# Request for Information (RFI)

# Email Security Appliance

# Sadržaj

# 1 Uvod

## 1.1 Ciljevi

Cilj ovog dokumenta je prikupljanje informacija za budući razvoj sigurnosti email sistema BH Telecoma za period od 2023.-2026. godine. BH Telecom pruža usluge email hostinga duži niz godina za fizička i pravna lica. Također, BH Telecom koristi mail security rješenja za osiguranje mail prometa korporativne mreže BH Telecoma.

## 1.2 Ciljana publika

Ovaj dokument je namijenjen kompanijama koje su vendori ili intergatori Email Security rješenja. Rješenja koja nisu implementirana u okruženjima sa minimalno 50.000 mailbox-ova u Evropi ili Sjevernoj Americi neće biti uzeta u razmatranje.

## 1.3 Terminologija

DKIM - Domain Keys Identified Mail
DNS – Domain Name Server
ESA – Email Security Appliance
HAT – Host Access Table
LB – Load Balancer
LDAP – Lightweight Directory Access Protocol
MTA – Mail Transfer Agent
MX – Mail Exchange
RAT – Recipient Access Table
SBRS – Sender Base Reputation Score
SMA – Security Management Appliance
SMTP – Simple Mail Transfer Protocol
SPF - Sender Policy Framework
S/MIME - Secure/Multipurpose internet Mail Extensions

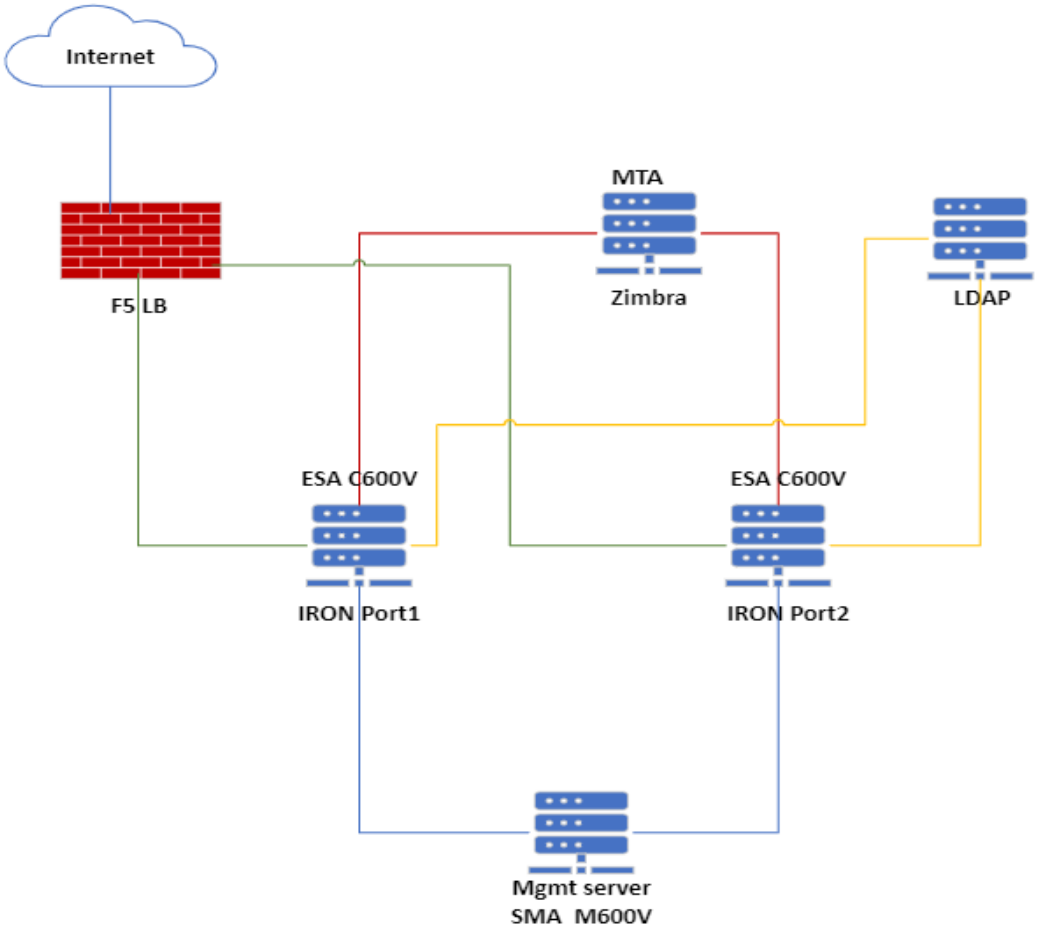
# 2 Arhitektura postojećeg rješenja

## 2.1 Karakteristike postojeće arhitekture

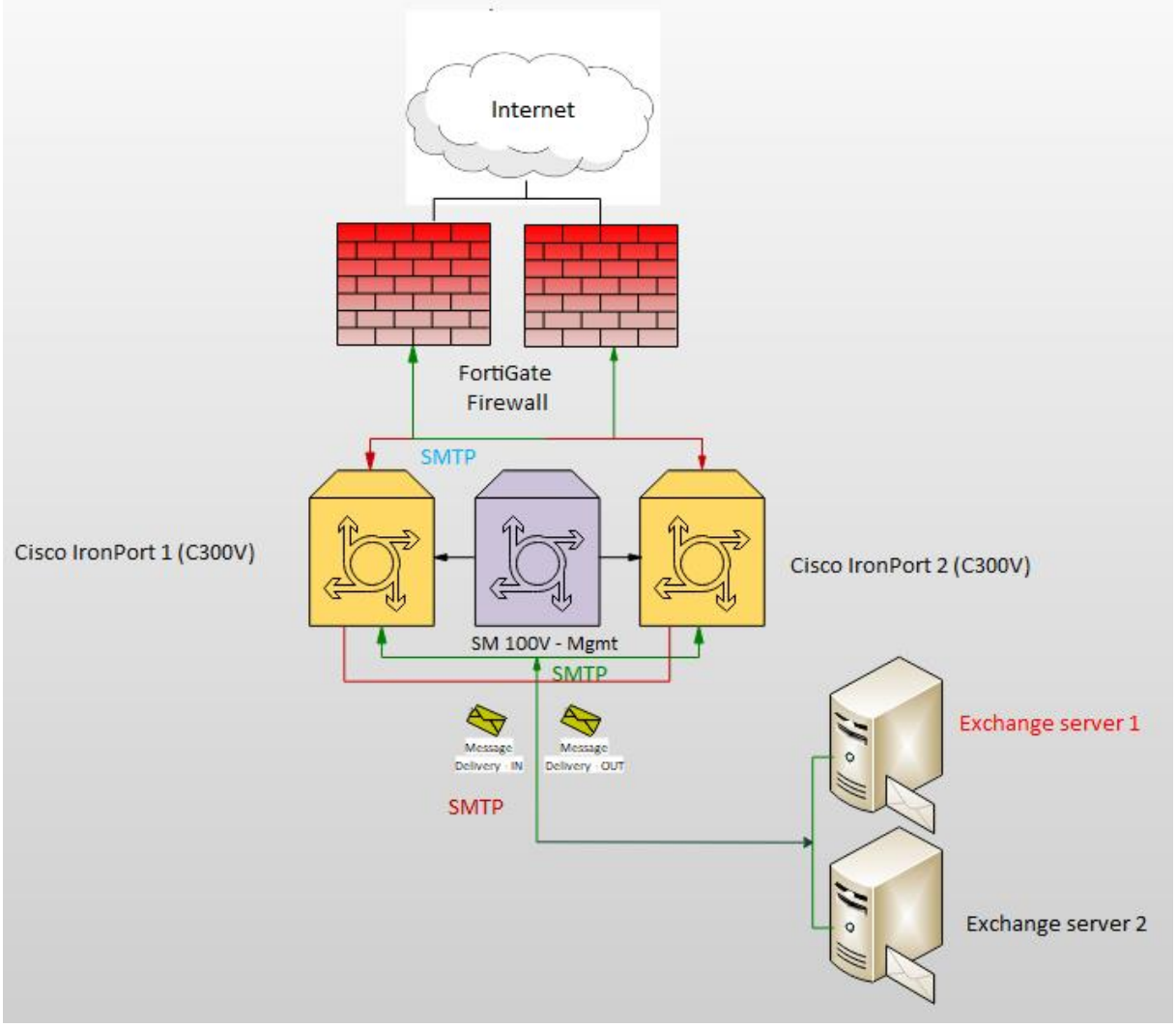
BH Telecom trenutno posjeduje 5 Email Security Appliance-a (ESA) i dva Security Management Server (SMA) proizvođača Cisco. Navedeni elementi se koriste na slijedeći način. Jedan ESA element se koristi u standalone režimu. Ostali elementi su konfigurisani na način da su od po dva ESA elementa kreirana po dva clustera gdje se svaki cluster nadgleda i upravlja od strane jednog od SMA elementa. Na slikama broj 1 i 2 prikazane su logičke scheme opisanih clustera sa pripadajućim SMA elementom.

Postojeći sistem se koristi za mail komunikaciju domena @bih.net.ba, @bhtelecom.ba i hosting domena korisnika Hosting usluge BH Telecoma. MX zapisi za domene @bih.net.ba i hosting domene pokazuju na hostname-e mail01-1.bih.net.ba i mail02-1.bih.net.ba odnosno na IP adrese 80.65.86.245 i 80.65.86.246 respektivno koje su mapirane na mail security rješenje. MX zapis za domenu @bhtelecom.ba pokazuje na hostname-e mail01.bhtelecom.ba i mail02.bhtelecom.ba odnosno na adrese 195.222.61.253 i 195.222.61.254 respektivno koje su mapirane na drugi dio sistema mail security arhitekture za potrebe ove domene. Također, za potrebe klijentskog slanja maila za domenu @bih.net.ba i hosting domene koristi se opisano mail security rješenje gdje se u konfiguraciji outgoing mail servera koriste slijedeći hostname-ovi ssl.bih.net.ba, smtp.bih.net.ba, out.mail.bih.net.ba koji

pokazuju na IP adresu 80.65.86.251 te smtpgold.bih.net.ba koji pokazuje na mail adresu 80.65.86.247. Pored navedenog, mail security sistem posjeduje mogućnost kreiranje većeg broja interface, a posljedično i većeg broja listenera što otvara mogućnosti segmentacije korisnika po načinu na koji je dozvoljeno slanje mailova. Dodatno, mail security sistem koristi veći broj interface za slanje odlaznih mailova čime se stiče dodatna kontrola odlaznog saobraćaja, segmentacije korisnika i reputacije IP adresa koje se koriste za slanje maila. Na slikama u nastavku prikazane su pojednostavljene scheme mail arhitekture koja se štiti postojećim email security rješenjem




*Slika 1 Schema Mail Security rješenja za @bih.net.ba i hosting domene*




*Slika 2 Schema Mail Security rješenja na internoj @bhtelecom.ba domeni*

Navedene mašine su instalirane na Vmware virtualnoj platformi. U tabeli 1 prikazane su specifikacije navedenih mašina:

| Tip mašine | CPU | RAM (GB) | HDD (GB) | OS |
|---|---|---|---|---|
| SMA M600V | 8 | 8 | 2000 | AsyncOS 14.2.0-203 |
| ESA C600V | 8 | 8 | 500 | AsyncOS 14.2.0-620 |
| ESA C600V | 8 | 8 | 500 | AsyncOS 14.2.0-620 |
| SMA M100V | 2 | 8 | 250 | AsyncOS 13.6.2 |
| ESA C300V | 4 | 8 | 500 | AsyncOS 13.0.4 |
| ESA C300V | 4 | 8 | 500 | AsyncOS 13.0.4 |
| ESA C100V | 2 | 6 | 200 | AsyncOS 8.5.7-042 |

*Tabela 1 Specifikacije mašina*

## 2.2 Funkcionalnosti postojećeg sistema

### 2.2.1 Mrežni interface

Postojeći sistem oslanja se na virtualizacijsku platformu na kojoj su instalirane virtualne mašine odgovarajuće namjene (Security appliance, Management appliance). Na svim čvorovima postojećeg rješenja moguće je dodati veći broj mrežnih interface. Dodatno, moguće je kreirati veći broj interface u istom subnetu čime se otvara mogućnost segmentacije korisnika u dolaznom i odlaznom saobraćaju te redudancija u radu servisa.

### 2.2.2 Listeneri

Postojeći sistem posjeduje funkcionalnosti kreiranja listenera na kojem je startan smtp servis za potrebe prijema maila. Kroz kreiranje listenera određuje se da li se radi o javnim ili privatnim listenerima u smislu da li su namijenjeni za dolazni ili odlazni mail. Upotrebom i definisanjem HAT (*Host Access Table)* i RAT (*Recipient Address Table)* postiže se upravljanje listenerima u smislu saobraćaja koji će biti primljen i obrađen od strane ESA-e.

### 2.2.3 Antispam i antivirus

Svi dolazni i odlazni mailovi se skeniraju s ciljem utvrđivanja spam saobraćaja i potencijalnog saobraćaja koji može sadržavati viruse. Za potrebe skeniranja virusa u mailovima koji prolaze kroz mail security rješenje koristi se Sophos antivurs engine gdje se antivirusne politike dodatno uređuju od strane mail security administratora s ciljem kreiranja potrebnih pragova u donošenju odluka (smanjenje false positive odluka). Što se tiče zaštite od spam saobraćaja, mail security rješenje koristi IronPort Anti-Spam mehanizam ugniježden u mail security rješenje. Kao i za antivirus politiku, moguće je od strane administratora mijenjati kriterije na osnovu kojih se određena email poruka proglašava kao spam.

Navedena podešavanja anti-virus i anti-spam politika moguće je napraviti kroz definisanje Mail politika koje je moguće definisati po željenim pošiljaocima i primaocima poruka te je iste moguće definisati kao mail politike za dolazni i odlazni mail saobraćaj.

### 2.2.4 Content filteri

Slično korištenju anti-virus i anti-spam politika kreirani su i filteri sadržaja (*Content filters)*. Filteri sadržaja rade po principu „If-then“ uslova gdje jedan filter podrazumijeva uparivanje uslova i akcije. U dijelu uslova moguće je odabrati slijedeće:

- Tijelo poruke ili attachment „sadrži“
- URL kategorija
- URL reputacija
- Veličina poruke
- Jezik poruke
- Detekcija makroa
- Sadržaj attachment-a
- Informacija o datoteci u attachment-u
- Zaštita attachment-a
- Zaglavlje subjecta maila
- Ostala zaglavlja
- Sender envelope
- Recipient envelope
- Dolazni listener
- Udaljena IP adresa/Hostname
- Reputacijska vrijednost
- Reputacija domene
- DKIM autentikacija
- Detekcija lažiranog maila
- SPF verifikacija
- S/MIME gateway poruka
- S/MIME gatrway verifikacija
- Verifikacija dupliciranih granica
- Geolokacija

Kada dolazni ili odlazni mail odgovaraju postavljenom uslovu na tako detektovan mail moguće je primjeniti jednu od slijedećih akcija:

- Karantin
- Skidanje attachment-a po sadržaju
- Skidanje attachment-a po informaciji o datoteci
- Skidanje attachment-a koji sadrži macro
- Sigurno printanje
- URL kategorija
- URL reputacija
- Dodavanje disclaimer teksta
- Preskakanje outbreak filter skeniranja

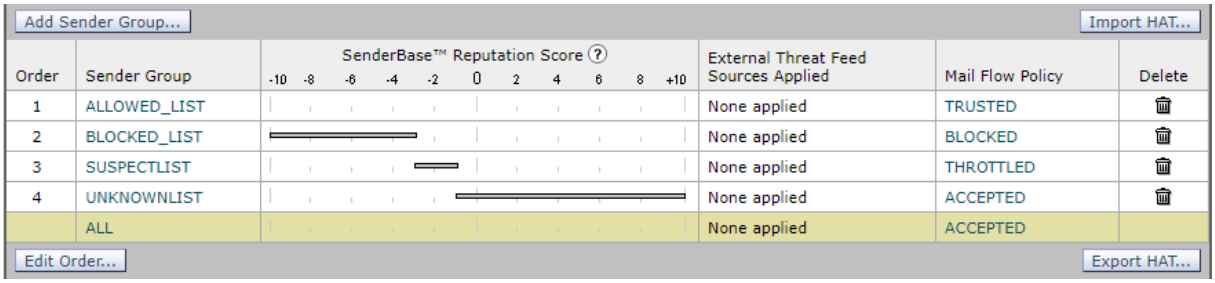
- Preskakanje DKIM potpisivanja
- Slanje kopije (bcc)
- Notifikacija
- Promjena primalaca poruke
- Izmjena destinacijaske IP adrese
- Dostavljanje maila sa specifičnog IP interface-a
- Skiranje zaglavlja
- Dodavanje/izmjena zaglavlja
- Detekcija lažiranog maila
- Dodavanje oznake na poruku
- Upisivanje u log
- S/MIME potpisivanje/enkripcija po dostavi
- Odbijanje maila (bounce – s povratnom informacijom)
- Preskoči ostale filtere
- Odbacivanje maila (bez povratne informacije)

### 2.2.5 LDAP integracija

Mail security sistem, preciznije, ESA node-ovi su povezani sa LDAP serverom za potrebe autentikacije odlaznih mailova kao i za provjeru dolaznih mailova. Radi se o autenticiranoj komunikaciji s openLDAP serverom uz korištenje username i passworda po portu 389. Moguće je kreirati različite LDAP server profile sa različitim queryima poput Accept, Routing, SMTP querya.

### 2.2.6 SRBS reputacija

Postojeći sistem se u velikoj mjeri oslanja na provjeru reputacije IP adrese mail sendera kroz SenderBase reputacijsku bazu. Na osnovu SRBS rezultata donosi se odluka da li se uspostavlja veza na IP nivou. Opisani procesi definišu se kroz HAT i RAT karakteristike listener-a kako je prikazano na slici broj 2.




*Slika 2 HAT (Host Access Table)*

### 2.2.7 Message filteri

Postojeći sistem posjeduje funkcionalnosti message filtera mail poruka. Radi se moćnom alatu koji vrši manipulaciju mailova u trenutku prijem na odgovarajući listener te posjeduje mogućnost upravljanja nastavkom mail toka.

### 2.2.8 Centralizovano izvještavanje

Postojeći sistem organizovan je na način da su kreirana dvije arhitekture koje sačinjavaju dva ESA elementa i jedan SMA element, te od jednog standalone ESA elementa. Kada se govori arhitekturi sa dva ESA elementa i jednim SMA elementom važno je spomenuti opciju centralizovanog izvještavanja.

Centralizovano izvještavanja predstavlja izvještavanja o mail prometu kroz oba ESA elementa s jedne tačke odnosno sa SMA elementa. Na ovaj način postiže se brže i efikasnija analiza mail prometa te posljedično tome efikasniji troubleshooting i otklanjanje problema.

### 2.2.9 Karantin

Postojeće rješenje posjeduje funkcionalnost smještanja mail poruka u karantin. U zavisnosti od uzroka smještanja poruke u karantin razlikuju se slijedeći karantini:

- Spam karantin
- Virus karantin
- Policy karantin
- Outbreak karantin

Svaki karantin ima karantin politiku koja opisuje akcije koje će biti sprovedene nad mailovima koji se nalaze u datom karantinu i u koje vrijeme.

### 2.2.10 Destinacijske kontrole

Postojeće rješenje posjeduje mogućnost postavljanja ograničenja i pravila slanja maila zavisno od odredišne domene. Na ovaj način definišu se paramteri slanja prema određenoj domeni kao što su broj istovremenih sesija, broj poruka po sesiji, broj primalaca u jedinici vremena, korištenje TLS-a i slični parametri.

### 2.2.11 Adresne liste

Postojeće rješenje posjeduje mogućnost kreiranja adresnih listi. Adresne liste predstavljaju spisak mail adresa, domena ili IP adresa za koje se primjenjuje određeni set pravila. Preciznije adresene liste se koriste u slučaju izuzimanja seta korisnika od akcija predefinisanih filterima ili pravilima u mail tokovima.

### 2.2.12 Rječnici (Dictionaries)

Postojeće rješenje posjeduje mogućnost kreiranja rječnika. Rječnik predstavlja spisak domena ili mail adresa koje su objedinjene u jedan logički objekat. Rječnik se koristi u mail toku da se za korisnike (domene, mail adrese) definišu akcije u politikama mail tokova odnosno u filterima sadržaja.

### 2.2.13 Geolokacija

Postojeće rješenje posjeduje mogućnost korištenja geolokacijske informacije IP adrese s koje dolazi mail saobraćaj. Navedena infoormacija pruža mogućnost upravljanja mail prometom s određenog goegrafskog područja.

# 3 Zahtjevi

Sistem mora podržavati funkcionalnosti postojećeg mail security sistema s akcentom na slijedeće karakteristike:

- Ponuđeno rješenje mora biti virtualizirano i prilagođeno za instalaciju na VMware virtualizacijskoj platformi
- Licenca treba da pokriva Email Security arhitekturu u cjelosti.
- Email Security arhitektura nije ograničena brojem komponenti od kojih se sastoji.
- Potrebno je omogućiti mehanizam za licencno pokrivanje novoinstaliranih komponenti Email Security sistema

- Licenca mora podržavati minimalno 30.000 mailboxa ili u slučaju licenciranja po prometu 40.000 dolaznih poruka po satu odnosno 10.000 odlaznih poruka po satu.
- Potrebno je da pripadajuća licenca ima rok validnosti 3 godine.
- Informaciju o reputaciji sender IP adrese dolaznih i odlaznih mailova po ugledu na SenderBase.
- Sistem mora posjedovati mogućnost integracije sa LDAP serverom.
- Mail security rješenje mora ponuditi mogućnosti antispam i antivirus zaštita mail saobraćaja.
- Potrebno je omogućiti izmjenu pragova za donošenje odluke o spam positive i virus positive mailovima.
- Mail security rješenje mora ponuditi mogućnosti kreiranja kantina za spam i drugi neželjeni saobraćaj (costum kantine).
- Sistem mora ponuditi mehanizme za ograničavanje brzine i količine slanja mail poruka (rate control) na nivou listenera.
- Sistem mora ponuditi mehanizme za destination control zavisno od destinacijske domene.
- Potrebno je omogućiti slanje različitih mail poruka preko različitih IP adresa kroz definisanje više interface-a na jednom subnetu ili na neki drugi način.
- Email Security rješenje mora podržavati opciju kreiranja clustera.
- Centralizovano izvještavanje – Uvid u mail saobraćaj na svakom od hostova s centralne konzole, odnosno sa Security Management elementa.



Kantonalni sud Sarajevo **Br. UF/I-520/04** Identifikacioni broj: **4200211100005** Porezni broj: **0107880400** PDV broj: **200211100005**
**Računi BH Telecoma d.d. Sarajevo**
ASA Banka Naša i snažna d.d. Sarajevo, glavni račun BH Telecoma - KM: 1401010007090054; RAIFFEISEN BANK d.d. BiH, KM: 1610000030950092, IBAN: BA39 1611 0000 0124 8933, SWIFT: RZBABA2S; UNICREDIT BANK d.d. Mostar, KM: 3383202250226088, IBAN: BA39 3383 2048 9065 5134, SWIFT: UNCRBA22; NLB BANKA d.d. Sarajevo, KM: 1322600311707003; INTESA SANPAOLO BANKA d.d. BiH, KM: 1540012000318547; SPARKASSE BANK d.d. BiH, KM: 1990490005000203; UNION BANKA d.d. Sarajevo, KM: 1020500000020853; NOVA BANKA a.d. Banja Luka, KM: 5550050047194638; BOSNA BANK INTERNATIONAL d.d. Sarajevo, KM: 1410010000000941; ASA BANKA d.d. Sarajevo, KM: 1340100000160849; PRIVREDNA BANKA SARAJEVO d.d. Sarajevo, KM: 1010000050732105; ZIRAATBANK BH d.d. Sarajevo, KM: 1860001060841009;