualni poslužitelj s instaliranom bazom podataka

CDU platforma omogućuje kreiranje VM-a s instaliranom i licenciranom bazom podataka:

- MS SQL Enterprise edition
- Oracle 18C SE2 s WebLogic SE2 aplikacijskim poslužiteljem.

Moguće je ostvarivanje dodatne redundancije kreiranjem 2 identična poslužitelja te uspostavom replikacije na nivou baze podataka.
Baze podataka otvorenog koda su podržane na platformu u punom smislu te se instaliraju i konfiguriraju prema najboljim praksama.

6.3 Snimanje sigurnosne kopije (backup podataka)

Backup virtuanih poslužitelja radi se jednom dnevno korištenjem VM snapshot tehnologija na zasebni backup uređaj s retencijom podataka 30 dana.

Backup baza podataka i aplikacija za koji nije moguć aplikacijski-konzistentni backup kroz VM snapshot, korisnik sam treba preusmjeriti (koristeći nativne alate baza podataka ili aplikacija: rman, export dump,...) na Tier3 diskove koji su prezentirani virtualnim poslužiteljima u tom slučaju (diskovi s zasebnog storage-a). Tako napravljeni backupi će također jednom dnevno biti pokupljeni kroz VM snapshot backup i biti čuvani 30 dana. Korisnik sam treba brinuti o rotaciji/brisanju starih backup podataka s tog diska (Općenito nije potrebno držati više od dvije kopije disk backupova jer se backup na backup uređaj radi svaki dan)
Backup transakcijskih logovi baza podataka se isto mogu stavljati na takve Tier3 diskove frekvencijom kako zahtjeva aktivnost na bazama, ali će oni biti pokupljeni kroz backup sustav jednom dnevno.

NFS share-ovi se također backupiraju (za one koji se temeljem LLD-a tako definirano) korištenjem snapshot tehnologija na zasebni backup uređaj s retencijom od 30 dana, ali kroz zaseban backup job što znači da uglavnom neće biti backupirani u isto vrijeme kao i VM-ovi na koje su mountani.

Zadana frekvencija backupa (snapshot VM-ova i NFS-ova) je jednom dnevno s backup prozorom od 00:00 u ponoć do 8:00 s retencijom od mjesec dana. U iznimnim slučajevima možemo dogovoriti i drugačiju frekvenciju backupa, ako je zaista potrebno.

Restore podataka:
restore VM-ova rade djelatnici CDU-a u dogovoru s korisnikom (na istu/orginalnu lokaciju ili na neku privremenu lokaciju odakle se mogu izvući samo neki potrebni podaci).
U slučaju restora baza podataka s backup diskova, djelatnici CDU-a prezentiraju snapshot kopiju Tier 3 backup diskova iz vremenskog trenutka u koji se želi vratiti, a korisnik sami dalje radi restore/recover baze podataka koristeći nativne alate s kojima je rađeni i backup.

6.4 Antivirusna zaštita

Svi sustavi instalirani na Windows okruženju su automatski zaštićeni od virusa i zlonamjernog koda putem zaštite instalirane u hipervizor CDU platforme. Korisnik ne mora provoditi instalacijske procese i procedure te nabavljati antivirusni softver.

6.5 Geo redundancija (Pričuvna lokacija/DR zaštita)

U sklopu usluge je omogućena geo redundantna zaštita servisa na nivou dva fizička podatkovna centra na dvije lokacije. Svaki virtualni poslužitelj kreiran na infrastrukturi je automatski geo redundatno zaštićen i u slučaju ispada jedne fizičke lokacije podatkovnog centra, isti će biti pokrenut na drugoj lokaciji u drugom fizičkom podatkovnom centru. Prebacivanje i pokretanje servisa je automatska radnja te nije potrebna dodatna manualna akcija.

6.6 Mrežni servisi

6.6.1 Interna LAN mreža

Svi virtualni poslužitelji se vežu na LAN mrežu unutar CDU platforme prilikom kreiranja poslužitelja. CDU platforma automatizmom dodjeljuje mrežni segment iz privatne klase te se time osigurava jedinstveni harmonizirani adresni prostor svih hostanih servisa. Platforma je koncipirana na način da su unaprijed odvojene sigurnosne zone putem segmentacije mreže (Internal, frontend DMZ, backend DMZ). Mikrosegmentacija omogućava da se svaki kreirani poslužitelj nalazi u svojoj sigurnosnoj zoni što osigurava visok nivo zaštite. Mrežni raspon rezerviran za IaaS uslugu je 172.16.0.0/14 Mrežna segmentacija je predefinirana prema tablici ispod.

Mrežni segment	Predefinirani mrežni raspon
Internal	172.16.x.0/25
FrontEnd DMZ	172.16.x.128/26
BackEnd DMZ	172.16.x.192/26

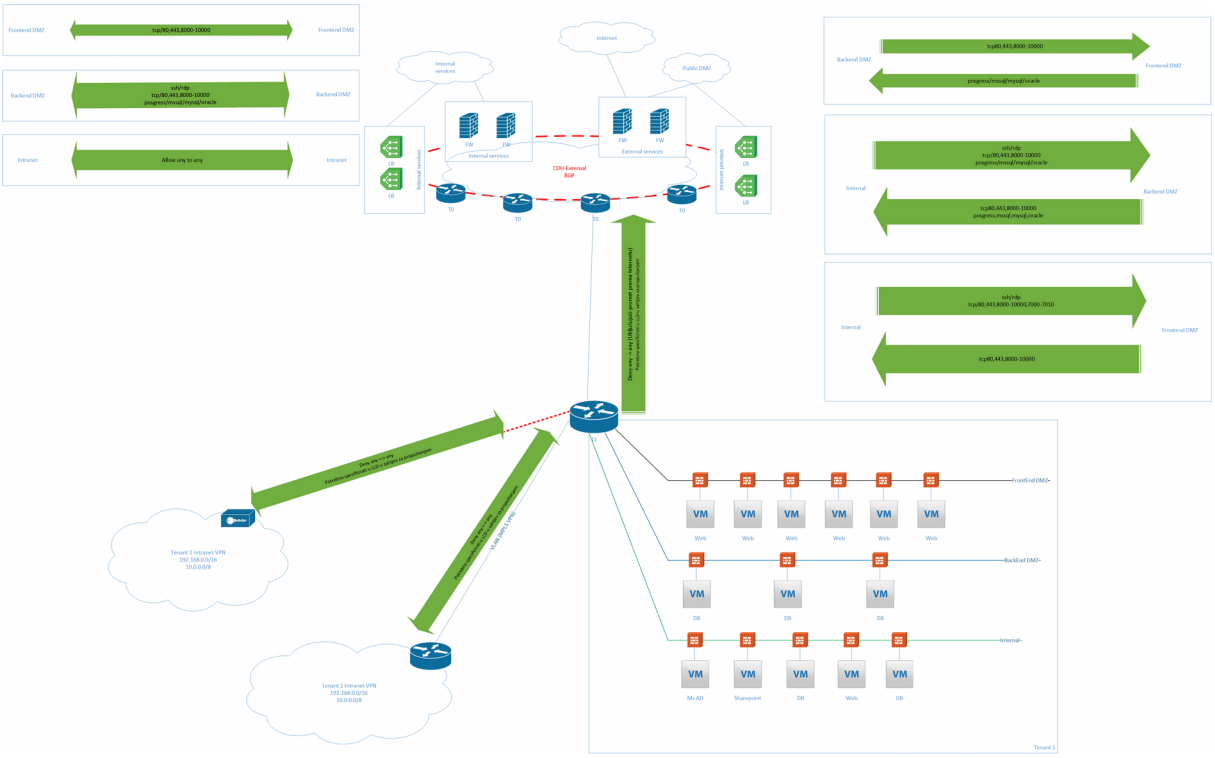
6.6.2 Pristup javnoj Internet mreži

Virtualni poslužitelji na CDU platformi nemaju direktni pristup javnoj Internet mreži zbog visoke razine sigurnosti CDU platforme. U slučaju da je servis hostan na CDU platformi ima potrebu za komunikacijom sa servisom koji je objavljen na javnoj Internet mreži tada će se komunikacija obavljati putem GSB platforme odnosno API management sustava. Na taj način se osigurava sigurna i kontrolirana komunikacija između servisa. U iznimnim situacijama je moguće na zahtjev propustiti strogo kontroliran promet prema endpoint-u na Internetu.

6.6.3 Mikrosegmentacija (distribuirani vatrozid)

Na CDU platformi je implementirana mikrosegmentacija na nivou VM-a te istu nije moguće isključiti ili zaobići. Svaki VM instaliran na platformi je automatski zaštićen distribuiranim NSX vatrozidom koji štiti

VM od mrežnog pristupa bilo unutar istog mrežnog segmenta ili iz drugog mrežnog segmenta. Mikrosegmentacija je unaprijed postavljena i prikazana je na slijedećoj slici:



6.6.4 Softverski NSX Load Balancer (interni load balancer)

Softverski Load Balancer (interni) se koristi za balansiranje mrežnih servisa instaliranih na VM-ima. VIP adresa se može konfigurirati u jednom od mrežnih segmenata koji pripadaju projektu. Interni load balancer je jedina opcija u slučaju kad se balansira servis unutar projekta.

6.6.5 Hardverski F5 Load Balancer (eksterni load balancer)

Hardverski Load Balancer (eksterni) je baziran na F5 fizičkom uređaju te se koristi za objavljivanje servisa prema Internet/Hitronet mreži. Isti na sebi ima konfiguriran Web Applikacijski firewall (WAF) koji štiti objavljeni servis. Uloga eksternog load balancera je adresna translacija servisa te može imati ulogu SSL offload-a za kriptiranje servisa prema pristupnim mrežama.

6.6.6 Hardverski L7 vatrozid

Hardverski L7 vatrozid baziran je na Palo Alto Networks uređaju služi kao perimetar vatrozida za zaštitu servisa objavljenih na javnoj mreži Internet mreži ili Hitronet mreži.

6.7 DNS

CDU platforma nudi uslugu udomljavanja DNS domena kako za javne servise tako za interne hitronet servise.

6.7.1 Javni DNS

CDU platforma posjeduje DNS infrastrukturu visoke raspoloživosti, visokog kapaciteta i brzine odziva. Korisnik može udomiti primarni i sekundarni DNS poslužitelj za javne domene. Također za sve servise hostane na CDU platformi se može koristiti reverzni DNS.

6.7.2 Interni DNS i DNS cache za virtualne poslužitelje

Svi servisi objavljeni na privatnim mrežama se mogu objaviti u internom DNS-u koji će biti podešen za internu domenu ssc.gov.hr.
Svi virtualni poslužitelji kreirani na CDU platformi će imati konfiguriran interni DNS kao glavni DNS poslužitelj (DNS cache) koji će biti podešen za odgovore za sve javne i interne DNS zapise.

6.8 NTP

Platforma je u potpunosti vremenski sinkronizirana i krajnji korisnik ne treba brinuti o sinkronizaciji vremena te će svi virtualni poslužitelji biti unaprijed konfigurirani za korištenje centralnog NTP servisa.

6.9 Autentikacija korisnika (CDU IDAM)

CDU platforma posjeduje LDAP/Kerberos/Radius servis (CDU IDAM) za korisničke račune zaposlenika tijela državne uprave. Isti je sinkroniziran s registrom zaposlenih. Upravljanje korisničkim računima i resetiranje lozinke se vrši kroz centralni službenički portal.
Na zahtjev je moguće dobiti pristup na CDU IDAM platformu za potrebe servisa hostanog na CDU platformi.
CDU IDAM je tehnološki baziran na FreeIPA tehnologiji.

6.10 Linux softverski repozitorij

CDU platforma posjeduje interne softverske repozitorije za sve linux distribucije koje su dostupne na platformi. Repozitoriji su preslika originalnih repozitorija.
Svi kreirani virtualni poslužitelji automatski su spojeni na interne repozitorije softverskih paketa.

6.11 Gitlab servis

CDU platforma posjeduje interni Gitlab repozitorij koji se koristi za CI/CD za CDU hostane servise.

6.12 Mail relay servis

CDU platforma ima ugrađen mail relay servis kojim je jedino moguće slanje elektronske pošte u svijet. Mail relay servis je dostupan svim virtualnim poslužiteljima i udomljenim aplikacijama i koristi se bez dodatne autentikacije.
Podaci za spajanje na mail servis:
FQDN smtp servera: servmail.ssc.gov.hr
port: TCP/25
IP adresa: 172.31.0.21

Za sve javne domene čiji mailbox-ovi nisu udomljene na CDU platformi potrebno je dodati SPF DNS zapise u javni DNS za domenu u čije ime se šalje elektronska pošta. IP adrese koje se dodaju u SPF zapis:

Record name: @
Record type: TXT
Record: "v=spf1 a:spf.mail.cdu.gov.hr -all"

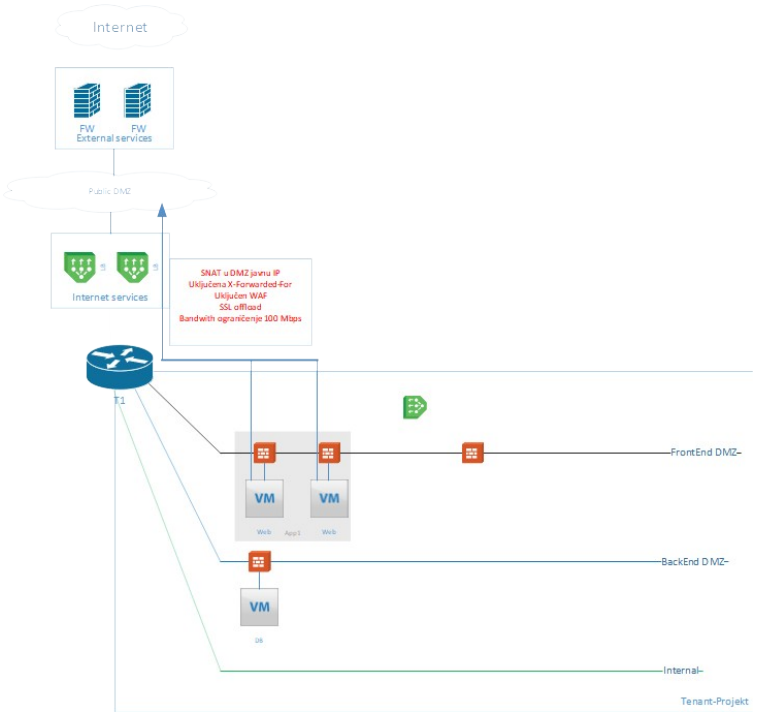
7 Pristupna mreža

CDU servisi mogu biti dostupni kroz više tipova pristupnih mreža i kombinacija pristupa. Slijedeći tipovi pristupnih mreža su dostupni korisnicima:

- Javna Internet mreža, (servis je dostupan na Internetu)
- IPsec VPN tunel preko Interneta (servis je dostupan ostvarenjem VPN tunela s korisnikovom mrežom)
- Hitronet mreža (servis je dostupan korisnicima Hitronet mreže),
- Hitronet VPN (servis je dostupan u privatnoj mreži korisnika kao dodatna lokacija na privatnim adresama)
- VPN klijentski pristup preko Interneta (svako pojedinačno računalo/korisnik imaju VPN pristup do serisa
- Carnet VPN (servis je dostupan u privatnoj mreži korisnika kao dodatna lokacija na privatnim adresama)- CARNET JE U PROCESU SPAJANJA!!
- MPLS privatnog Telekom operatera

8 Referentna arhitektura javnog servisa

U ovom poglavlju je objašnjena arhitektura javno dostupnog servisa hostanog na CDU platformi u IaaS usluzi. Servis se sastoji od web, aplikacijskog i DB sloja instaliranog na posebnim VM-ovima na CDU platformi. Zbog postizanja visoke dostupnosti i mogućnosti skaliranja, web i aplikacijski slojevi su implementirani u vidu više VM-ova te se javni servis balasira putem hardverskog load balancer-a (HLB).
Slika ispod prikazuje arhitekturu javno dostupnog servisa hostanog na CDU platformi u IaaS modelu.



8.1 *Oglašavanje servisa na javnoj Internet mreži*

Pristup korisnika iz javne mreže se realizira putem javne Internet mreže i IP adrese iz DMZ mreže. Servisna javna VIP adresa se putem eksternog load balancera objavljuje na Internetu. Eksterni load balancer je konfiguriran u SNAT modu, a da bi se zadržala informacija o izvorišnim adresama klijenata

koristi se X-forwarded-For metoda u HTTP zaglavljima. Na servisu se može konfigurirati SSL offload čime se rasterećuju web poslužitelji za procese enkripcije web prometa.
Svi hostani servisi su limitiranog bandwith-a na 100 Mbps čime se povećava nivo sigurnosti i s druge strane osigurava da servis zbog tehničkih problema ne utječe na cjelokupnu platformu. Povećanje limita je moguće, ali za istu je potrebno provesti analizu i donijeti odluku o opravdanosti zahtjeva.
Svi servisi objavljeni na Internetu mogu biti zaštićeni WAF zaštitom (web application firewall) koji se zasebno konfigurira na eksternim load balancerima.
DMZ mreža se dodatno štiti L7 Palo Alto firewall-om na kojem se radi aplikacijska inspekcija prometa s uključenim DDoS mehanizmima.
CDU platforma osigurava javnu IP adresu i vrši konfiguraciju Load balancera i vatrozida.

8.2 Interni load balancing

Interno balansiranje servisa je jedino moguće kroz interni load balancer. VIP adresu servisa je moguće smjestiti u bilo koji segment. Interni VIP servisa nije moguće dohvatiti izvan mrežnog segmenta tenanta.

8.3 Udaljeni pristup

Udaljeni pristup na poslužitelje za potrebe administracije i instalacije te održavanja je jedino moguć kroz posebni CDU servis za klijentski udaljeni pristup.

8.4 Pristup Internetu sa hostanog sustava

Direktan pristup Internetu sa instaliranih VM-ova nije moguć.

8.5 Ažuriranje operacijskih sustava i sistemskog softvera

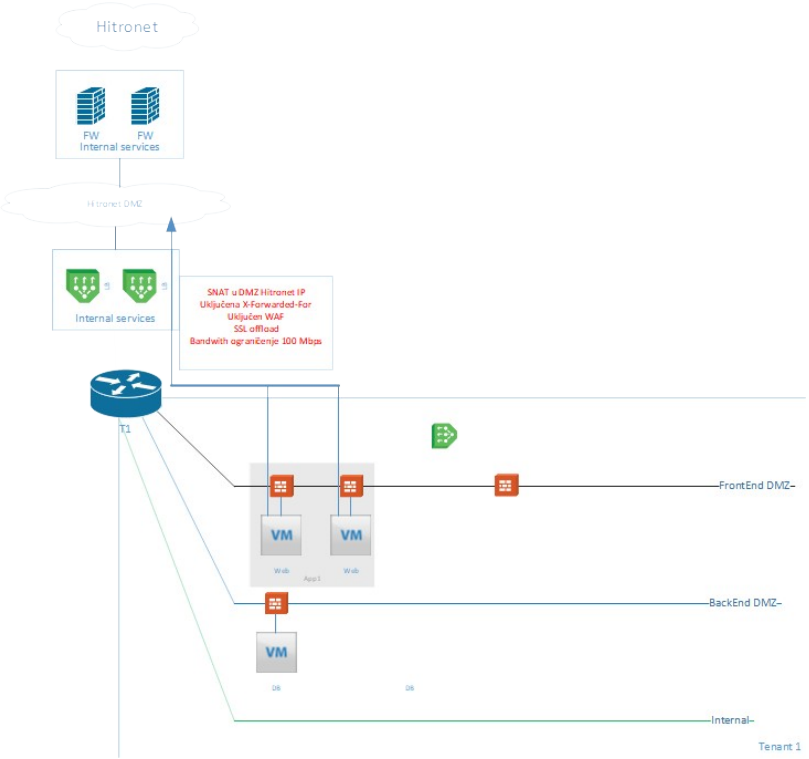
Instalacija i ažuriranje sistemskog softvera se vrši sa internih depo/wsus poslužitelja koji su konfigurirani na sustavu i dostupni su svim instaliranim VM-ovima. Održavanje i ažuriranje depo i wsus poslužitelja je obaveza CDU tima. U slučaju posebne potrebe za softverom koji nije moguće dohvatiti sa internih depo poslužitelja isti će biti omogućen na zahtjev.

8.6 Pristup vanjskim servisima

U slučaju potrebe da hostani sustav/servis mora zvati vanjski javni ili privatni servis, isti će biti dostupan putem GSB (Government Service Bus) platforme tj. kroz API management platformu. Na zahtjev će se vanjski servis kreirati na GSB platformi te će mu se omogućiti pristup sa hostanog sustava.
Iznimno je moguće dopustiti servisu direktni spoj prema drugom servisu, ali isključivo kontrolirano kroz posebno pravilo na vatrozidu.

9 Referentna arhitektura Hitronet troslojnog servisa

U ovom poglavlju je objašnjena arhitektura Hitronet oglašenog servisa hostanog na CDU platformu u IaaS usluzi. Servis se sastoji od web, aplikacijskog i DB sloja instaliranog na posebnim VM-ovima na CDU platformi. Zbog postizanja visoke dostupnosti i mogućnosti skaliranja, web i aplikacijski slojevi su implementirani u vidu više VM-ova te se Hitronet servis balasira putem eksternog load balancer-a.
Slika ispod prikazuje arhitekturu Hitronet oglašenog servisa hostanog na CDU platformi u IaaS modelu.



9.1 Oglašavanje servisa na Hitronet mreži

Pristup korisnika iz Hitronet mreže se realizira putem spoja CDU platforme na Hitronet mrežu i dodijeljene IP adrese iz Hitronet rezerviranog raspona adresa. Servisna Hitronet VIP adresa se putem eksternog load balancera objavljuje na Hitronet-u. Eksterni load balancer je konfiguriran u SNAT modu, a da bi se zadržala informacija o izvorišnim adresama klijenata koristi se X-forwarded-For metoda u HTTP zaglavljima. Na servisu se može konfigurirati SSL offload čime se rasterećuju web poslužitelji za procese enkripcije web promet-a.
Svi hostani servisi su limitiranog bandwith-a na 100 Mbps čime se povećava nivo sigurnosti i s druge strane osigurava da servis zbog tehničkih problema ne utječe na cjelokupnu platformu. Povećanje limita je moguće, ali za istu je potrebno provesti analizu i donijeti odluku o opravdanosti zahtjeva.
Svi servisi objavljeni na internetu moraju biti zaštićeni WAF zaštitom (web application firewall) koji se zasebno konfigurira na F5 platformi.
CDU platforma osigurava Hitronet IP adresu i vrši konfiguraciju Load balancera i vatrozida.

9.2 Interni load balancing

Interno balansiranje servisa je jedino moguće kroz interni load balancer. VIP adresu servisa je moguće smjestiti u bilo koji segment. Interni VIP servisa nije moguće dohvatiti izvan mrežnog segmenta tenanta.

9.3 Udaljeni pristup

Udaljeni pristup na poslužitelje za potrebe administracije i instalacije te održavanja je jedino moguć kroz posebni CDU servis za klijentski udaljeni pristup.

9.4 Pristup Internetu sa hostanog sustava

Direktan pristup Internetu sa instaliranih VM-ova nije moguć.

9.5 Ažuriranje operacijskih sustava i sistemskog softvera

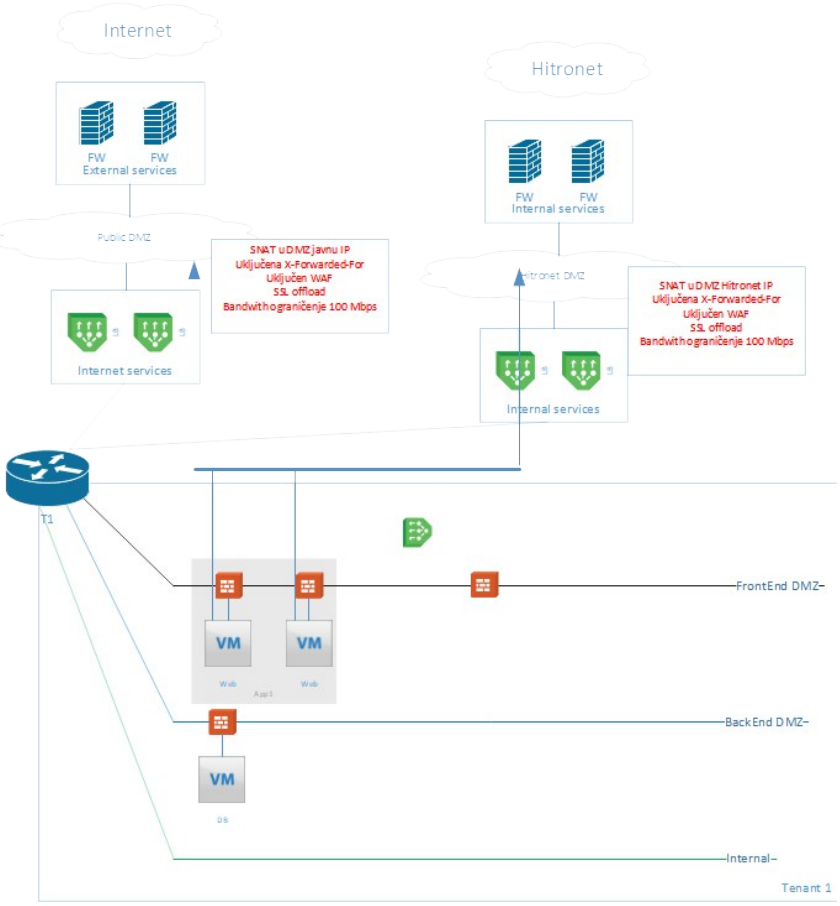
Instalacija i ažuriranje sistemskog softvera se vrši sa internih depo/wsus poslužitelja koji su konfigurirani na sustavu i dostupni su svim instaliranim VM-ovima. Održavanje i ažuriranje depo i wsus poslužitelja je obaveza CDU tima. U slučaju posebne potrebe za softverom koji nije moguće dohvatiti sa internih depo poslužitelja isti će biti omogućen na zahtjev.

9.6 Pristup vanjskim servisima

U slučaju potrebe da hostani sustav/servis mora pristupati vanjskim javnim ili privatnim servisima, isti će biti dostupni putem GSB platforme tj. kroz API management platformu. Na zahtjev će se vanjski servis kreirati na GSB platformi te će mu se omogućiti pristup sa hostanog sustava.
Iznimno je moguće dopustiti servisu direktni spoj prema drugom servisu, ali isključivo kontrolirano kroz posebno pravilo na vatrozidu.

10 Referentna arhitektura servisa koji je u isto vrijeme dostupan iz Javne Internet mreže i Hitronet mreže

U ovom poglavlju je objašnjena arhitektura servisa koji je u isto vrijeme dostupan iz Hitronet mreže te javne Internet mreže. Servis se sastoji od web, aplikacijskog i DB sloja instaliranog na posebnim VM-ovima na CDU platformi. Zbog postizanja visoke dostupnosti i mogućnosti skaliranja, web i aplikacijski slojevi su implementirani u vidu više VM-ova te se servisi balasira putem hardverskog load balancer-a (HLB).
Slika ispod prikazuje arhitekturu servisa hostanog na CDU platformi u IaaS modelu.



10.1 *Oglašavanje servisa na Hitronet mreži*

Pristup korisnika iz Hitronet mreže se realizira putem spoja CDU platforme na Hitronet mrežu i dodijeljene IP adrese iz Hitronet rezerviranog poola adresa. Servisna Hitronet VIP adresa se putem F5 hardverskog load balancera objavljuje na ~~Internetu~~ Hitronetu. F5 load balancer je konfiguriran u SNAT modu, a da bi se zadržala informacija o izvorišnim adresama klijenata koristi se X-forwarded-For metoda u HTTP zaglavljima. Na servisu se konfigurira SSL offload čime se rasterećuju web poslužitelji za procese enkripcije web promet-a.
Svi hostani servisi su limitiranog bandwith-a na 100 Mbps čime se povećava nivo sigurnosti i s druge strane osigurava da servis zbog tehničkih problema ne utječe na cjelokupnu platformu. Povećanje limita je moguće, ali za istu je potrebno provesti analizu i donijeti odluku o opravdanosti zahtjeva.
Svi servisi objavljeni na internetu moraju biti zaštićeni WAF zaštitom (web application firewall) koji se zasebno konfigurira na f5 platformi.

DMZ mreža se dodatno štiti L7 Palo Alto firewall-om na kojem se radi aplikacijska inspekcija prometa s uključenim DDoS mehanizmima.

10.2 Interni load balancing

Interno balansiranje servisa je jedino moguće kroz interni load balancer. VIP adresu servisa je moguće smjestiti u bilo koji segment. Interni VIP servisa nije moguće dohvatiti izvan mrežnog segmenta tenanta.

10.3 Oglašavanje servisa na javnoj Interent mreži

Pristup korisnika iz javne mreže se realizira putem javne Internet mreže i IP adrese iz DMZ mreže. Servisna javna VIP adresa se putem F5 hardverskog load balancera objavljuje na Interntu. F5 load balancer je konfiguriran u SNAT modu, a da bi se zadržala informacija o izvorišnim adresama klijenata koristi se X-forwarded-For metoda u HTTP zaglavljima. Na servisu se konfigurira SSL offload čime se rasterećuju web poslužitelji za procese enkripcije web promet-a.
Svi hostani servisi su limitiranog bandwith-a na 100 Mbps čime se povećava nivo sigurnosti i s druge strane osigurava da servis zbog tehničkih problema ne utječe na cjelokupnu platformu. Povećanje limita je moguće, ali za istu je potrebno provesti analizu i donijeti odluku o opravdanosti zahtjeva.
Svi servisi objavljeni na internetu moraju biti zaštićeni WAF zaštitom (web application firewall) koji se zasebno konfigurira na f5 platformi.
DMZ mreža se dodatno štiti L7 Palo Alto firewall-om na kojem se radi aplikacijska inspekcija prometa s uključenim DDoS mehanizmima.

10.4 Mikrosegmentacija

Distribuirani firewall (Mikrosegmentacija) predstavlja prvi mehanizam obrane sustava. Mikrosegmentacija postavlja softverski firewall ispred svakog instaliranog VM-a i ne može se isključiti ili onemogućiti.

10.5 Udaljeni pristup

Udaljeni pristup na poslužitelje za potrebe administracije, instalacije i održavanja je jedino moguć kroz posebni CDU servis za klijentski udaljeni pristup. Udaljeni pristup je detaljno opisan u dokumentu „Udaljeni pristup trećih strana“.

10.6 Pristup Internetu sa hostanog sustava

Direktan pristup Internetu sa instaliranih VM-ova nije moguć.

10.7 Ažuriranje operacijskih sustava i sistemskog softvera

Instalacija i ažuriranje sistemskog softvera se vrši sa internih depo/wsus poslužitelja koji su konfigurirani na sustavu i dostupni su svim instaliranim VM-ovima. Održavanje i ažuriranje depo i wsus poslužitelja je obaveza CDU tima. U slučaju posebne potrebe za softverom koji nije moguće dohvatiti sa internih depo poslužitelja isti će biti omogućen na zahtjev.

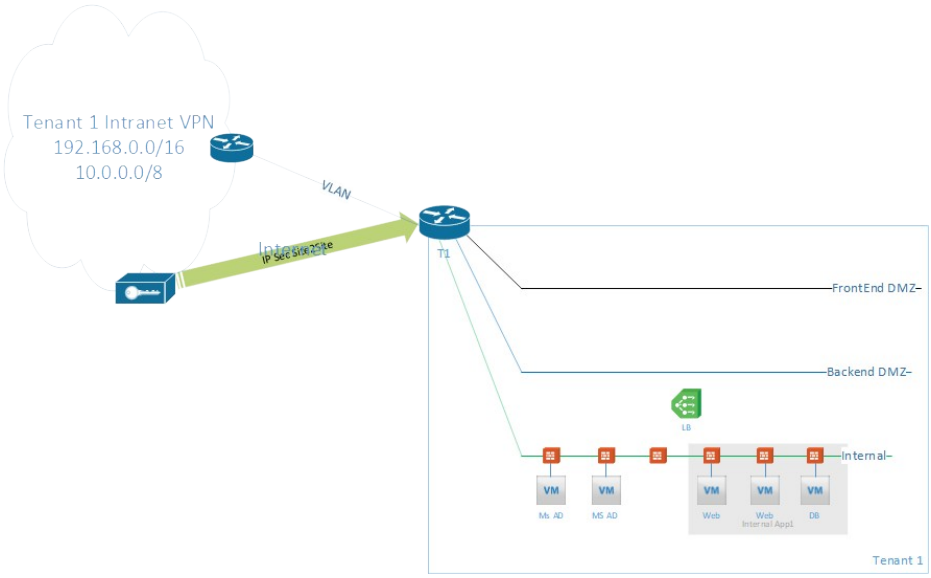
10.8 Pristup vanjskim servisima

U slučaju potrebe da hostani sustav/servis mora pristupati vanjskim javnim ili privatnim servisima, isti će biti dostupni putem GSB platforme tj. kroz API management platformu. Na zahtjev će se vanjski servis kreirati na GSB platformi te će mu se omogućiti pristup sa hostanog sustava.

11 Referentna arhitektura servisa koji je dostupan samo iz interne mreže putem privatne mreže L3 VPN-a ili IPsec VPN-a

U ovom poglavlju je objašnjena arhitektura servisa koji je dostupan samo iz interne mreže korisnika. Interna mreža podrazumjeva zatvorenu štićenu mrežu u kojoj se koristi IP raspon rezerviran za privatne mreže. Servis hostan u ovom modelu nije dostupan niti jednom drugom tenantu. Interni Load balancer je jedina opcija za balansiranje servisa prema internoj mreži.

Slika ispod prikazuje arhitekturu servisa hostanog na CDU platformi u IaaS modelu.



12 Matrica odgovornosti za IaaS uslugu

Ispod je prikazana matrica odgovornosti za IaaS uslugu.

KOMPONENTA SUSTAVA	ODGOVORNOST
Podatkovni centar (UPS, Agregati, klimatizacija …)	CDU tim
Fizička sigurnost podatkovnog centra	
Hardver (poslužitelji, diskovna polja)	
Mrežna infrastruktura	
Pristup internetu	
Upravljanje javnim IP adresama	
Upravljanja privatnim IP adresama	
Spajanje telekom operatera i Hitronet mreže na CDU platformu	
Sinkronizacija vremena na platformi	
DNS hosting za javne IP adrese i domene	
Virtualizacijski sloj	
Mrežna sigurnost	
Hardverski load balancing	
Web aplikacijski firewall	
DDoS zaštita	
Backup platforme i hostanih servisa	
Upravljanja georedundancijom (DR funkcionalnost)	
Udaljeni pristup trećih strana (VPN pristup dobavljača)	
Nazor CDU platforme	
Upravljanje template-ima za kreiranje virtualnih poslužitelja	
Odobravanje i dodjeljivanje resursa korisniku	
Kreiranje virtualnih poslužitelja i upravljanje dodijeljenim resursima	
Operacijski sustav na virtualnom poslužitelju	
Aplikacijski softver na virtualnom poslužitelju	
Baze podataka	
Aplikacijski softver	