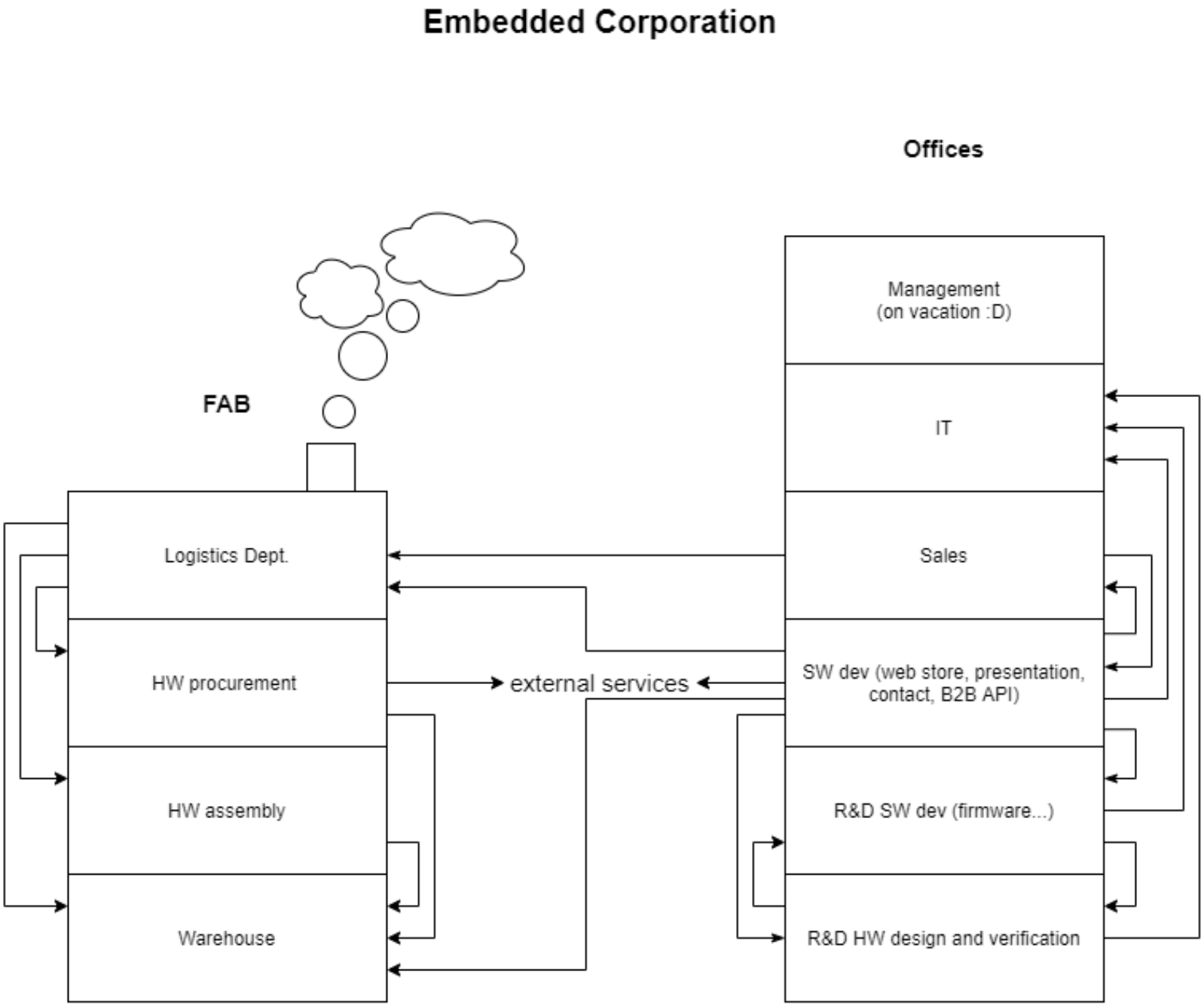
14.11.2021. Projekat - prvi dio



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

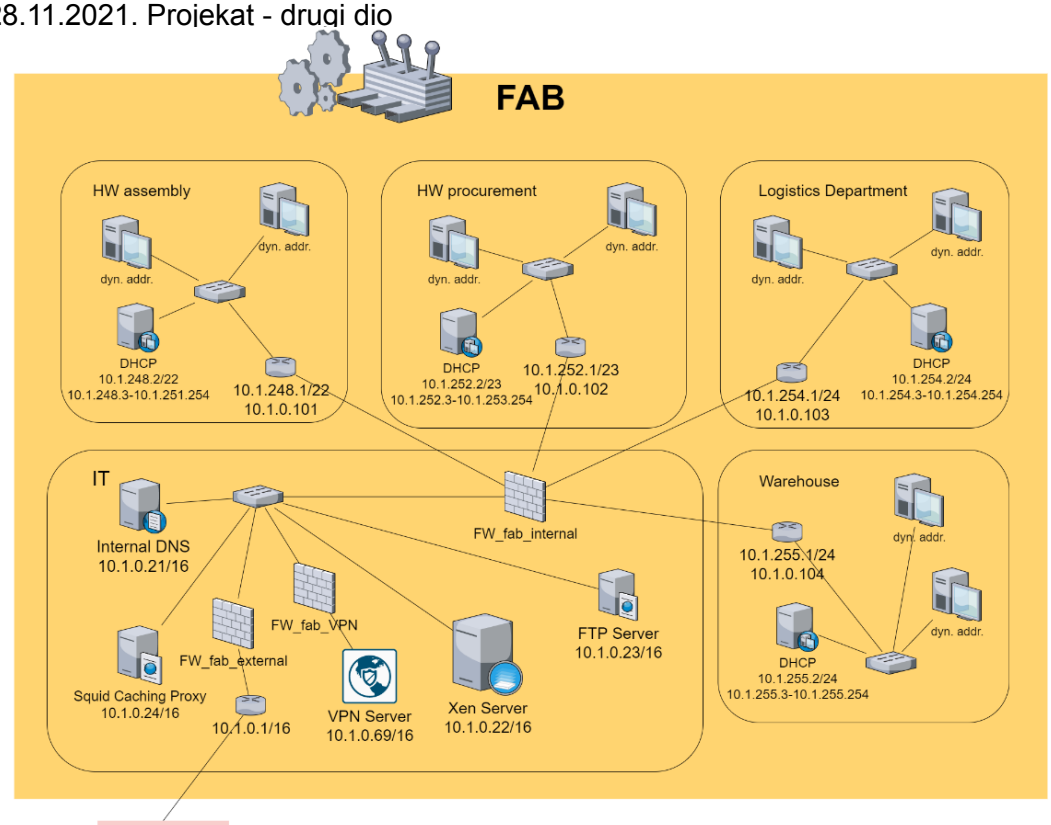
  Omogućava funkcionisanje cele IT infrastrukture koja je potrebna za normalno funkcionisanje svih drugih sektora u firmi. To obuhvata konfiguraciju mreže, hosting servisa za eksternu komunikaciju, hosting internih servisa kao i obezbeđivanje resursa potrebnih za rad R&D setora (build i rendering serveri...).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

28.11.2021. Projekat - drugi dio

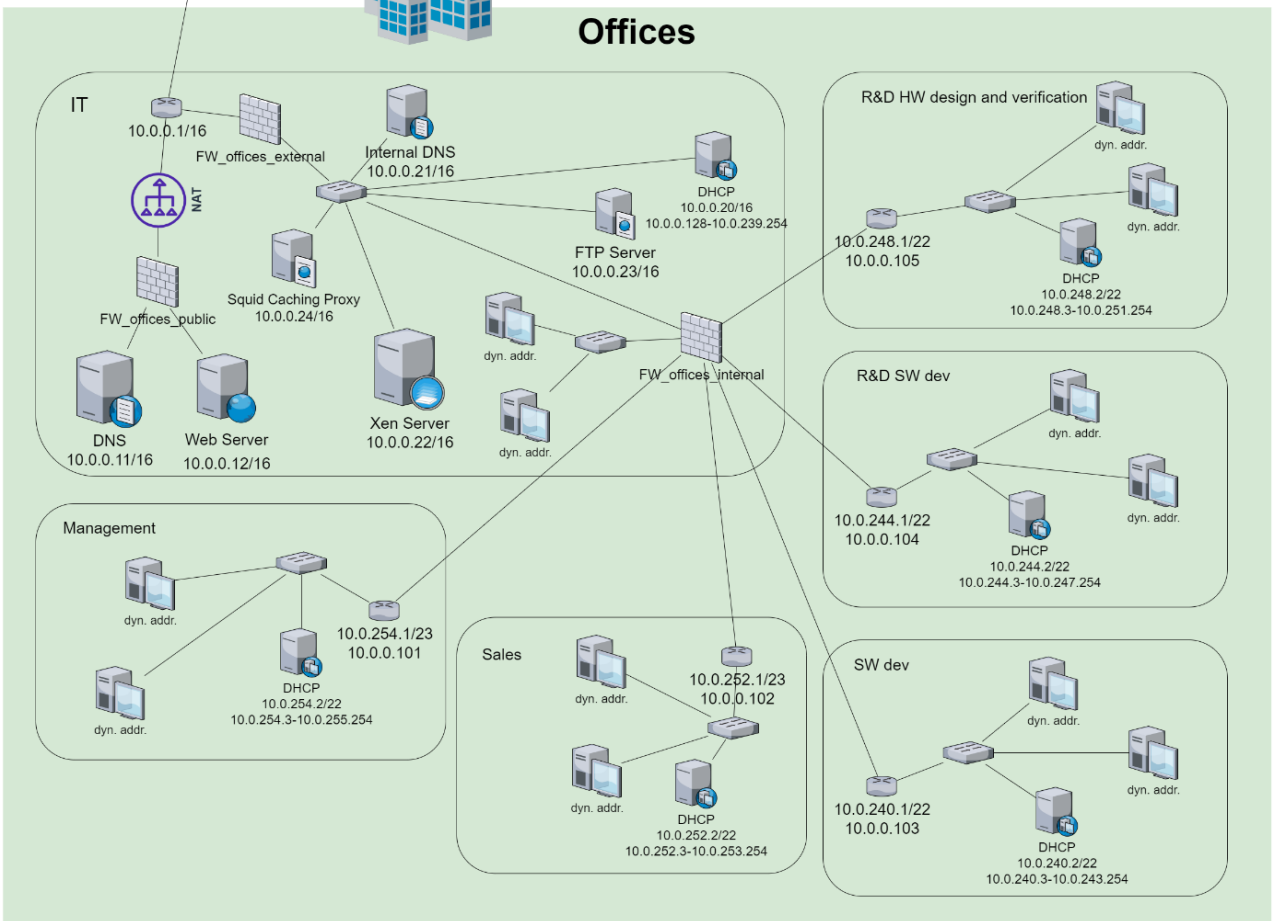
Proširenja u odnosu na napisano za prvi dio projekta:

- 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	gbiteth1
10.1.0.101	255.255.0.0	0.0.0.0	gbiteth0
0.0.0.0	0.0.0.0	10.1.0.1	gbiteth0

HW procurement

10.1.252.1	255.255.254.0	0.0.0.0	gbiteth1
10.1.0.102	255.255.0.0	0.0.0.0	gbiteth0
0.0.0.0	0.0.0.0	10.1.0.1	gbiteth0

Logistics Department

10.1.254.1	255.255.255.0	0.0.0.0	gbiteth1
10.1.0.103	255.255.0.0	0.0.0.0	gbiteth0
0.0.0.0	0.0.0.0	10.1.0.1	gbiteth0

Warehouse

10.1.255.1	255.255.255.0	0.0.0.0	gbiteth1
10.1.0.104	255.255.0.0	0.0.0.0	gbiteth0
0.0.0.0	0.0.0.0	10.1.0.1	gbiteth0

Management

10.0.254.1	255.255.254.0	0.0.0.0	gbiteth1
10.0.0.101	255.255.0.0	0.0.0.0	gbiteth0
0.0.0.0	0.0.0.0	10.0.0.1	gbiteth0

Sales

10.0.252.1	255.255.254.0	0.0.0.0	gbiteth1
10.0.0.102	255.255.0.0	0.0.0.0	gbiteth0
0.0.0.0	0.0.0.0	10.0.0.1	gbiteth0

SW dev

10.0.240.1	255.255.252.0	0.0.0.0	gbiteth1
10.0.0.103	255.255.0.0	0.0.0.0	gbiteth0
0.0.0.0	0.0.0.0	10.0.0.1	gbiteth0

R&D SW dev

10.0.244.1	255.255.252.0	0.0.0.0	gbiteth1
10.0.0.104	255.255.0.0	0.0.0.0	gbiteth0
0.0.0.0	0.0.0.0	10.0.0.1	gbiteth0

R&D HW design and verification

10.0.248.1	255.255.252.0	0.0.0.0	gbiteth1
10.0.0.105	255.255.0.0	0.0.0.0	gbiteth0
0.0.0.0	0.0.0.0	10.0.0.1	gbiteth0

FAB - IT

10.1.0.1	255.255.0.0	0.0.0.0	gbiteth1
10.1.248.1	255.255.252.0	10.1.0.101	gbiteth1
10.1.252.1	255.255.254.0	10.1.0.102	gbiteth1
10.1.254.1	255.255.255.0	10.1.0.103	gbiteth1
10.1.255.1	255.255.255.0	10.1.0.104	gbiteth1
0.0.0.0	0.0.0.0	upstream	gbiteth0

Offices - IT

10.0.0.1	255.255.0.0	0.0.0.0	gbiteth1
10.0.254.1	255.255.254.0	10.0.0.101	gbiteth1
10.0.252.1	255.255.254.0	10.0.0.102	gbiteth1
10.0.240.1	255.255.252.0	10.0.0.103	gbiteth1
10.0.244.1	255.255.252.0	10.0.0.104	gbiteth1
10.0.248.1	255.255.252.0	10.0.0.105	gbiteth1
0.0.0.0	0.0.0.0	upstream	gbiteth0

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)
- Dozvoliti

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

Projekat radili:

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