Agencija za podršku informacijskim sustavima i informacijskim tehnologijama d.o.o.

Referentna arhitektura servisa u IaaS modelu

Javno
V 2.0

Vlasnik dokumenta:	CDU
Autor:	Mr.Sc. Mladen Goršeta, dipl.ing. elektrotehnike
Oznaka dokumenta:	CDU_AS_01
Verzija:	2.0
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

1.2 Povezani dokumenti

Ovaj dokument je povezan s dokumentima:

Oznaka dokumenta	**verzija**

1.3 Odobrenja

Ovaj dokument mora odobriti:

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

1.4 Distribucija

Ovaj dokument mora biti dostavljen:

Ime	**Titula**	**Datum**	**Broj kopija**	

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.

Podržane verzije softvera koje se mogu koristi na CDU platformi su navedene u posebnom dokumentu: „CDU infrastrukturni standard“.

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 aplikacijski 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

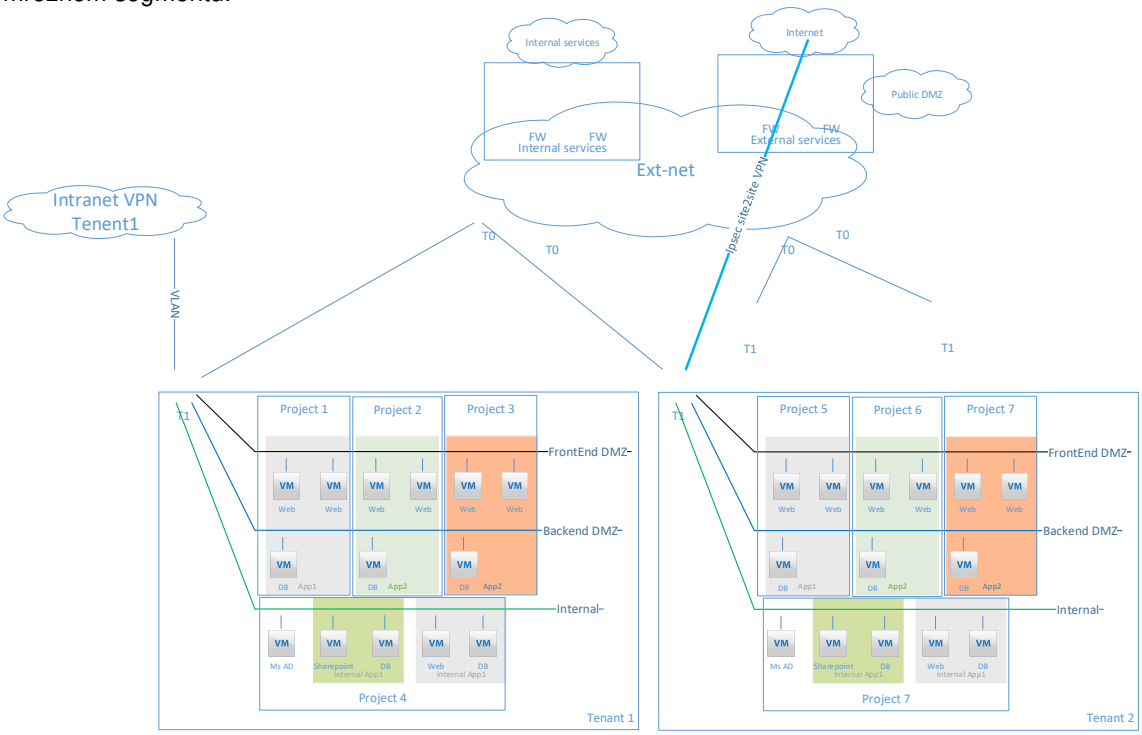
Svaki servis udomljen na CDU infrastrukturi može biti dostupan putem minimalno jednog ili više tipova mrežnog pristupa:

- 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 terminiranje kriptiranog tunela. CDU platforma osigurava na svojoj strani terminiranje 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 Arhitektura IaaS usluge

Arhitektura IaaS usluge je prikazana na slici ispod. Za svakog pojedinačnog korisnika se kreira posebni virtualni podatkovni centar s jednim dediciranim virtualnim ruterom. Virtualni podatkovni centri su međusobno mrežno izolirani. Svaki korisnički tenant inicijalno ima jedan projekt s unaprijed dodijeljenim resursima. Projekt predstavlja administrativno odvajanje sustava unutar Tenanta. Npr. javno dostupni sustav održavan od strane jednog dobavljača se smješta u jedan projekt i na taj projekt se može dopustiti pristup samo određenom dobavljaču. Projekti su mrežno odvojeni korištenjem mikrosegmentacije te virtualni pslužitelji različitih projekata su mrežno izolirani iako se nalaz u istom mrežnom segmentu.



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

Virtualni poslužitelji mogu imati pristup dijeljenom mrežnim diskovima putem SMB ili NFS protokola. Dijeljeni diskovni prostori se dodjeljuju na zahtjev s centralnog diskovnog polja baziranog na Tier 3 disku.

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)

CDU platforma automatski snima sigurnosne kopije svih kreiranih resursa na platformi prema standardnoj politici:

- Backup se provodi jednom dnevno (u noćnim satima)
- Backup se snima na nivou VM-a
- Backup se replicira na drugu lokaciju čime se osigurava DR funkcionalnost za snimljene kopije podataka

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 fizičkog podatkovnog centra. Svaki virtualni poslužitelj kreiran na infrastrukturi je automatski geo redundatno zaštićen i u slučaju ispada fizičke lokacije podatkovnog centra, isti će biti pokrenut 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, fronetend DMZ, backend DMZ). Mikrosegmentacija omogućava da se svaki kreirani poslužitelj nalazi u svojoj sigurnosnoj zoni što osigurava visok nivo zaštite. Mrežna segmentacija je predefinirana prema tablici ispod.

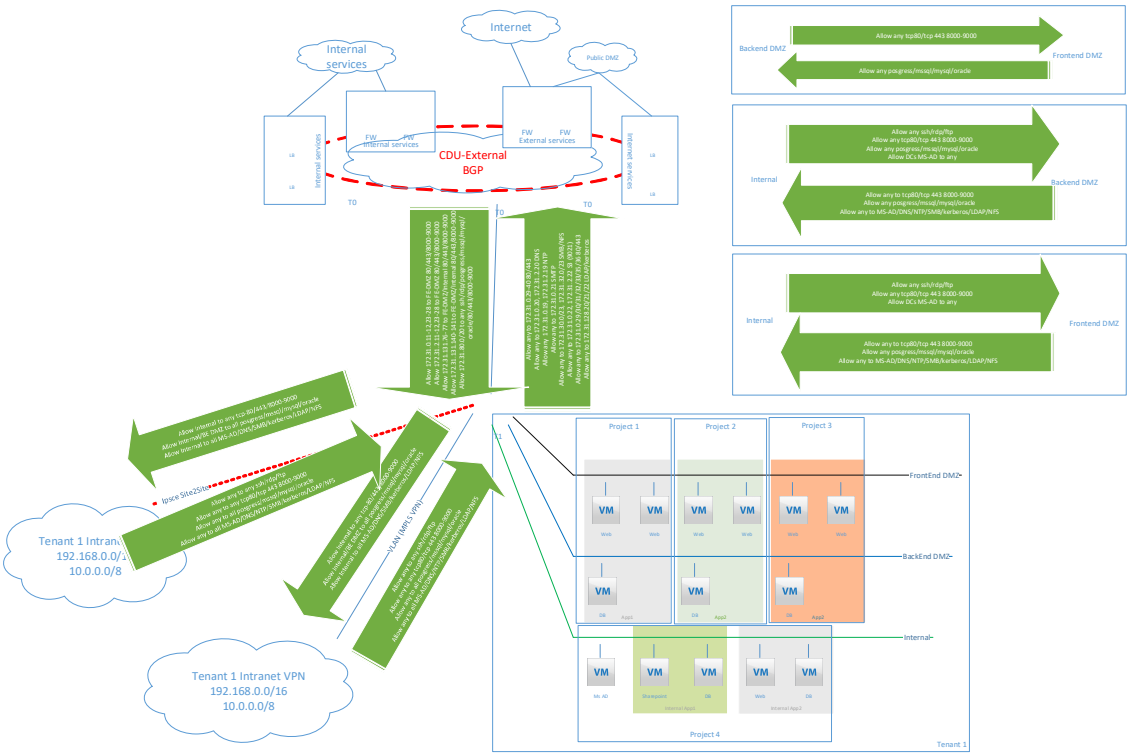
Mrežni segment	Predefinirani mrežni raspon
Internal	172.31.x.0/25
FronetEnd DMZ	172.31.x.128/26
BackEnd DMZ	172.31.x.192/26

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 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.

6.6.3 Mikrosegmentacija (distribuirani firewall)

CDU platforma omogućuje mikrosegmentaciju 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 lodabalancer (SLB)

Softverski load balancer (SLB) se koristi za balansiranje mrežnih servisa instaliranih na VM-ima. VIP adresa se uvijek nalazi u istom mrežnom segmentu u kojem su instalirani VM-ovi (one arm konfiguracija).

6.6.5 Hardverski load balancer (HLB)

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

6.6.6 Hardverski L7 Firewall

Hardverski L7 firewall baziran na Palo Alto Networks uređaju služi za zaštitu servisa objavljenih na javnoj mreži Internet mreži ili Hitronet mreži.

6.6.7 DNS

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

6.6.7.1.1 Javni DNS

CDU platforma posjeduje DNS infrastrukture visoke raspoloživosti i 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 reversni DNS.

6.6.7.1.2 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 cdu.local.
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.

6.6.8 NTP

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

6.6.9 Objavljivanje servisa na internetu

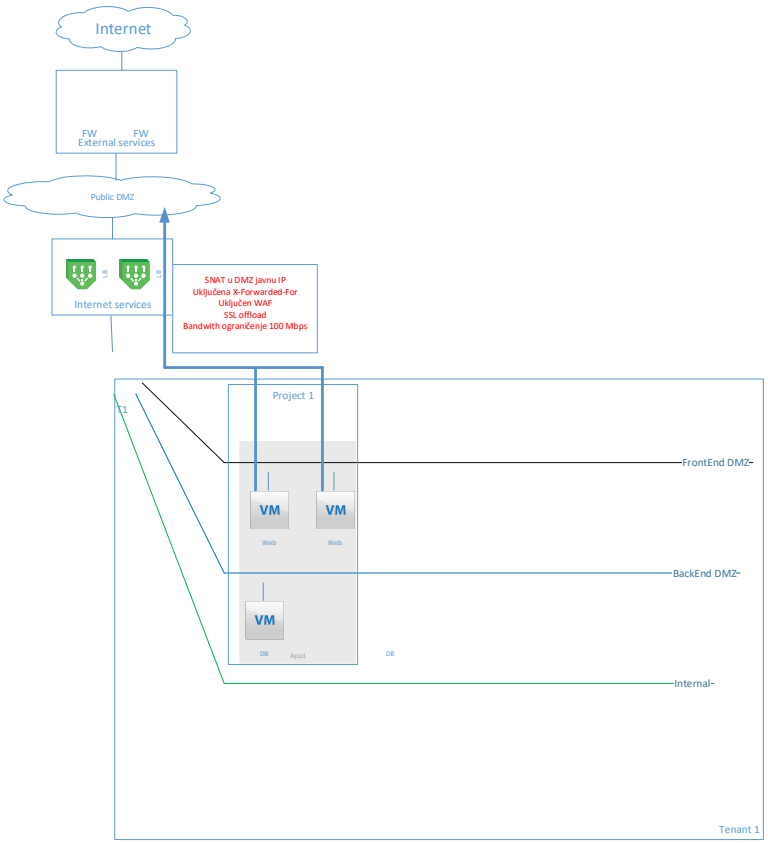
U slučaju da je servis hostan na CDU platformi javni servis, isti se objavljuje putem HLB-a na javnoj Internet mreži koji vrši adresnu translaciju iz privatne u javnu adresu i enkripciju prometa putem SSL sertifikata. Nije moguće objaviti servis na internetu direktno sa virtualnog poslužitelja.

6.6.10 Autentikacija korisnika

Glavni Autentikacijski servis za sve usluge je NIAS servis.
CDU platforma posjeduje LDAP/Kerberos/Radius servis s OTP funkcionalnosti 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.

7 Referentna arhitektura javnog servisa

U ovom poglavlju je objašnjena arhitektura javno dostupnog 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 javni servis balasira putem hardverskog load balancer-a (HLB).
Slika ispod prikazuje arhitekturu javno dostupnog servisa hostanog na CDU platformi u IaaS modelu.



7.1 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.

7.2 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.

7.3 Udaljeni pristup

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

7.4 Pristup internetu sa hostanog sustava

Direktan pristup Internetu sa instaliranih VM-ova nije moguć.

7.5 Ažuriranje operacijskih sustava i sistemskog softvera

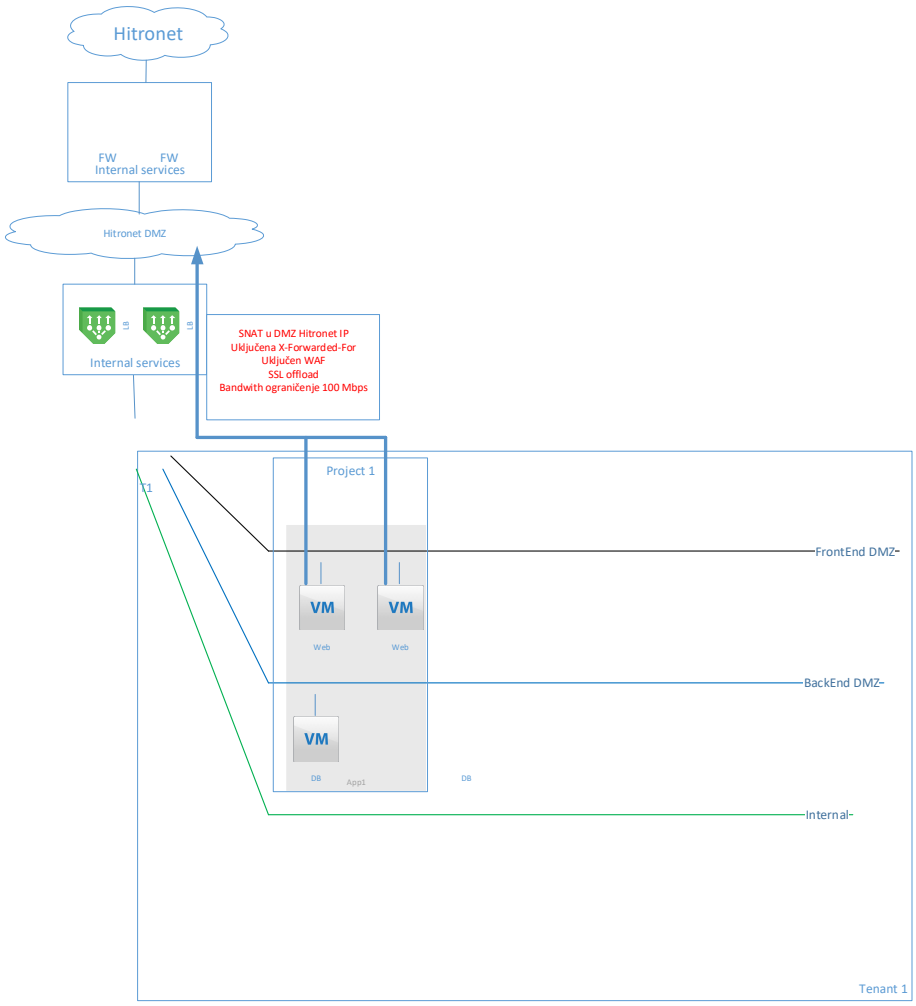
Instalacija i ažuriranje sistemskog softvera se vrši sa internih depo/wsus poslužitelja koji su konfigurirani na sustavu i dostupnim svim instaliranim VM-ovima. Održavanje i ažuriranje depo i wsus poslužitelja je obaveza CDU tima. U slučaju posebne potrebe za softverom koji nije moguće dohvatiti sa internih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

7.6 Pristup vanjskim servisima

U slučaju potrebe da hostani sustav/servis mora zvati vanjski javni ili privatni servis, isti će biti dostupan 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.

8 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 hardverskog load balancer-a (HLB). Hitronet oglašeni servis se balansira putem F5 hardverskog load balancer-a sa uključenim dodatnim sigurnosnim mehanizmima.
Slika ispod prikazuje arhitekturu hitronet oglašeno servisa hostanog na CDU platformi u IaaS modelu.



8.1 Oglašavanje servisa na Hitronet mreži

Pristup korisnika iz Hitronet mreže se realizira putem spoja CDU platforme na Hitronet mrežu i dodijeljene IP adrese iz Hitromnet rezerviranog raspona adresa. Servisna Hitronet VIP adresa se putem F5 hardverskog load balancera objavljuje na Hitronet-u. 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.

8.2 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.

8.3 Udaljeni pristup

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

8.4 Pristup internetu sa hostanog sustava

Direktan pristup Internetu sa instaliranih VM-ova nije moguć.

8.5 Ažuriranje operacijskih sustava i sistemskog softvera

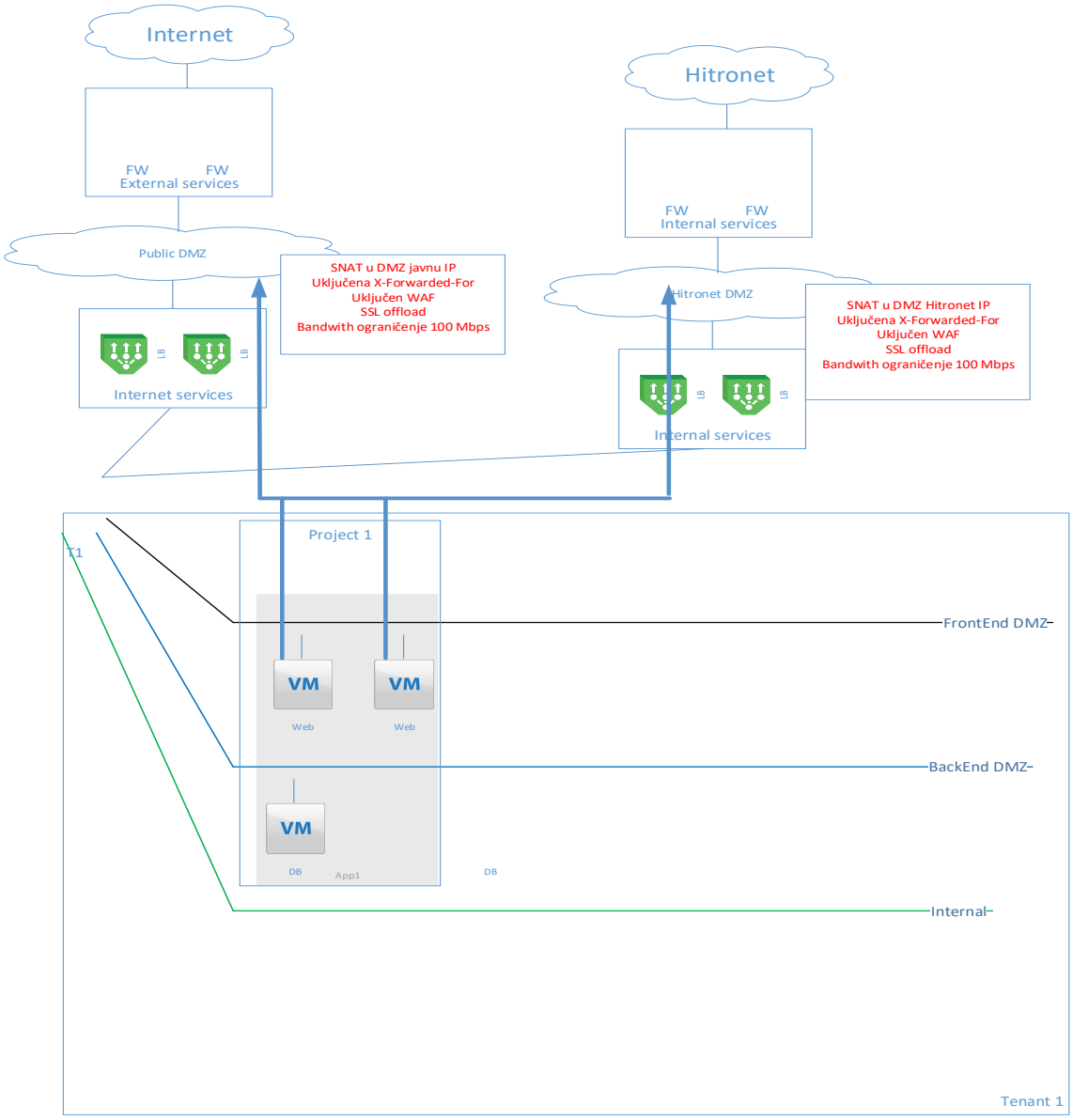
Instalacija i ažuriranje sistemskog softvera se vrši sa internih depo/wsus poslužitelja koji su konfigurirani na sustavu i dostupnim svim instaliranim VM-ovima. Održavanje i ažuriranje depo i wsus poslužitelja je obaveza CDU tima. U slučaju posebne potrebe za softverom koji nije moguće dohvatiti sa internih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

8.6 Pristup vanjskim servisima

U slučaju potrebe da hostani sustav/servis mora 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.

9 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.



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 Hitromnet rezerviranog pula adresa. Servisna Hitronet 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.

9.2 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.

9.3 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.

9.4 Udaljeni pristup

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

9.5 Pristup internetu sa hostanog sustava

Direktan pristup Internetu sa instaliranih VM-ova nije moguć.

9.6 Ažuriranje operacijskih sustava i sistemskog softvera

Instalacija i ažuriranje sistemskog softvera se vrši sa internih depo/wsus poslužitelja koji su konfigurirani na sustavu i dostupnim 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.

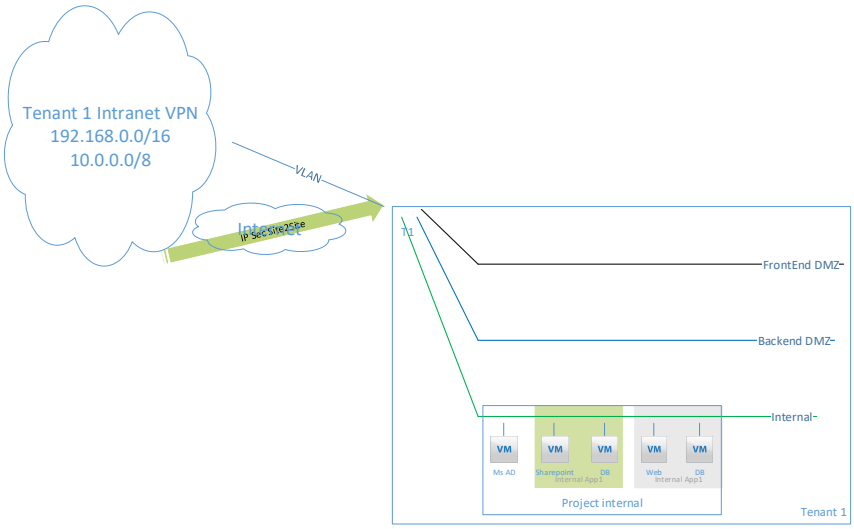
9.7 Pristup vanjskim servisima

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.

10 Referentna arhitektura servisa koji je dostupan samo iz interne mreže putem privatne mreže 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 kojej se koristi IP raspon rezerviran za privatne mreže. Pristupna mreža je definirana u poglavlju 4.2 ovog dokumenta. Servis hostan u ovom modelu nije dostupan niti jednom drugom tenantu.

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



11 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-ovima za kreiranje virtualnih poslužitelja	
Odobravanje i dodjeljivanje resursa korisniku	
Kreiranje virtualnih poslužitelja i upravljanje dodijeljenim resursima	Korisnik
Operacijski sustav na virtualnom poslužitelju	
Aplikacijski softver na virtualnom poslužitelju	
Baze podataka	
Aplikacijski softver	