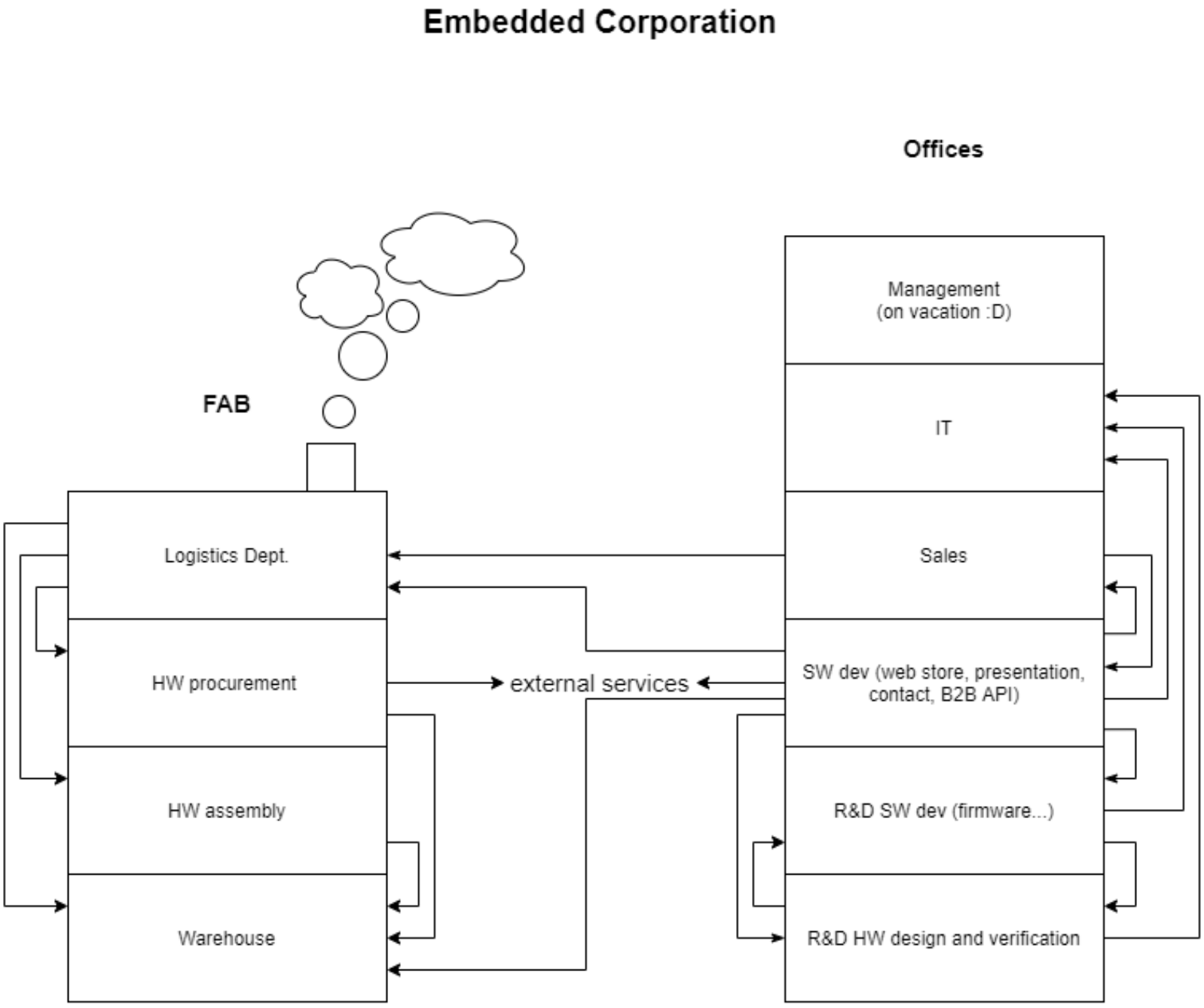
14.11.2021. Projekat - prvi dio



Na slici iznad je okvirno predstavljena struktura firme koja se bavi kreiranjem i proizvodnjom hardvera (Printed Circuit Board Assembly and Design). Firmu grubo delimo na dva dela (na slici simbolično predstavljeni kao zgrade) po poslovima koje obavljaju. Prvi od njih je “fabrika”, koji podrazumijeva planiranje proizvodnje, nabavku i skladištenje sirovina i čipova (SMD), proizvodnju PCB-ova i skladištenje tih gotovih proizvoda. Drugi deo, predstavljen kao “kancelarije” se sastoji od R&D sekcije (gde se osmišljavaju PCB ploče i implementira firmware

za njih), sekcija za predstavljanje firme i komunikaciju sa tržištem, prodajni sektor, kao i IT sektor koji se bavi upravljanjem IT infrastrukture svih sektora u celoj firmi.

Sektori sa njihovim zaduženjima:

- Warehouse
  Skladište ima interni servis za praćenje stanja svih dostupnih proizvoda i sirovina kojima raspolaže firma.
- HW assembly
  PCBA proizvodni pogon. Komunicira sa Warehouse servisom kako bi dobavio sve sirovine potrebne za izradu zadatog hardvera.
- HW procurement
  Sektor zadužen za nabavku sirovina i SMD čipova (po nalogu departmana za logistiku). To podrazumijeva klijentski servis koji komunicira sa servisima drugih firmi u svrhu automatizovane nabavke SMD čipova ili drugih sirovina. Ovaj servis komunicira sa Warehouse servisom kako bi ažurirao stanje proizvoda koji su nabavljeni.
- Logistics Department
  Ima zadatak da na osnovu poručenih proizvoda koje dobija od Sales i/ili Web store servisa “odluči” na koji način će obezbediti sve potrebne sirovine za proizvodnju. Prvo, komunicira sa Warehouse-om kako bi saznao kojim sirovinama organizacija trenutno raspolaže. Nalaže HW procurement servisu da nabavi sirovine koje nedostaju. Komunicira sa HW assembly servisom koji treba da proizvede.
- R&D HW design and verification
  Sektor koji se bavi dizajniranjem i osmišljavanjem novih PCB ploča koje firma planira da ubaci u proizvodnju. U stalnom je kontaktu sa R&D SW dev servisom kako bi se napravio funkcionalan model ploče. Takođe, vrši proveru funkcionalnosti (verifikaciju) svih napravljenih ploča. Kontaktira IT sektor sa zahtjevima za dostavljanje potrebnih resursa (build/render serveri, nabavka alata potrebnih za istraćivanje i razvoj, itd.)
- R&D SW dev (firmware...)
  Sektor u kome su zaposleni programeri zaduženi za razvoj i održavanje firmware-a koji se ugrađuje u PCB ploče. Stalno komunicira sa R&D HW design and verification sektorom oko uspostavljanja zahteva koji se mogu implementirati. Kontaktira IT sektor sa zahtjevima za dostavljanje potrebnih resursa (build serveri, nabavka alata potrebnih za istraćivanje i razvoj, itd.)
- SW dev (web store, presentation, contact, B2B API)
  Predstavlja sektor koji obuhvata developere čiji je zadatak razvijanje i održavanje Web Shop-a koji nudi raspoložive proizvode firme (obično podrazumijeva maloprodaju). Razvijaju mehanizam za stupanje u kontakt sa Sales sektorom firme radi uspostavljanja inicijalne saradnje i definisanja ugovora sa drugim firmama. Razvijaju B2B (Business to business) interfejs (API) zarad obavljanja specifičnih većih poslovnih transakcija sa drugim organizacijama sa kojima je već definisan poslovni odnos (pokriveni slučajevi ugovorom o saradnji, te se tako

preskače korak ponovnog pregovaranja sa Sales sektorom). B2B API ima četiri slučaja korišćenja, i to su: dodatna nabavka već postojećih ploča, potraživanje update-a softvera (firmware) neke hardverske komponente, zahtev za izradu nove komponente koja je unapred dizajnirana (isključiva PCBA usluga), i zahtev za osmišljavanje i izradu "custom" komponente za šta se angažuje R&D sekcija firme, a nakon toga se i proizvodi data ploča (PCBA) u zahtevanoj količini.
Kontaktira IT sektor sa zahtevima za dostavljanje potrebnih resursa (hosting servisa, itd.)

- Sales

  Sektor koji definiše poslovne odnose sa drugim firmama. Omogućava novim klijentima upotrebu B2B API-a koji služi za obavljanje svih kompleksnijih ili repetitivnih usluga koje pruža firma. U slučajevima one-time nabavke proizvoda koji su već u ponudi firme, zahtev se prosljedjuje direktno sektoru za logistiku (fabrici).
- IT

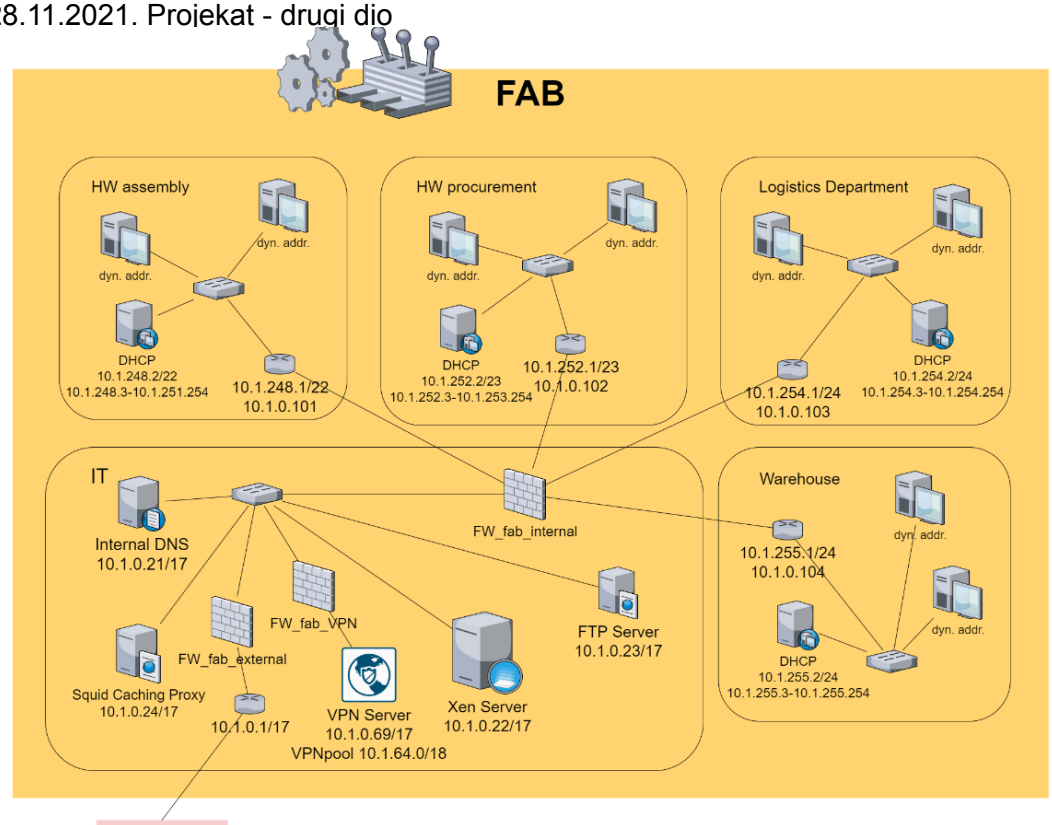
  Omogućava funkcionisanje cele IT infrastrukture koja je potrebna za normalno funkcionisanje svih drugih sektora u firmi. To obuhvata konfiguraciju mreže, hosting servisa za eksternu komunikaciju, hosting internih servisa kao i obezbeđivanje resursa potrebnih za rad R&D setora (build i rendering serveri...). Takođe se brine o bezbednosti infrastrukture celokupnog sistema.
- Management
  - is on vacation.

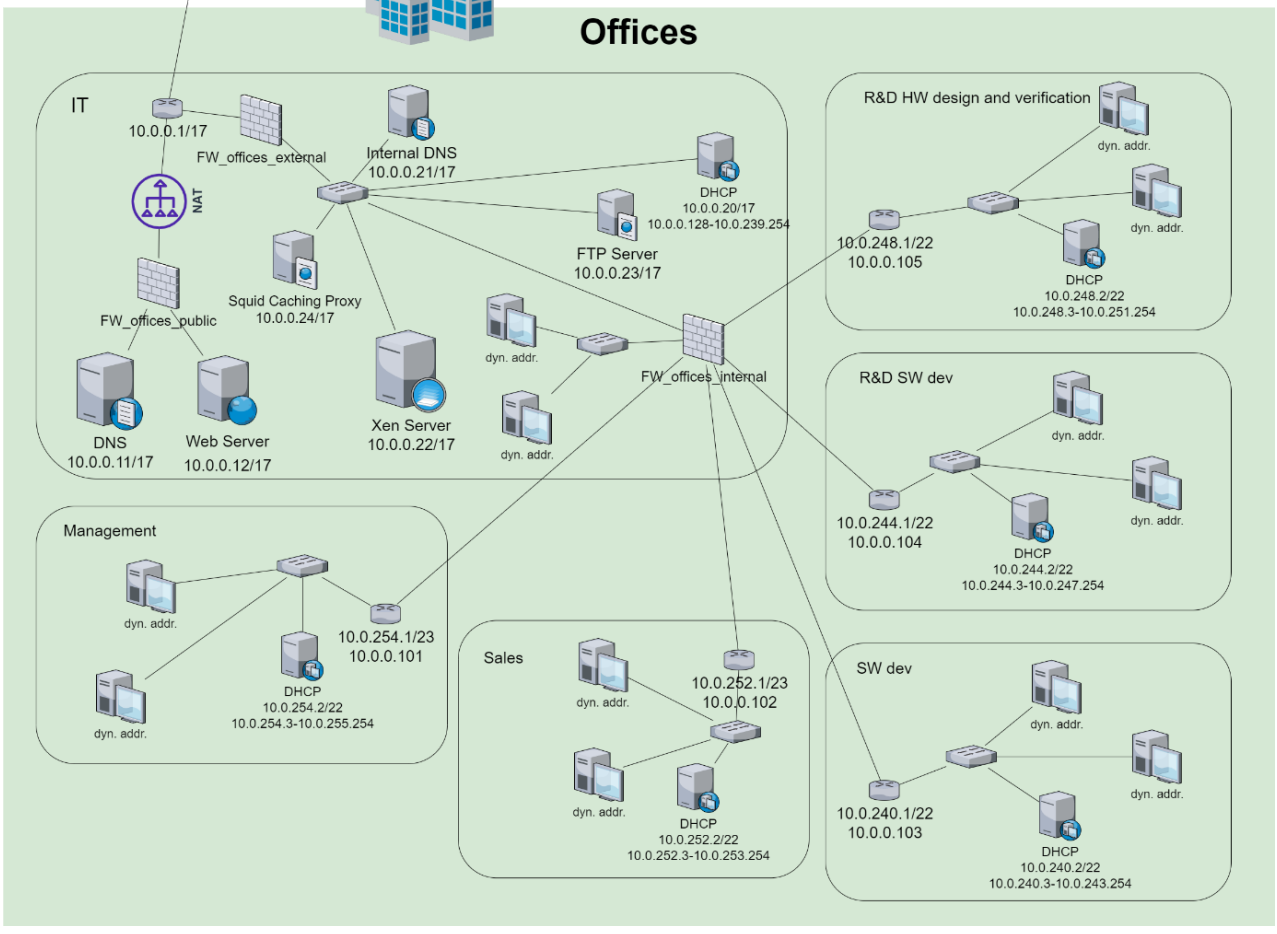
28.11.2021. Projekat - drugi dio

Proširenja u odnosu na napisano za prvi dio projekta:

- Za potrebe optimizacije/smanjenja korištenja protoka sa eksternim svijetom se koristi proxy server sa omogućenim keširanjem - Squid Caching Proxy
- Kako su "fabrika" i "kancelarije" zamišljene kao fizički odvojene lokacije, za pristup internim servisima i mrežnoj infrastrukturi se koristi Virtual Private Network (na slici označeno sa VPN Server elementom u FAB dijelu)
- Svi interni servisi, build/render serveri, kanali komunikacije između sektora itd. se hostuju na serverima sa Xen hypervisor arhitekturom (na slici dvije instance označene kao Xen Server)

28.11.2021. Projekat - drugi dio





Embedded Corporation

2.12.2021. Projekat - treći dio

Najnovija (izmijenjena) arhitektura mreže je prikazana na slici u dijelu dva (stara slika je izbačena).

Prepravke u odnosu na drugi dio projekta:

- Izbačeno nepotrebno nizanje rutera u IT sektorima (i u FAB i u Offices),
- IT unutar FAB se računa kao proširenje IT Offices sektora,
- Ispravno pozicionirane Squid proxy instance u mreži.

Za sve klijentske uređaje (radne stanice), autokonfigurisane tabele rutiranja će dati punu funkcionalnost. Ispod su prikazane tabele rutiranja za sve rutere koji postoje u mreži.

HW assembly

10.1.248.1	255.255.252.0	0.0.0.0	gbiteth0
10.1.0.101	255.255.128.0	0.0.0.0	gbiteth1
10.1.252.1	255.255.254.0	10.1.0.102	
10.1.254.1	255.255.255.0	10.1.0.103	
10.1.255.1	255.255.255.0	10.1.0.104	
0.0.0.0	0.0.0.0	10.1.0.1	

HW procurement

10.1.252.1	255.255.254.0	0.0.0.0	gbiteth0
10.1.0.102	255.255.128.0	0.0.0.0	gbiteth1
10.1.248.1	255.255.252.0	10.1.0.101	
10.1.254.1	255.255.255.0	10.1.0.103	
10.1.255.1	255.255.255.0	10.1.0.104	
0.0.0.0	0.0.0.0	10.1.0.1	

Logistics Department

10.1.254.1	255.255.255.0	0.0.0.0	gbiteth0
10.1.0.103	255.255.128.0	0.0.0.0	gbiteth1
10.1.248.1	255.255.252.0	10.1.0.101	
10.1.252.1	255.255.254.0	10.1.0.102	
10.1.255.1	255.255.255.0	10.1.0.104	
0.0.0.0	0.0.0.0	10.1.0.1	

Warehouse

10.1.255.1	255.255.255.0	0.0.0.0	gbiteth0
10.1.0.104	255.255.128.0	0.0.0.0	gbiteth1
10.1.248.1	255.255.252.0	10.1.0.101	
10.1.252.1	255.255.254.0	10.1.0.102	
10.1.254.1	255.255.255.0	10.1.0.103	
0.0.0.0	0.0.0.0	10.1.0.1	

FAB - IT

10.1.0.1	255.255.128.0	0.0.0.0	gbiteth0
10.1.248.1	255.255.252.0	10.1.0.101	
10.1.252.1	255.255.254.0	10.1.0.102	
10.1.254.1	255.255.255.0	10.1.0.103	
10.1.255.1	255.255.255.0	10.1.0.104	
0.0.0.0	0.0.0.0	upstream	gbiteth1

Management

10.0.254.1	255.255.254.0	0.0.0.0	gbiteth0
10.0.0.101	255.255.128.0	0.0.0.0	gbiteth1
10.0.252.1	255.255.254.0	10.0.0.102	
10.0.240.1	255.255.252.0	10.0.0.103	
10.0.244.1	255.255.252.0	10.0.0.104	
10.0.248.1	255.255.252.0	10.0.0.105	
0.0.0.0	0.0.0.0	10.0.0.1	

Sales

10.0.252.1	255.255.254.0	0.0.0.0	gbiteth0
10.0.0.102	255.255.128.0	0.0.0.0	gbiteth1
10.0.240.1	255.255.252.0	10.0.0.103	
10.0.244.1	255.255.252.0	10.0.0.104	
10.0.248.1	255.255.252.0	10.0.0.105	
10.0.254.1	255.255.254.0	10.0.0.101	
0.0.0.0	0.0.0.0	10.0.0.1	

SW dev

10.0.240.1	255.255.252.0	0.0.0.0	gbiteth0
10.0.0.103	255.255.128.0	0.0.0.0	gbiteth1
10.0.244.1	255.255.252.0	10.0.0.104	

10.0.248.1	255.255.252.0	10.0.0.105	
10.0.240.1	255.255.252.0	10.0.0.103	
10.0.254.1	255.255.254.0	10.0.0.101	
0.0.0.0	0.0.0.0	10.0.0.1	

R&D SW dev

10.0.244.1	255.255.252.0	0.0.0.0	gbiteth0
10.0.0.104	255.255.128.0	0.0.0.0	gbiteth1
10.0.240.1	255.255.252.0	10.0.0.103	
10.0.248.1	255.255.252.0	10.0.0.105	
10.0.252.1	255.255.254.0	10.0.0.102	
10.0.254.1	255.255.254.0	10.0.0.101	
0.0.0.0	0.0.0.0	10.0.0.1	

R&D HW design and verification

10.0.248.1	255.255.252.0	0.0.0.0	gbiteth0
10.0.0.105	255.255.128.0	0.0.0.0	gbiteth1
10.0.240.1	255.255.252.0	10.0.0.103	
10.0.244.1	255.255.252.0	10.0.0.104	
10.0.252.1	255.255.254.0	10.0.0.102	
10.0.254.1	255.255.254.0	10.0.0.101	
0.0.0.0	0.0.0.0	10.0.0.1	

Offices - IT

10.0.0.1	255.255.128.0	0.0.0.0	gbiteth0
10.0.254.1	255.255.254.0	10.0.0.101	
10.0.252.1	255.255.254.0	10.0.0.102	
10.0.240.1	255.255.252.0	10.0.0.103	
10.0.244.1	255.255.252.0	10.0.0.104	
10.0.248.1	255.255.252.0	10.0.0.105	
0.0.0.0	0.0.0.0	upstream	gbiteth1

17.12.2021. Projekat - četvrti dio

Najnovija (izmijenjena) arhitektura mreže je prikazana na slici u dijelu dva (stara slika je izbačena/zamijenjena).

Prepravke u odnosu na treći dio projekta:

- Dodati “eksterni” firewall-i u Offices i u FAB.

Donešena je odluka da treba izbjegavati podešavanje firewall-a na klijentskim uređajima kad god je to moguće (jeste uvijek :D).

Podrazumijevano podešavanje na svim firewall-ima u cijeloj arhitekturi jeste **DROP ALL**.

FW_offices_public:

- Forward DNS zahtjeva na port 53 za host DNS servera.
- Forward HTTP(S) komunikacije na Web server (portovi 80 i 443).
- SSH i SFTP (port 22 i 23) konekcije ka DNS Serveru i Web Serveru dozvoliti samo sa interne, office mreže (10.0.0.1/16)

FW_offices_external:

- Dozvoliti outgoing HTTP(S), FTP, DNS.
- Dozvoliti outgoing L2TP/IPSec.
- Dozvoliti SSH i SFTP komunikaciju sa DNS Serverom i Web Serverom.

FW_offices_internal:
- Dozvoliti outgoing L2TP/IPSec.
- Dozvoliti outgoing HTTP(S), FTP.
- Dozvoliti Squid Proxy (port 3128).
- ACCEPT ALL za komunikaciju između odgovarajućih interfejsa za R&D sektore i SW dev.
- Dozvoliti incoming SSH za sve (drugi firewall limitira pristup na samo one sa IT porijeklom)

FW_fab_external:
- Dozvoliti outgoing HTTP(S), FTP.
- Dozvoliti incoming L2TP/IPSec.

FW_fab_VPN:
- Dozvoliti outgoing HTTP(S) ka Xen Serveru (10.1.0.22/16).
- Dozvoliti FTP ka FTP Serveru (10.1.0.23/16)
- Dozvoliti SSH prolaz.

FW_fab_internal:
- Dozvoliti outgoing HTTP(S), DNS, FTP.
- Dozvoliti Squid Proxy (port 3128).

Svi mrežni i dijeljeni uređaji kojima je moguće udaljeno upravljanje i konfigurisanje trebaju po mogućnosti da imaju isključene Web interfejse a da koriste SSH protokol za pristup. Ovo je definisano sa ciljem izbjegavanja javne dostupnosti, PWN napada, i većeg attack surface-a na expose-ovanim servisima.

Sigurnosna politika kompanije za SSH je:

PasswordAuthentication no
PubkeyAuthentication yes

6.1.2022. Projekat - simulacija

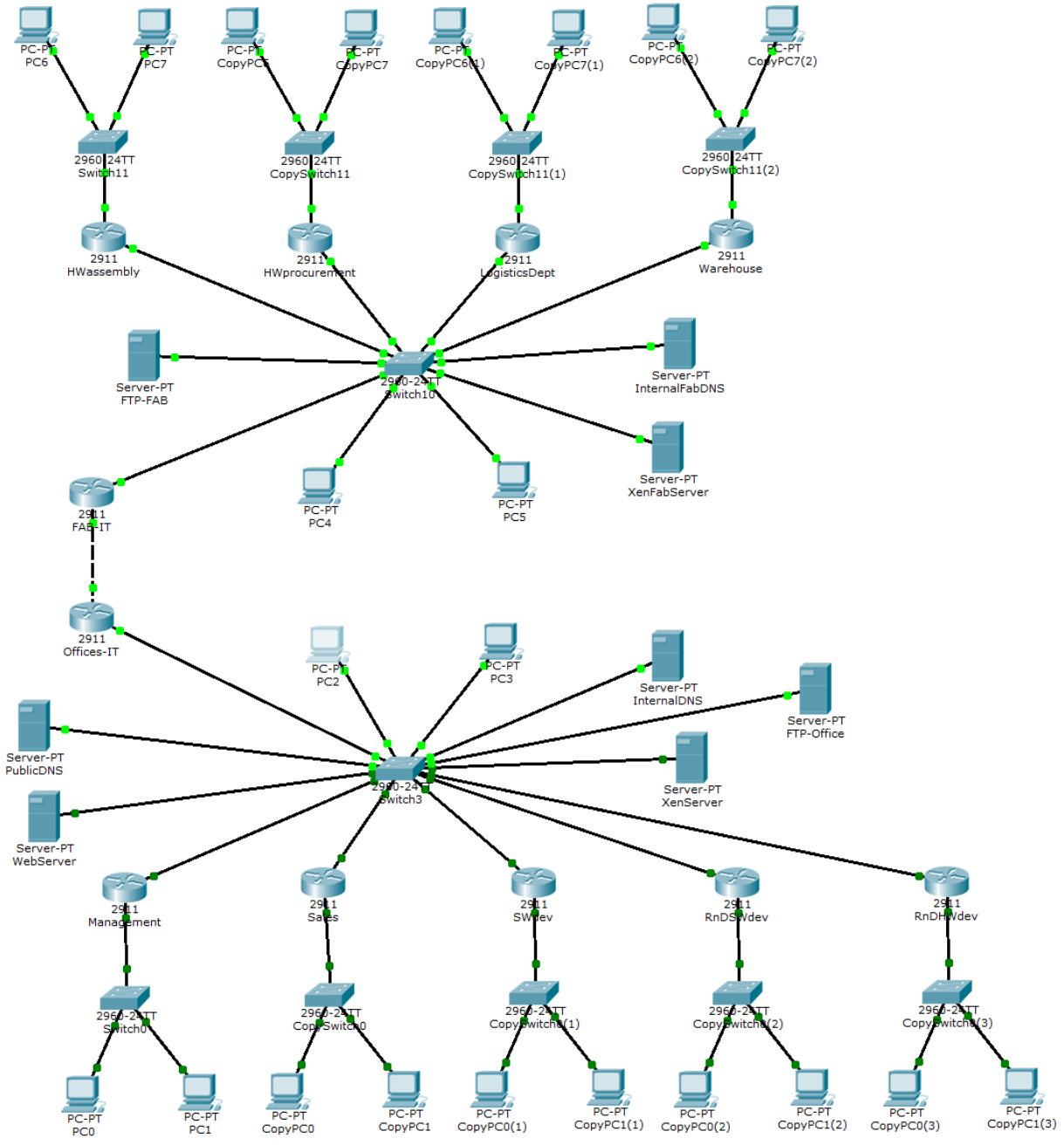
Najnovija (izmijenjena) arhitektura mreže je prikazana na slici u dijelu dva (stara slika je izbačena/zamijenjena).

Prepravke u odnosu na prethodne dijelove projekta:
- Na Office i FAB ruterima je promijenjena maska sa /16 na /17, da bi se izbjegao overlapping mreža.
- Tabele rutiranja su prepravljene u skladu sa prethodnim tačkama.

Za potrebe simulacije u Cisco Packet Tracer-u, napravljene su sledeće izmjene u odnosu na ranije predstavljen u arhitekturu:

- DHCP serveri su implementirani na ruterima na ne kao odvojeni uređaji na mrežama.
- Firewall-i nisu diskretni uređaji, već su pravila implementirana na interfejsima rutera.
- Xen server je predstavljen prostim HTTP(S) serverom.
- Sigurnosna politika - autentifikacija isključivo sa javnim ključevima nije ispoštovana jer studentska verzija CPT-a nema najnoviji firmware za seriju sutera c19xx.
- VPN server je implementiran na FAB ruteru a ne kao diskretni uređaj.
- Internet (zona između Office i FAB rutera), je implementirana direktnim povezivanjem rutera, ali bez default gateway rute na obje strane i upotrebom inside NAT-a na oba rutera za njihove unutrašnje mreže.
- Nije postojala mogućnost simuliranja proxy-ja.

Simulacija (pkt fajl) je dostupna na sledećem link-u. Topologija se može vidjeti na sljedećoj slici.



DHCP (primjer):
(config mode)
ip dhcp excluded-address 10.0.0.1 10.0.0.128
ip dhcp pool MY_LAN
network 10.0.0.1 255.255.128.0
default-router 10.0.0.1
dns-server 10.0.0.21

Rutiranje (primjer):
(config mode)
ip route 10.0.254.0 255.255.254.0 10.0.0.101
ip route 10.0.252.0 255.255.254.0 10.0.0.102
ip route 10.0.240.0 255.255.252.0 10.0.0.103
ip route 10.0.244.0 255.255.252.0 10.0.0.104
ip route 10.0.248.0 255.255.252.0 10.0.0.105
ip route 0.0.0.0 0.0.0.0 10.0.0.1
ip routing

ip route 10.1.248.0 255.255.252.0 10.1.0.101
ip route 10.1.252.0 255.255.254.0 10.1.0.102
ip route 10.1.254.0 255.255.255.0 10.1.0.103
ip route 10.1.255.0 255.255.255.0 10.1.0.104
ip route 0.0.0.0 0.0.0.0 10.1.0.1
ip routing

NAT(FAB, Offices):
(config mode)
ip nat pool net-1 1.0.0.2 1.0.0.2 netmask 255.0.0.0
access-list 100 deny ip 10.1.0.0 0.0.255.255 10.1.64.0 0.0.63.255
access-list 100 permit ip 10.1.0.0 0.0.63.255 any
access-list 100 permit ip 10.1.128.0 0.0.127.255 any
access-list 100 permit ip 10.1.64.0 0.0.63.255 any
ip nat inside source list 100 pool net-1 overload
(inteface 0/0)
ip nat inside
(inteface 0/1)
ip nat outside

(config mode)
ip nat pool net-0 1.0.0.1 1.0.0.1 netmask 255.0.0.0
access-list 1 permit 10.0.0.0 0.0.255.255
ip nat inside source list 1 interface gigabitEthernet 0/1 overload

(inteface 0/0)
ip nat inside
(inteface 0/1)
ip nat outside

(config mode)
ip nat inside source static tcp 10.0.0.12 80 1.0.0.1 80
ip nat inside source static tcp 10.0.0.12 443 1.0.0.1 443
ip nat inside source static udp 10.0.0.11 53 1.0.0.1 53

VPN (FAB external router):
(config mode)
license boot module c2900 technology-package securityk9
(save and reload)
ip local pool VPN 10.1.64.0 10.1.127.255
aaa new-model
aaa authentication login UserVPN local
aaa authorization network GroupVPN local
username uservpn secret ciscovpn
crypto isakmp policy 100
(isakmp config)
encryption aes 256
hash sha
authentication pre-share
group 5
lifetime 3600
exit
(config mode)
crypto isakmp client configuration group GroupVPN
(isakmp group config)
key ciscogroupvpn
pool VPN
exit
(config mode)
crypto ipsec transform-set SetVPN esp-aes esp-sha-hmac
crypto dynamic-map DynamicVPN 100
(crypto map config)
set transform-set SetVPN
reverse-route
exit
(config mode)
crypto map StaticMap client configuration address respond
crypto map StaticMap client authentication list UserVPN
crypto map StaticMap isakmp authorization list GroupVPN

crypto map StaticMap 20 ipsec-isakmp dynamic DynamicVPN
(external interface config)
crypto map StaticMap

SSH (serveri, na ruterima):
license boot module c2900 technology-package securityk9
copy run start
ip domain-name office.it.ec.rs
crypto key generate rsa
2048
ip ssh version 2
line vty 0 4
transport input ssh
exit
username cisco password cisco
enable password root
Napomena: studentska verzija Cisco Packet Tracera nema u ponudi ruter koji omogucava pubkey servere!? Koristena serija rutera u ovom projektu je c19xx.

Firewall-i:

IT Offices router:

```
access-list 114 permit tcp any any eq 80
access-list 114 permit tcp any any eq 443
access-list 114 permit udp any any eq 53
access-list 114 permit udp any any eq 21
access-list 114 permit udp any any eq 500
access-list 114 permit udp any any eq 4500
access-list 114 permit tcp any any gt 1024
access-list 114 permit udp any any gt 1024
access-list 113 deny tcp any host 1.0.0.1 eq 22
access-list 113 permit ip any any
int g 0/1
ip access-group 114 out
ip access-group 113 in
```

IT FAB router:

```
access-list 114 permit tcp any any eq 80
access-list 114 permit tcp any any eq 443
access-list 114 permit udp any any eq 53
access-list 114 permit udp any any eq 21
access-list 114 deny ip any any
access-list 113 deny tcp any host 1.0.0.2 eq 22
access-list 113 permit ip any any
int g 0/1
ip access-group 114 out
ip access-group 113 in
```

Zajednicka podasavanja za preostale rutere:

```
access-list 111 permit udp any eq bootpc any eq bootps
access-list 111 permit tcp any any eq 80
access-list 111 permit tcp any any eq 443
access-list 111 permit tcp any any eq 21
access-list 111 permit udp any any eq 53
interface gigabitEthernet 0/0
ip access-group 111 in
exit
access-list 113 permit tcp any any gt 1024
```

access-list 113 permit udp any any gt 1024
interface gigabitEthernet 0/1
ip access-group 113 in
exit

Management router:

access-list 113 permit tcp 10.0.0.0 0.0.127.255 host 10.0.0.101 eq 22
access-list 111 deny tcp any host 10.0.0.1 eq 22

Sales router:

access-list 111 permit udp any any eq 500
access-list 113 permit udp any eq 500 any
access-list 111 permit udp any any eq 4500
access-list 113 permit udp any any eq 4500
access-list 113 permit tcp 10.0.0.0 0.0.127.255 host 10.0.0.102 eq 22
access-list 111 deny tcp any host 10.0.0.1 eq 22

SW Dev:

access-list 111 permit udp any any eq 500
access-list 113 permit udp any eq 500 any
access-list 111 permit udp any any eq 4500
access-list 113 permit udp any any eq 4500
access-list 113 permit tcp 10.0.0.0 0.0.127.255 host 10.0.0.103 eq 22
access-list 111 deny tcp any host 10.0.0.1 eq 22

R&D SW Dev router:

access-list 111 permit ip any 10.0.248.0 0.0.3.255
access-list 113 permit ip 10.0.248.0 0.0.3.255 any
access-list 113 permit tcp 10.0.0.0 0.0.127.255 host 10.0.0.104 eq 22
access-list 111 deny tcp any host 10.0.0.1 eq 22

R&D HW router:

access-list 111 permit ip any 10.0.244.0 0.0.3.255
access-list 113 permit tcp 10.0.0.0 0.0.127.255 host 10.0.0.105 eq 22
access-list 111 deny tcp any host 10.0.0.1 eq 22

Warehouse router:

access-list 113 permit tcp 10.1.0.0 0.0.127.255 host 10.1.0.104 eq 22
access-list 111 deny tcp any host 10.1.0.1 eq 22

HW Assembly router:

access-list 113 permit tcp 10.1.0.0 0.0.127.255 host 10.1.0.101 eq 22
access-list 111 deny tcp any host 10.1.0.1 eq 22

HW Procurement router:

access-list 113 permit tcp 10.1.0.0 0.0.127.255 host 10.1.0.102 eq 22
access-list 111 deny tcp any host 10.1.0.1 eq 22

Logistics router:

access-list 113 permit tcp 10.1.0.0 0.0.127.255 host 10.1.0.103 eq 22
access-list 111 deny tcp any host 10.1.0.1 eq 22

Projekat radili:

Igor Šikuljak E2 78/2021
Andrej Hložan E2 80/2021
Radoš Milićev E2 88/2021