PRIMJENA I SPECIFIČNOSTI PROTOKOLA ZA ZAŠTITU DOMENE ELEKTRONIČKE POŠTE

Međeši, Hrvoje

Master's thesis / Specijalistički diplomski stručni

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Algebra University College / Visoko učilište Algebra**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:225:548205

VISOKO UČILIŠTE ALGEBRA

DIPLOMSKI RAD

PRIMJENA I SPECIFIČNOSTI PROTOKOLA ZA ZAŠTITU DOMENE ELEKTRONIČKE POŠTE

Hrvoje Međeši

Zagreb, rujan 2019.

Sažetak

Kroz ovaj rad cilj mi je bio objasniti i prikazati koliko je zapravo razmjena poruka elektroničkom poštom sigurna i koliko bitno može utjecati na korisnike kao i na organizacije. Osim sigurnost, glavni motiv mi je bio i provjeriti sa tehnološkog aspekta koji su sve mehanizmi i protokoli uključeni u cijeli taj proces. Zbog kompleksnosti teme odlučio sam se koristiti sve relevantne protokole električne pošte koji postoje: SMTP, IMAP i POP3 protokol, te istražiti njihove prednosti i mane bitne prilikom konfiguracije i implementacija u odabranom sustavu. Kroz autentikacijske protokole SPF, DKIM i DMARC se određuje na koji način je poruka elektroničke pošte došla od pošiljatelja do primatelja i da li je putem izvršila sve obaveze prema srodnim mehanizmima. Pitanja koja se nameću su da li je zbilja iza te poruke onaj tko se predstavlja da je, da li je poruka poslana na zaštićen način i što će se poduzeti sukladno tome? Napadi koji se izvršavaju nad spomenutim protokolima su neizbježni i svakodnevni, te se njima mora posvetiti dovoljno pažnje pri reakciji na njih i prevenciji. Kao veće kategorije odabrao sam napade neželjene pošte, napade zloćudnim programima, phishing napade i napade na povjerljive i poslovne podatke.

Through this thesis, my main goal was to explain and demonstrate how secure email messaging really is and how significantly it can affect the users and organizations as well. Apart from security. My main motive was to check from a technological point of view, which mechanisms and protocols are involved in the whole process. Due to the complexity of the topic, I decided to use all the relevant e-mail protocols that exists: SMTP, IMAP, POP3 protocol, and explore their advantages and disadvantages important for configuration and implementation in the selected system. The SPF, DKIM and DMARC authentication protocols determine how the e-mail message came from the sender to the recipient and whether it fulfilled all obligations under the related mechanisms. The questions that arise are whether the person behind that message is who he pretends to be, is the message sent in a secure manner and what will be done accordingly? Attacks against these protocols are unavoidable and happens every day, and they must be given sufficient care in their response and prevention. As larger categories, I have selected spam attacks, malware, attacks, phishing attacks and attacks on confidential and business information.

Ključne riječi: elektronička pošta, protokol, autentikacija, SMTP, SPF, DKIM, DMARC

Sadržaj

1.Uvod

Potreba za komunikacijom putem elektroničke pošte je iznimna i ima golemi utjecaj na organizacije i pojedince koji u privatnom i poslovnom okruženju razmjenjuju na milijarde poruka elektroničke pošte dnevno. Ako se ta brojka uzme u obzir i ako se toj brojci doda još i podatak da se u prosjeku polovica poruka smatra malicioznima ili neželjenom poštom, zadatak svake organizacije je učiniti svoje sustave za razmjenu elektroničke pošte sigurnijim i otpornijim na razne oblike napada na njih. Poruka se može poslati i isporučiti na više načina, i svaki način koristi drugačije protokole koji izvršavaju zatražene radnje. Svaki protokol potreban da bi se veza između pošiljatelja i primatelja poruke elektroničke pošte uspostavila mora poštovati niz pravila i tehničkih detalja kao što su: siguran komunikacijski kanal, valjano ime domene ili način autentikacije. U ovom radu će se prikazati razlike i glavne karakteristike od sva tri protokola za razmjenu poruka elektroničke pošte SMTP, IMAP i POP3. Pojasniti će se zašto se SMTP protokol temelji na imenu domena, koji je protokol zadužen za primanje elektroničke pošte sa udaljenog poslužitelja, koja je razlika između online i offline načina rada, kao i međusobnu povezanost između sva tri protokola. Napadi koji se izvršavaju na elektroničku poštu su sve učestaliji, konkretniji i čine veliku štetu organizaciji i na njih je potrebno reagirati na vrijeme. Svi relevantni napadi kao što su neželjena pošta, zlćudni programi i phishing napadi obraditi će se kroz ovaj rad, prikazati koji su aktualni programi za sprječavanje napade dostupni na tržištu i koje su im karakteristike. SPF, DKIM i DMARC imaju snažnu vezu između sebe i jedan drugom pomažu da se poruke elektroničke pošte prenose na siguran i pouzdan način. Konkretno DMARC ne može funkcionirati ukoliko domena sa koje se šalje poruka nema objavljeni SPF i DKIM potpis. Na koji način će se to odraditi u praksi, pojasnit će se u nekoliko poglavlja. Kroz rad prikazati će se konfiguracija i način implementacije pojedinog protokola kroz Cisco platformu naziva Ironport. Ironport koristi mehanizme za zaštitu web-a i elektroničke pošte, te se smatra jednim od vodećih proizvoda za ublaživanje prijetnji, razvoja povjerljive komunikacije, kao i upravljanjem sigurnosnih rješenja.

2.Protokoli elektroničke pošte

Protokol elektroničke pošte metoda je kojom se uspostavlja komunikacijski kanal između dva računala i elektronička pošta se prenosi između njih. Prilikom prijenosa elektroničke pošte uključeni su poslužitelj elektroničke pošte i barem dva računala, pri kojem jedno računalo šalje poštu, a drugo ju prima. Poslužitelj pošte pohranjuje pošte i omogućuje uređaju koji ju je primio da joj pristupi i po potrebi je preuzme. Poslužiteljem elektroničke pošte može se nazvati određeni stroj u računalnom centru koji je odgovoran za slanje i primanje elektroničke poruke. Takav poslužitelj za poštu sastoji se od različitih komponentnih programa koji koriste različite protokole za međusobnu komunikaciju. Postoje tri opće prihvaćena standarda za razmjenu poruka električke pošte , kako za slanje , tako i za primanje poruka – to su SMTP, POP3, IMAP. Ti se protokoli razlikuju u načinu na koji uspostavljaju konekcije i dopuštaju korisniku pristup porukama unutar pošte. Postoje različiti programi za korištenje elektroničke pošte. Microsoft Outlook jedan je od najpopularnijih komercijalnih programa, Lotus Notes je osobito čest, ali u zadnje vrijeme se sve manje koristi. Ti programi mogu podržavati razne protokole elektroničke pošte. Bitno je napomenuti da se i za različite protokole koriste i različiti portovi. U narednim poglavljima detaljnije će se opisati svaki od protokola, prikazati karakteristične značajke, kao i razlike

2.1.SMTP – Simple Mail Transfer Protocol

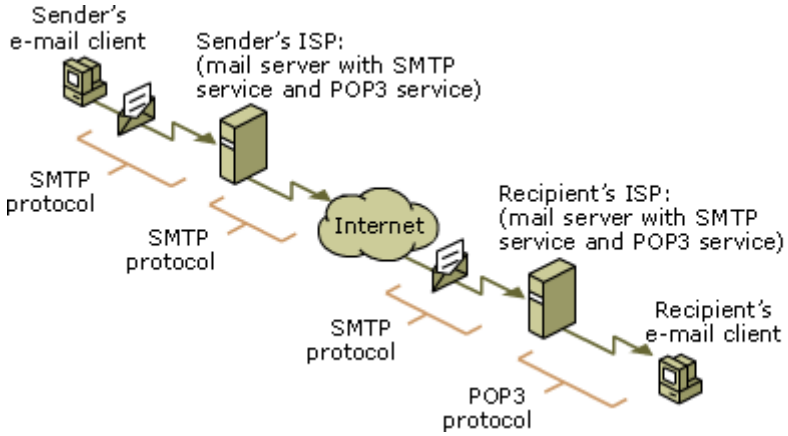
Kada govorimo o SMTP protokolu (eng. Simple Message Transfer Protocol) glavna namjena mu je sigurna i pouzdana razmjena poruka elektroničke pošte bez obzira na tehnologiju i sustav koji se koristi za ostvarenje same razmjene. Različiti standardi određuju različite primjene autentikacijskih mehanizama za SMTP protokol, a time ih i SMTP klijenti i poslužitelji prate i podržavaju. S obzirom da SMTP traži učinkovitu razmjenu informacija, potreban mu je komunikacijski kanal na koji se može osloniti, to ga dovodi do TCP (eng. Transmission Control Protocol) protokola, ma da se SMTP može koristiti i na ostalim protokolima. Razmjena počinje u trenutku kada SMTP klijent primi zahtjev za slanje poruke elektroničke pošte, tada provjerava ime domene primatelja poruke i na temelju imena domene definira s kojim SMTP poslužiteljem će komunicirati kako bi poslao poruku. SMTP poslužitelji ne moraju striktno biti odredišni poslužitelji, oni mogu preuzimati ulogu SMTP klijenta i poslati poruku do nekog sasvim drugog poslužitelja (napraviti relej). Mogu biti izlazni SMTP poslužitelji koji šalju poruke preko nekog od brojnih protokola koji su različiti od SMTP protokola. Što god da se koristilo mora doći do zakonite predaje odgovornosti u kojoj SMTP poslužitelj prije nego što zatvori sesiju mora preuzeti obvezu dostave poruke ili javiti klijentu ako nije moguće to učiniti. Onog trenutka kada

se veza uspostavi SMTP klijent potiče razmjenu poruke elektroničke pošte, te se time šalju naredbe između klijenta i poslužitelja kojima se preciziraju primatelj i pošiljatelj. Poruka se onda dohvaća sa dediciranog sustava i vrši se njena razmjena, uključujući i sva zaglavlja poruke. Prilikom slanja poruke prema većem broju primatelja, SMTP protokol šalje samo jednu kopiju poruke svim primateljima koji su na istom poslužitelju, time se štede mrežni resursi. Poslužitelj je dužan odgovoriti na svaku naredbu, a odgovori mogu biti:

- Da je naredba prihvaćena,
- Da se očekuje nastavak naredbe,
- Na poslužitelju je došlo do trenutne ili trajne greške

Čim se uspješno odradi razmjena poruke SMTP klijet zatraži prekid sesije s poslužiteljem ili može nastaviti s razmjenom drugih poruka elektroničke pošte. Postoji realna situacija u kojoj se ne mogu postaviti direktni komunikacijski kanali između klijenta primatelja i poslužitelja, tada se razmjena poruke provodi preko jednog ili više relejnih (eng. relay) ili izlaznih (eng.gateway) SMTP poslužitelja. Da bi znali koji relejni ili izlazni poslužitelj treba kontaktirati, SMTP klijent saznaje od DNS (eng. Domain name service) poslužitelja i pripadajućeg DNS MX (eng. Mail Exchanger) zapisa uz čiju pomoć se iz adrese primatelja dobiva podatak o imenu SMTP poslužitelja koji poruku prosljeđuje primatelju. Ono što SMTP klijent mora provjeriti je da li je domena unutar adresi primatelja valjana i ako jest mora pretražiti DNS MX zapise u potrazi za imenom adekvatnog SMTP poslužitelja. Ukoliko se otkrije da je domena unutar adrese nevažeća SMTP klijent javlja grešku, te ne prosljeđuje poruku elektroničke pošte. [1]

[1] CCERT-PUBDOC-2006-05-159 SMTP protokol; dostupno na https://www.cert.hr/wp-content/uploads/2006/08/CCERT-PUBDOC-2006-05-159.pdf



Slika 1. SMTP protokol

Za komunikacija između poslužitelja elektroničke pošte obično se koristi standardni TCP port 25 koji je predodređen za SMTP protokol. Klijenti elektroničke pošte uglavnom koriste određene portove koji su namijenjeni za „predaju“ (eng. submission):

- Port 587 – koristi se u slučaju kada klijent ili poslužitelj elektroničke pošte šalje poruku koju treba preusmjeriti odgovarajućem poslužitelju pošte
- Port 465 – ovaj port se koristi samo u slučaju kada neki od programa to zahtjeva, u većini slučajeva kod starijih sustava koji mogu komunicirati samo preko njega

Većina pružatelja internetski usluga danas blokira sav promet odlaznog porta 25 od strane svojih korisnika, kao mjeru predostrožnosti protiv neželjene elektroničke pošte. Iz istog razloga se obično konfigurira vatrozid tako da dopušta samo promet sa odlaznog porta 25 unutar određenih poslužitelja elektroničke pošte.

Bitno je naglasiti da je SMTP protokol isključivo push protokol, drugim riječima njime se može slati poruka, ali se ne može prozvati poslužitelj i sa njega dohvatiti poruka. Da bi se to ostvarilo, klijent svakako mora podržavati neki od protokola koji za to služe, POP3 ili IMAP protokol.

2.1.1.SMTP naredbe

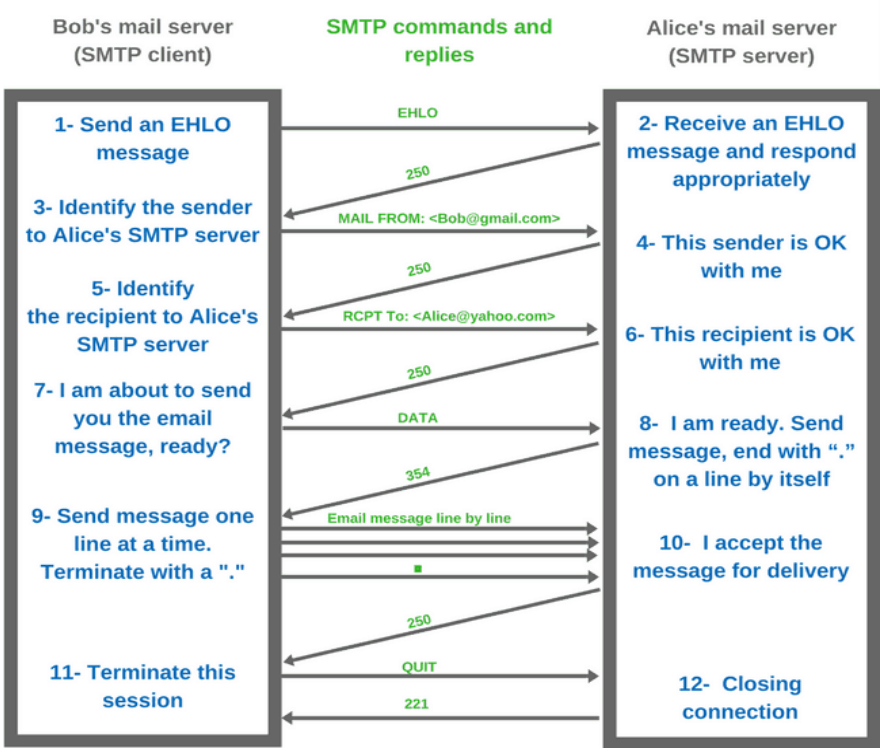
Klijent uspostavlja konekciju i ukoliko poslužitelj prihvati konekciju, započinje razmjena SMTP naredbi točno definiranim redoslijedom. SMTP naredbe predstavljaju tekstualne nizove znakova koji završavaju sa znakom kraja retka, a u sebi sadrže parametre odvojene od same naredbe. Neke od primarnih SMTP naredbi su:

- EHLO – tom naredbom se klijet predstavlja poslužitelju i obavještava poslužitelja da podržava ekstenzije SMTP protokola. Sadržaj EHLO naredbe kojim se klijent

predstavlja je ime njegove domene. Na pristiglu EHLO naredbu poslužitelj odgovara EHLO odgovorom ili javlja da poruka nije prepoznata ukoliko ne podržava SMTP ekstenzije,

- MAIL – naredba kojoj je glavni zadatak slanje poruke elektroničke pošte za identifikaciju pošiljatelja poruke. Ona sadrži informacije o izvršnoj adresi elektroničke pošte prema kojoj se šalju poruke o možebitnim greškama. Najčešći odgovori su za potvrdu identifikacije „250 OK“, te „550“ ili „553“ za trajnu ili privremenu grešku,
- RCPT – naredba kojom se prikazuje adresa elektroničke pošte primatelja poruke, odnosno putanja prosljeđivanja (eng. Forward Path) . Isti odgovor „250 OK“ se daje za potvrdu RCPT naredbe, ukoliko su poštovala procedura, te poslužitelj može pohraniti vrijednost putanje prosljeđivanja. Prilikom saznanja da je adresa elektroničke pošte nepostojeća, dobiva se odgovor „550 No such user“,
- DATA – ovom naredbom se opisuje sadržaj poruke. Poslužitelj nakon što zaprimi tu naredbu analizira svaki sljedeći primljeni redak kao sadržaj poruke dok ne dobije znak da je kraj poruke. Sa odgovorom „250 OK“ SMTP poslužitelj potvrđuje uspješnu konekciju,
- RSET – naredba kojom se prekida sesija, te se njome traži od poslužitelja da izbrišu pohranjeni podaci o primateljima poruka,
- VRFY – naredba kojom se potvrđuje da li adresa primatelja odgovara korisničkom imenu ili stvarnoj adresi elektroničke pošte,
- AUTH – poslužitelj ovom naredbom javlja klijentu da podržava ekstenziju za autentikaciju, kao i koji mehanizam autentikacije koji podržava. Bitno je napomenuti da se nakon uspješne autentikacije ne smije biti ni jedna AUTH naredba unutar iste sesije. [2]

[2] CCERT-PUBDOC-2006-05-159 SMTP protokol; dostupno na https://www.cert.hr/wp-content/uploads/2006/08/CCERT-PUBDOC-2006-05-159.pdf



Slika 2. Primjer SMTP naredbi

U današnje vrijeme postoje mnogobrojni dostupni oblici SMTP autentikacijskih metoda koji sprječavaju ili u potpunosti onemogućavaju zlonamjerne napadače u njihovim aktivnostima. Da nema tih autentikacijskih metoda, kao ni ostalih potrebitih sigurnosnih kontrola, poslužitelji elektroničke pošte bi lagano postali metom raznih napadača koji pokušavaju putem elektroničke pošte slati što veće količine poruka neželjene pošte, te ostalih vrsta napada u cilju onemogućavanja ispravnog rada poslužitelja.

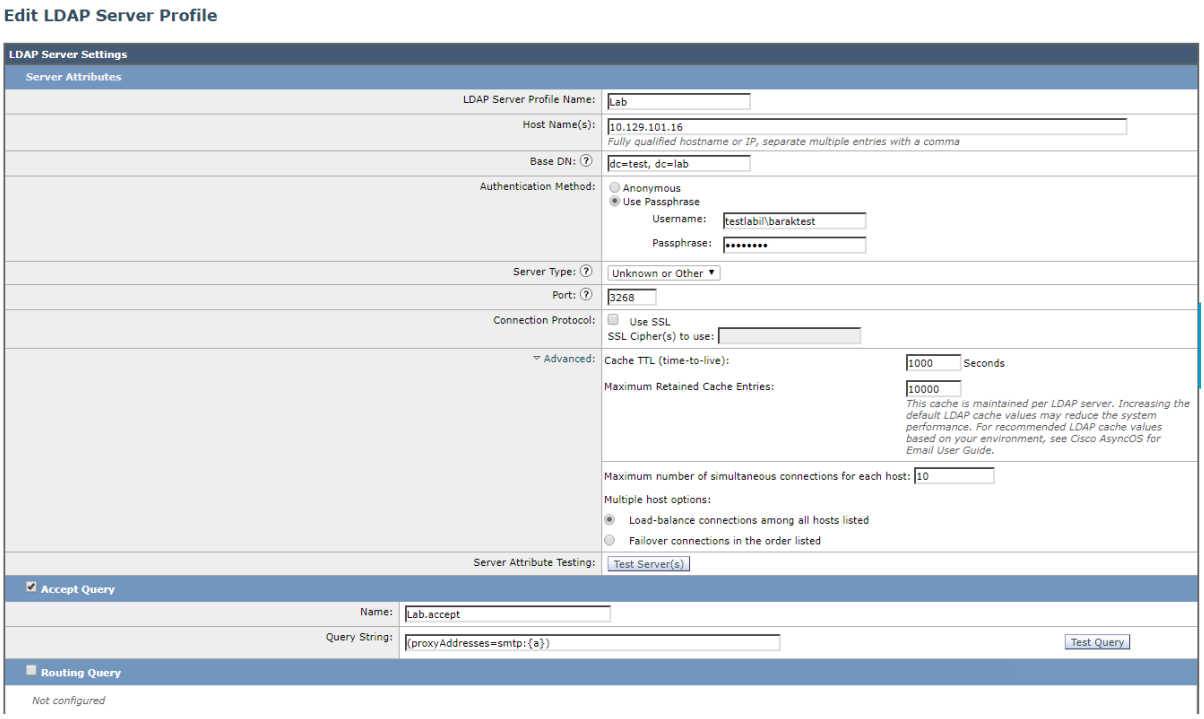
2.1.2. Autentikacija SMTP protokola kroz Ironport

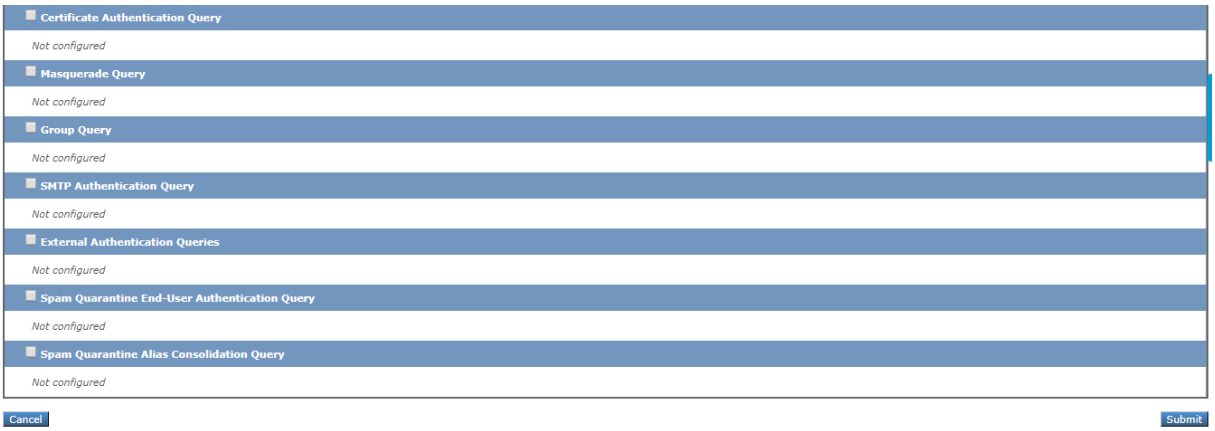
Praktična upotreba ovog mehanizma je da korisnici u određenoj organizaciji mogu slati elektroničku poštu putem poslužitelja pošte tog entiteta, čak i ako se povezuju sa udaljenih mjesta. Klijenti elektroničke pošte mogu izdati zahtjev za provjeru autentičnosti pri pokušaju slanja poruke. Korisnici također mogu koristiti SMTP autentikaciju za poruke odlazne pošte. Time se omogućuje Ironportu sigurna veza sa relejnim poslužiteljem. Ironport podržava dvije metode za provjeru autentičnosti korisnika:

- Putem LDAP direktorija,
- Korištenjem drugog SMTP poslužitelja.

Prilikom odabira autentikacije sa LDAP poslužiteljem, potrebno je odabrati SMTP AUTH vrstu upita koje se može pronaći unutar Add ili Edit LDAP Server Profile sekcije pri Ironportu. (ili

koristeći CLI naredbu *ldapconfig*) za kreiranje SMTP provjere autentičnosti kao što se prikazuje na slici 3. Za svaki LDAP poslužitelj koji se konfigurira može se konfigurirati SMTP AUTH upit koji će se koristiti kao profil SMTP provjere identiteta. Postoje dvije vrste upita za provjeru autentičnosti: povezivanje LDAP-om i korištenje lozinke kao atribut. Kada se koristi lozinka kao atribut, Ironport će dohvatiti dio lozinke u LDAP direktoriju. Lozinka može biti pohranjena u običnom tekstu ili šifrirana. Kad se koristi povezivanje LDAP-om, Ironport se pokušava prijaviti na LDAP poslužitelj pomoću vjerodajnica koje je pružio klijent. Ironport uzima korisničko ime pri razmjeni SMTP autentikacije i pretvara ga u LDAP upit koji dohvaća šifrirani ili vidljivi dio lozinke. Nakon toga odraditi će se svi potrebni mehanizmi šifriranja prema lozinkama dobivenim unutar SMTP autentikacije i usporediti rezultate sa onim što je preuzeto sa LDAP-a. Podudaranje znači da će se SMTP autentikacijska sesija nastaviti. Ukoliko se podudaranje ne ostvari rezultirati će se pogreškom u kodu.

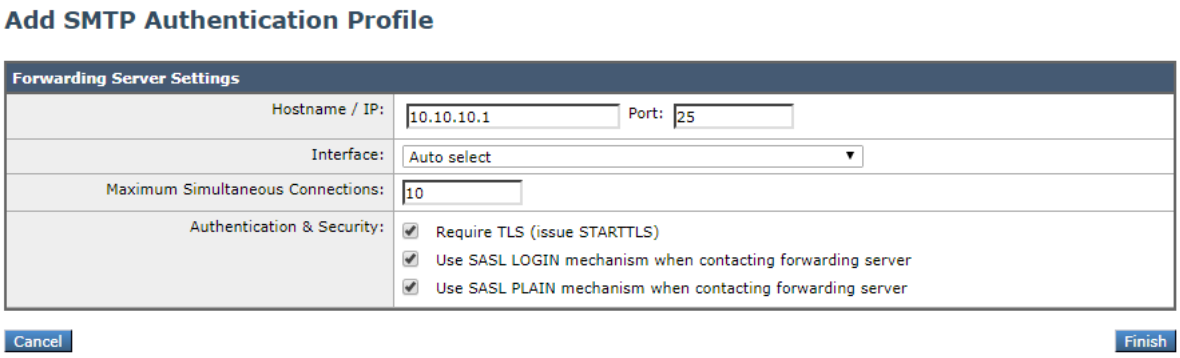




Slika 3. Autentikacija sa LDAP poslužiteljem

Ironport se može konfigurirati kako bi se provjerili korisničko ime i lozinka koji su isporučeni SMTP autentificiranom konekcijom korištenjem drugog SMTP poslužitelja. Poslužitelj za provjeru autentičnosti nije poslužitelj koji prenosi elektroničku poštu, već on odgovara samo na SMTP zahtjeve za provjeru autentičnosti. Kada je provjera autentičnosti uspjela, razmjena elektroničke pošte SMTP protokolom može se nastaviti. Ova se značajka ponekad naziva i „SMTP autentikacija s prosljeđivanjem“ " jer se samo prosljeđuju korisničko ime i lozinka prema drugom SMTP poslužitelju radi provjere autentičnosti, a na Ironportu se konfigurira ovako (Slika 4.):

1. Odabrati *Network -> SMTP Authentication*
2. Odabrati *Add Profile*
3. Upisati jedinstveno ime za SMTP autentikacijski profil
4. Pod Profile *Type* odabrati *Forward*
5. Odabrati *Next*
6. Odabrati ime hosta ili IP adresu i port poslužitelja za prosljeđivanje. Odabrati sučelje za prosljeđivanje koje se koristiti za prosljeđivanje zahtjeva za provjeru autentičnosti. Navesti broj maksimalnih simultanih konekcija. Potrebno je odlučiti da li je TLS protokol potreban za povezivanje Ironporta sa poslužiteljem za prosljeđivanje.
7. Izvršiti promjene



Slika 4. Konfiguriranje SMTP autentikacijskog profila

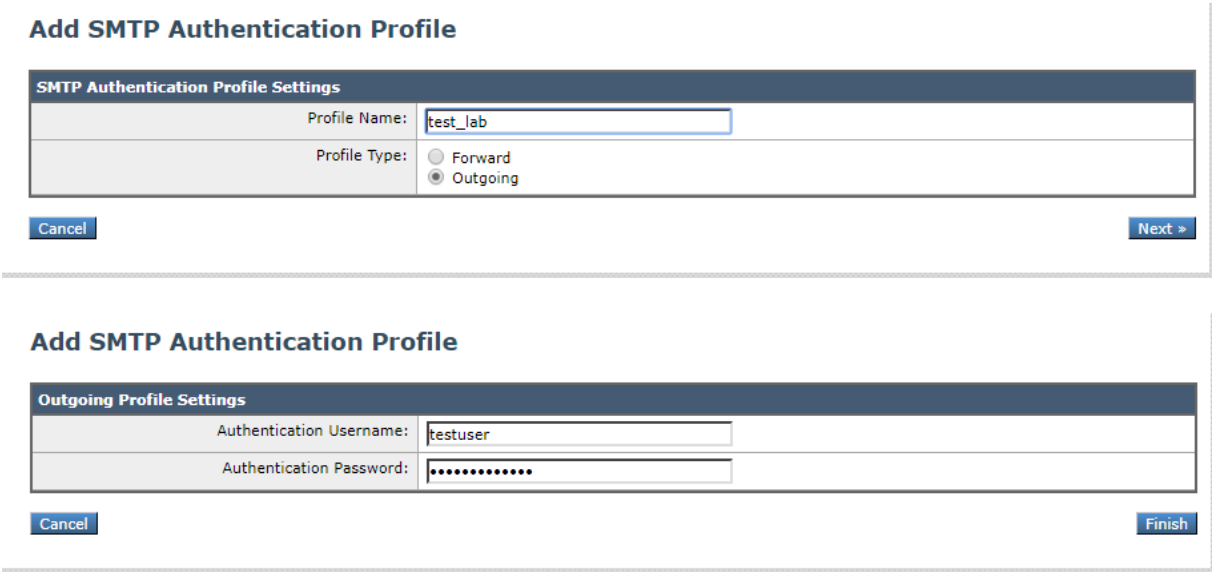
Za konfiguraciju LDAP-a temeljenim na SMTP provjeri identiteta, potrebno je prethodno kreirati SMTP upit za provjeru autentičnosti u kombinaciji sa LDAP profilom poslužitelja, a nalazi se u Ironportu pod sekcijom System -> Administration -> LDAP. Potom se može upotrijebiti upravo kreirani profil za stvaranje SMTP autentikacijskog profila:

1. Odabrati Network -> SMTP Authentication
2. Odabrati Add Profile
3. Upisati jedinstveno ime za SMTP autentikacijski profil
4. Pod Profile Type odabrati LDAP
5. Odabrati Next
6. Odabrati LDAP upit koji će se koristiti za ovaj profil provjere autentičnosti
7. Odabrati zadanu metodu šifriranja, može se izabrati SHA, Salted SHA, Crypt, Plain ili MD5
8. Izvršiti promjene

Ironport podržava korištenje klijentskih certifikata za provjeru autentičnosti SMTP konekcija između Ironporta i klijenata elektroničke pošte. Prilikom stvaranja profila za provjeru identiteta SMTP protokol odabire LDAP upit provjere autentičnosti, koji se koristiti za provjeru certifikata. Ukoliko organizacija koristi klijentske certifikate za provjeru autentičnosti korisnika, postoji mogućnost korištenja SMTP upita za provjeru identiteta kako bi provjerili može li korisnik koji nema certifikat slati poruke, čak i ako zapis kaže da je to dopušteno. SMTP provjera identiteta može se koristiti i za osiguravanje provjere slanja izlazne pošte, koristeći korisničko ime i lozinku. Kreira se SMTP profil za provjeru identiteta i veže ga se na SMTP rutu za sve domene. Pri svakom pokušaju isporuke elektroničke pošte, Ironport će se

prijaviti na relej elektroničke pošte s potrebnim vjerodajnicama. Kao što je prikazano na slici 5. prvo je potrebno kreirati odlazni SMTP autentikacijski profi:

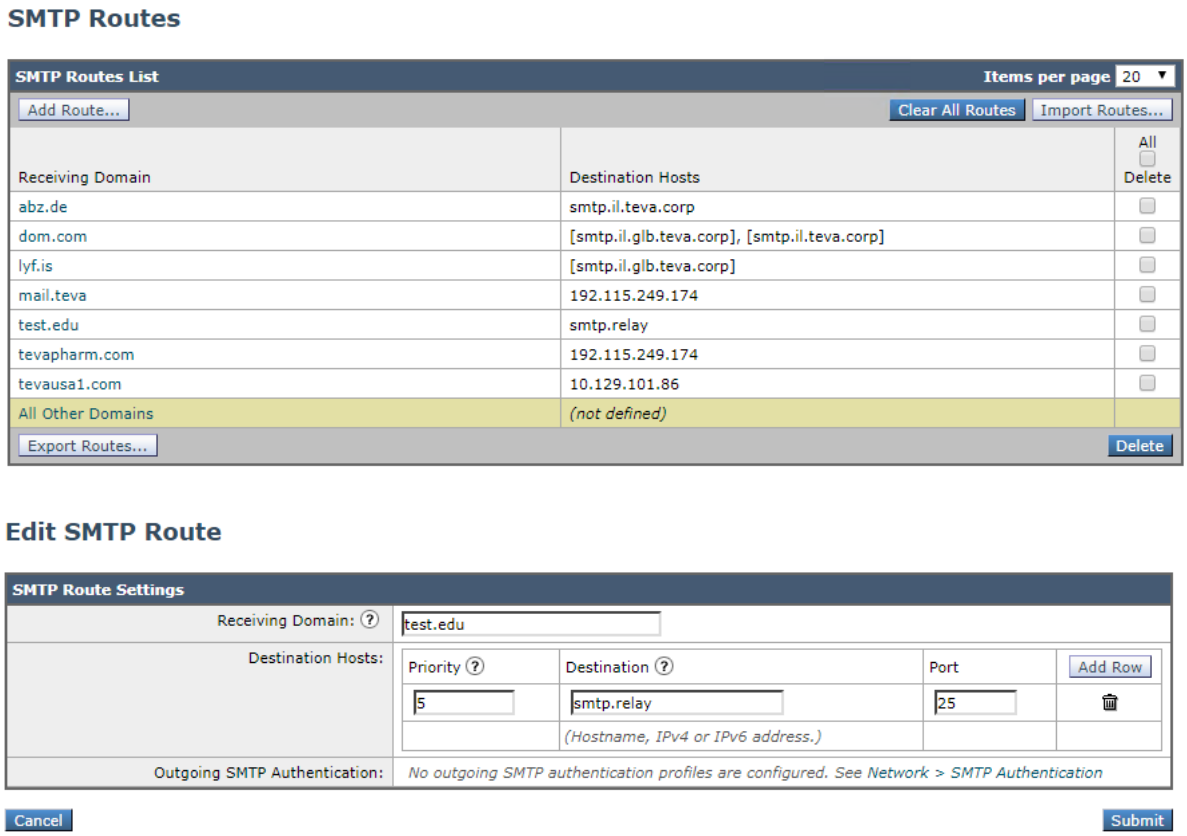
1. Odabrati Netwok -> SMTP Authentication
2. Odabrati Add Profile
3. Upisati jedinstveno ime za SMTP autentikacijski profil
4. Pod Profile Type odabrati Outgoing
5. Odabrati Next
6. Upisati korisničko ime i lozinku za autentifikacijski profil
7. Odabrati Završetak



Slika 5. Konfiguriranje autentikacijskog profila za izlaznu poštu

Drugi korak je konfigurirati SMTP rute za upotrebu odlaznog SMTP autentikacijskog profila koji je kreiran u prethodnom koraku (slika 6.):

1. Odabrati Network -> SMTP Routes
2. Odabrati All Other Domains pod Receiving Domain sekciji
3. Upisati ime odredišnog hosta za SMTP rutu. To je ime vanjskog releja za poštu koji se koristi za isporuku odlazne pošte
4. Odabrati odlazni SMTP autentikacijski profil
5. Izvršiti promjene



Slika 6. Konfiguriranje SMTP rute za upotrebu odlaznog SMTP autentikacijskog profila

Sljedeći događaji zabilježit će se u logovima elektroničke pošte kada je SMTP mehanizam provjere autentičnosti konfiguriran na Ironportu:

- Uspješni pokušaji provjere SMTP autentikacije,
- Neuspješni pokušaji provjere SMTP autentikacije,
- Nemogućnost povezivanja sa autentikacijskim poslužiteljem,
- Prekid sesije kada poslužitelj za prosljeđivanje stane dok čeka zahtjev za autentikaciju.

2.2.POP3 – Post Office Protocol

POP 3 (eng. Post Office Protocol) je standardni protokol elektroničke pošte koji se koristi za primanje elektroničke pošte sa udaljenog poslužitelja na klijenta elektroničke pošte konfiguriranog na računalu, koristeći TCP/IP konekciju. Njegova popularnost leži u jednostavnosti protokola za konfiguriranje i održavanje. Poslužitelji elektroničke pošte pružatelja internetskih usluga (eng. Internet Service Provider - ISP) također koriste POP3 protokol za primanje i čuvanje poruka elektroničke pošte namijenjenih svojim korisnicima.

Periodički će korisnici, uz pomoć svojih klijenata elektroničke pošte, provjeriti svoj poštanski pretinac, koji se nalazi na udaljenom poslužitelju, i preuzimati sve poruke elektroničke pošte upućene njima. Klijenti elektroničke pošte obično koriste dobro poznati TCP port 110 za povezivanje sa POP3 poslužiteljem. Ako je šifrirana komunikacija podržana na POP3 poslužitelju, korisnici se mogu povezati putem TLS (eng. Transport Layer Security) ili SSL (eng. Secure Sockets Layer) protokola preko TCP porta 995 za povezivanje sa poslužiteljem[3]. Zbog svog osnovnog cilja, pohrane i primanja elektroničke pošte, POP3 je kompatibilan s bilo kojim programom, kao npr. Outlook koji je najčešće i nativan. Kada korisnik odluči provjeriti ima ili u pretincu elektroničke pošte novih poruka, klijent će se povezati na POP3 poslužitelj. Zatim klijent elektroničke pošte isporučuje svoje korisničko ime i lozinku poslužitelju radi provjere autentičnosti. Jednom povezan, klijent izdaje niz tekstualnih naredbi za preuzimanje svih poruka elektroničke pošte. Zatim pohranjuje preuzete poruke lokalno kod korisnika prikazujući nove poruke elektroničke pošte i briše poslužiteljske kopije i prekida vezu s poslužiteljem. Prema zadanim postavkama, poruke elektroničke pošte brišu se sa poslužitelja nakon preuzimanja. Kao rezultat toga, poruke elektroničke pošte povezane su s tim računalom i nije moguće pristupiti istim porukama elektroničke pošte od klijenta na drugom računalu. Korisnik bi mogao zaobići ovaj problem konfigurirajući postavke klijenta za elektroničku poštu tako da ostavi kopiju poruka na poslužitelju. POP3 protokol oslobađa prostor poštanskih pretinaca na poslužitelju jer se poruke preuzimaju i brišu sa poslužitelja svaki puta kada klijent elektroničke pošte provjeri postoje li nove poruke. Offline poruke elektroničke pošte pohranjene na korisnikovom računalu nemaju ograničenje veličine poštanskog pretinca, nego je kapacitet ograničen veličinom kapaciteta tvrdog diska na korisnikovom računalu. Jedan od nedostataka POP3 protokola je taj što je korisniku teško izvući i prebaciti poruke ako se odluči za promjenu programa elektroničke pošte ili računala.

Prednosti POP3 protokola:

- Poruke se preuzimaju na korisničko računalo, te se mogu čitati kada je korisnik van mreže,
- potrebno je manje prostora za pohranu na poslužitelju, također sve se poruke pohranjuju lokalno na računalu,
- jednostavan za konfiguriranje i upotrebu.

[3] Conrad Chung: Understanding Post Office Protocol (POP3); dostupno na https://www.2brightsparks.com/resources/articles/understanding-post-office-protocol-pop3.pdf

Nedostatci POP3 protokola:

- porukama se ne može pristupiti s drugih računala,
- prebacivanje mape lokalne pošte na drugo računalo može biti kompliciranо,
- mape sa porukama elektroničke pošte mogu biti korumpirane, i tako se izgubiti sve poruke u poštanskom pretincu odjednom.

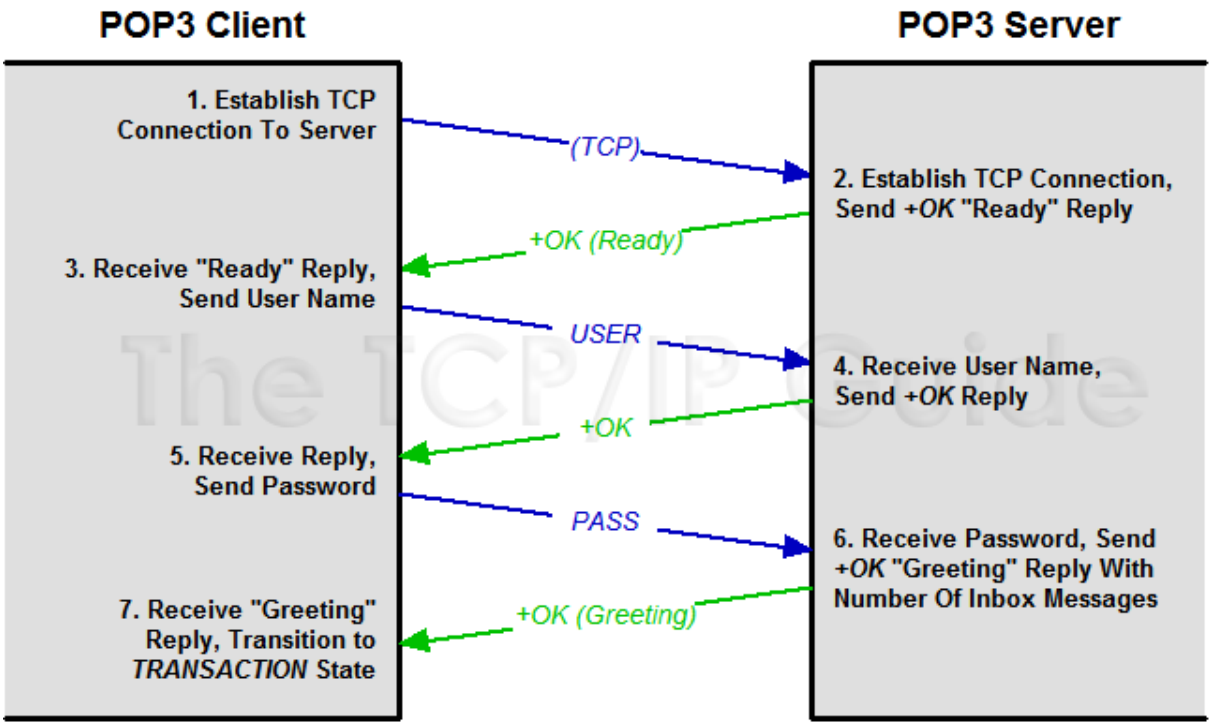
POP3 naredbe veličine su tri ili četiri slova i ne razlikuju velika i mala slova. Te se koriste u običnom ASCII tekstu. Koriste se dva osnovna odgovora:

- + OK - pozitivan odgovor, poslan kad je naredba ili akcija uspješno provedena
- - ERR - negativni odgovor, poslan kao pokazatelj da je došlo do pogreške.

Sesija između POP3 klijenta i POP3 poslužitelja započinje kada klijent pošalje zahtjev za TCP vezu prema poslužitelju prema slici 7. Veza se uspostavlja standardnim TCP "trosmjernim rukovanjem" (eng. three-way handshake), i time POP3 sesija započinje. Prvo od tri stanja POP3 sesije je stanje autorizacije, čija je odgovornost provjera autentičnosti POP3 klijenta sa poslužiteljem. Kada sesija započne sa autorizacijom, poslužitelj klijentu šalje odgovor da ga je prepoznao. Time poslužitelj javlja klijentu da je konekcija uspostavljena i klijent može poslati prvu naredbu. Primjer takvog odgovora bio bi:

+OK POP3 server ready

Klijent je sada dužan dokazati da je to stvarno korisnik koji pokušava pristupiti poštanskom pretincu. Kao i dokazati da korisnik ima pravo pristupa poslužitelju i identificira korisnika tako da poslužitelj zna koji poštanski pretinac se traži. Prvo klijent šalje *USER* naredbu zajedno sa korisničkim imenom ili adresom elektroničke pošte. Poslužitelj odgovara potvrdom. Klijent tada pomoću naredbe *PASS* šalje korisničku lozinku. Pod pretpostavkom da je prijava valjana, poslužitelj odgovara klijentu potvrdom koja ukazuje na uspješnu provjeru autentičnosti. Odgovor također obično određuje broj poruka koje čekaju u poštanskom pretincu.



Slika 7. Sesija između POP3 klijenta i POP3 poslužitelja

Ako je autorizacija uspješna, POP3 sesija prelazi u stanje transakcije u kojem se mogu provoditi naredbe za pristup elektroničkoj pošti. Ako su korisničko ime ili lozinka netočni, prikazati će se odgovor o pogrešci i sesija se neće nastaviti. Autorizacija također može biti neuspješna zbog tehničkih problema. Ako se podudara s računanjem poslužitelja, provjera autentičnosti je uspješna, u suprotnom sesija ostaje u stanju autorizacije. Nakon što POP3 klijent uspješno provjeri autentičnost korisnika koji pristupa poštanskom pretincu, sesija prelazi iz stanja autorizacije u stanje transakcije. Tamo POP3 klijent izdaje naredbe koje obavljaju transakcije pristupa poštanskom pretincu i preuzimaju poruku. Stanje transakcije je dosta nestrukturirano, tako da naredbe ne moraju biti izdane u određenom redoslijedu kako bi ispunili zahtjeve standarda. Nakon što klijent POP3 protokola dovrši sve transakcije pristupa i preuzimanja elektroničke pošte koje je trebao obaviti, sesija se na izgled čini gotovom. Međutim nije do kraja. POP3 protokol definira zadnje stanje sesije a to je stanje ažuriranja. Koje služi za obavljanje različitih funkcija održavanja, te nakon toga prekida POP3 sesiju, kao i temeljnu TCP konekciju. Prijelaz iz stanja transakcije u stanje ažuriranja događa se kada POP3 klijent izda QUIT naredbu. Ova naredba javlja POP3 poslužitelju da je konekcija sa klijentom završena i da se želi završiti sesija.

2.3.IMAP – Internet Message Access Protocol

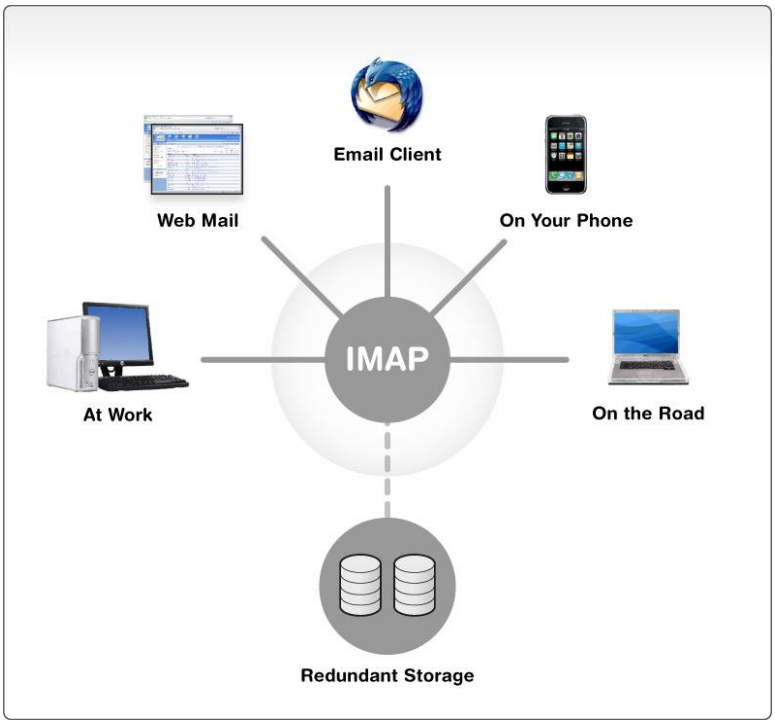
IMAP (eng. Internet Message Access Protocol) je protokol kojim se elektronička pošta prenosi sa udaljenog poslužitelja na lokalno računalo. Smatra se najčešće korištenim protokolom za takvu vrstu komunikacije. Svoju širinu dobiva zbog toga jer ga podržavaju razni besplatnih, kao i komercijalnih klijenti i poslužitelji. Autentikacija i enkripcija služe kao sigurnosni mehanizmi IMAP protokola. Autentikacijom se osigurava pristup pretincima elektroničke pošte samo ovlaštenim korisnicima, dok enkripcijom se štite podaci koji se šalju putem mreže. Zasigurno, jedna od ključnih prednosti je sposobnost istovremenog pristupanja istom poštanskom pretincu za veći broj klijenata, sa različitih lokacija (slika 8.). IMAP koristi naredbe koje klijent šalje poslužitelju, te ih poslužitelj zaprima, obrađuje i vraća kao odgovor klijentu. IMAP osigurava i sljedeće bitne funkcionalnosti:

- rad s MIME formatom poruka i dohvat pojedinih MIME dijelova s poslužitelja (npr. korisnik dohvaća tekstualni dio poruke, ali ne dohvaća privitak),
- tzv. online i offline način rada,
- dohvat statusa poruke i stvaranje vlastitih oznaka poruke,
- korištenje više poštanskih pretinaca i slanje poruka između njih te korištenje javnih ili dijeljenih mapa. [4]

IMAP poslužitelji primaju elektroničku poštu od programa koji služe za razmjenu poruka (npr. Microsoft Exchange), te se one skladište u dijeljeni prostor u formatu koji je razumljiv IMAP poslužitelju. Kako bi zaštitili komunikaciju između klijenta i poslužitelja, IMAP protokol koristi SSL podršku za enkripciju. Klijenti šalju zahtjeve na *portove* na kojem poslužitelj osluškuje zahtjeve:

- Port 143 – IMAP
- Port 585 - IMAP4-SSL (s ugrađenom SSL enkripcijom)
- Port 993 – IMAP preko SSL kanala

[4] NCERT-PUBDOC-2010-05-300: Sigurnost IMAP protokola; dostupno na https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-05-300.pdf



Slika 8. IMAP protokol

Zahvaljujući svome složenom dizajnu, IMAP je pouzdan i fleksibilan s obzirom da je moguće uvesti nove opcije bez da se naprave promijene unutar protokola. Isključeni IMAP, poznat i kao offline IMAP, dobar je primjer kako se ta prednost može koristiti. Klijent električne pošte lokalno sprema cijeli sadržaj poštanskog pretinca na računalo. U tom trenutku korisnik može stvoriti mape i premještati, označavati ili brisati poruke elektroničke pošte tijekom izvan mrežnog rada. Sljedeći put kad se klijent poveže s IMAP serverom, klijent i poslužitelj sinkroniziraju sve promjene. Unatoč nekim ranim problemima u implementaciji ova metoda sada djeluje uredno i stvara prednost IMAP protokola.

2.3.1.IMAP naredbe

IMAP protokol obuhvaća između 30 i 50 naredbi koje se upotrebljavaju za komunikaciju između klijenta i poslužitelja. Format naredbi smatra se ne promjenjivim, a svaka naredba prima posebno definirane argumente. IMAP naredbe koje se najčešće koriste su:

- LOGIN - omogućava autentikaciju korisnika putem korisničkog imena i lozinke koji se u tekstualnom obliku šalju putem mreže. Zbog rizika koji predstavlja za sigurnost, njezina se uporaba ne preporuča. LOGIN kao ulazne parametre koristi korisničko ime i lozinku korisnika. Poslužitelj kao odgovor vraća:
  - OK za uspješnu prijavu
  - NO za neuspješnu prijavu
  - BAD za loše oblikovanu naredbu,
- AUTHENTICATE - prima samo jedan argument koji sadrži ime autentikacijskog mehanizma. Uspješna autentikacija završit će odgovorom OK, a neuspješna odgovorom NO ili BAD, ovisno o vrsti pogreške,
- SELECT - ova naredba izvodi se nakon provjere identiteta korisnika, a njome korisnik odabire pretinac kojem će pristupiti. Naredba kao ulazni argument prima ime pretinca. Odgovori poslužitelja isti su kao za LOGIN (OK, NO, BAD). U odgovoru poslužitelj vraća:
  - oznake poruka (FLAGS)
  - broj poruka u pretincu (EXISTS)
  - broj novih poruka (RECENT),
- CAPABILITY - Naredba koju može izvesti bilo koji klijent, neovisno o tome je li provjeren njegov identitet ili nije, te se dohvaćaju mogućnosti podržane na korištenom IMAP poslužitelju,
- STARTTLS - mora podržavati svaki poslužitelj, a omogućuje kriptiranje komunikacije TLS protokolom,
- LOGINDISABLED - mora podržavati svaki poslužitelj, te onemogućuje korištenje nesigurne naredbe LOGIN. [5]

[5] NCERT-PUBDOC-2010-05-300: Sigurnost IMAP protokola; dostupno na https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-05-300.pdf

3.Sigurnost elektroničke pošte

Sigurnost elektroničke pošte opisuje razne tehnike čuvanja osjetljivih podataka unutar komunikacije između klijenta i poslužitelja, kao i čuvanje informacija koje su bitne za organizaciju od neovlaštenog pristupa, gubitka ili kompromitiranja. Elektronička pošta je popularan medij za širenje zlonamjernih programa, neželjene pošte ili phishing napada, u cilju dohvaćanja informacija, prevare, zarade ili jednostavno ulaska u sustav zbog nečasnih radnji. Sigurnost elektroničke pošte potrebna je jednako za privatne korisnike, kao i za poslovne korisnike, a postoje razne mjere obrane i zaštite od napadača koje je potrebno poduzeti kako bi se preventivno i trenutno poboljšala sigurnost elektroničke pošte. Neke od tih mjera obrane, kao i njihove prednosti i mane opisati ćemo u nastavku rada.

3.1.SPAM napadi

Spam bi se u najkraćim crtama mogao opisati kao neželjena elektronička pošta koja se šalje sa namjerom oglašavanja promidžbenog sadržaja, u svrhu napada ili kao sredstvo primjene zlonamjernih poveznica. Elektronička pošta je izvor koji neželjena pošta u potpunosti i najčešće koristi za slanje poruka. Predvodnici neželjene pošte nazivaju se spameri (eng. spammers). [6] Spam se elektroničkom poštom šalje kako da bi pružio razne usluge, kao što su lažne obavijesti o potencijalnoj zaradi, internetska kupovina i slične akcije, bez prethodnog odobrenja korisnika za primanje istih. Još jedan problem koji predstavlja neželjena pošta je taj da se zbog nagomilanih poruka može zagušiti slobodni prostor za validne poruke, a time se ne mogu isporučivati nove poruke. Neželjena pošta je spamerima postala omiljena jer ne predstavlja nikakav trošak i teško ih je optužiti i otkriti. Adrese se prikupljaju preko raznih chatova, web stranica ili virusom zaraženih računala. Najčešći način prikupljanja adresa je pomoću robotskih skupljača (eng. harvester) – bota koji na webu traži adrese elektroničke pošte. Pošto su spameri izrazito snalažljivi napadači, razvili su mrežu preko koje međusobno razmjenjuju baze prikupljenih adresa. Kako bi saznali je li poruka poslana na ispravnu adresu, poruka neželjene pošte najčešće sadrži upute i poveznicu na URL. Napadači za slanje poruka sve više koriste mrežu sastavljenu od inficiranih (eng. zombie) računala, poznatiju pod nazivom "botnet" tako da ih je teško otkriti. Napadači svoju infrastrukturu često smještaju u zemlje koje nemaju zakonski definirane kazne za širenje poruka neželjene pošte.

[6] SPAM – Cert.hr; dostupno na https://www.cert.hr/19795-2/spam/

Postoji nekoliko različitih načina na koji se neželjena pošta može poslati:

- Neželjena pošta unutar klijenta elektroničke pošte - također poznati i kao Junk elektroničke pošte,
- Neželjena pošta poslana razmjenom poruka – cilja na korisnike usluga trenutnih poruka (npr. Skype), SMS-ova ili privatnih poruka unutar web preglednika,
- Neželjena pošta poslana putem društvenih mreža - neželjena pošta koja se može očitovati na više načina, uključujući nepristojnost, uvrede, govor mržnje, lažne kritike, lažne prijatelje, te lažne osobne podatke,
- Snowshoe neželjena pošta - je tehnika korištenja širokog raspona IP adresa i adresa elektroničke pošte s neutralnom reputacijom za široku distribuciju neželjene pošte.

Jedna od metoda je i korištenje prazne poruke elektroničke pošte. To uključuje slanje elektroničke pošte s praznim tijelom i naslovom poruke. Tehnika se može upotrijebiti u napadu na poslužitelj elektroničke pošte koji pokušava provjeriti adrese elektroničke pošte za distribuciju tako da se identificiraju nevažeće odbačene adrese. U ovakvoj vrsti napada, napadač ne treba unositi tekst u poruku elektroničke pošte. U drugim slučajevima, naizgled prazna poruka elektroničke pošte može sakriti određene viruse koji se mogu širiti putem HTML koda ugrađenog u elektroničku poštu. Napadači su razvili metode za prikrivanje neželjene pošte i konstantno pronalaze načine kako zaobići spam filtre kojima se sustavi brane od napada.

Najčešći oblik zaštite od neželjene pošte je postavljanje filtera ispred poslužitelja elektroničke pošte. Kad se isporuči poruka elektroničke pošte, ona prvo mora proći kroz filter prije nego dođe do filtera neželjene pošte. Poruka sa poslužitelja elektroničke pošte prelazi na klijenta. Još jedan uobičajeni oblik zaštite od neželjene pošte je postavljanje filtera izravno na poslužitelju elektroničke pošte. Jedan od problema je taj da se neželjena pošta ne može vratiti natrag u ovoj metodi. Korištenje filtra kojim se provjerava sadržaj može biti vrlo skup jer filter mora provjeriti cijelu poruku, a zatim primijeniti određeni skup pravila na sadržaj koji se neprekidno mijenja.

Za sprečavanje neželjene pošte koriste se različite tehnike. Nijedna tehnika ne rješava u potpunosti problem sa neželjenom poštom, a svaka od njih ima kompromise između pogrešno odbijene legitimne poruke elektroničke pošte i odbacivanja sve neželjene pošte. Anti-spam tehnike mogu se razvrstati u nekoliko kategorija: one koje zahtijevaju radnje pojedinaca, one koje mogu automatizirati administratori elektroničke pošte, te one koje mogu automatizirati

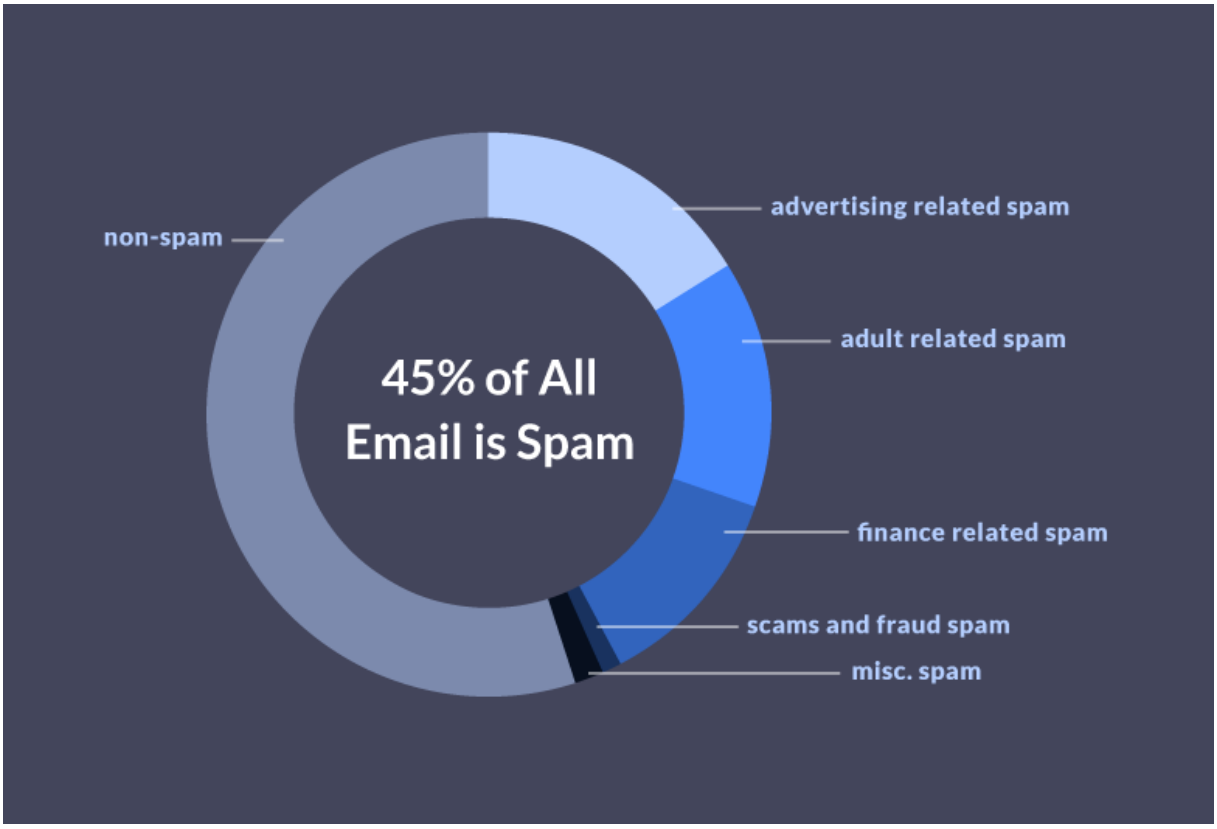
pošiljatelji elektroničke pošte. Postoji nekoliko tehnika pomoću kojih se ograničava dostupnost adresa elektroničke pošte, s ciljem da smanje mogućnost vjerojatnosti primanja neželjene pošte:

- Diskrecija - dijeljenje adrese elektroničke pošte samo ograničenoj grupi primatelja jedan je od načina smanjivanja mogućnosti da će adresa biti ukradena i ciljana od strane napadača,
- Promjena adresa - adrese elektroničke pošte objavljene na raznim internetskim stranicama podložne su prikupljanju od strane napadača. Mijenjanje adresa praksa je prikrivanja adrese elektroničke pošte kako bi se spriječilo da se automatski prikuplja na ovaj način, ali ipak omogućuje korisniku da rekonstruira izvornu adresu,
- Izbjegavati odgovore na poruke neželjene pošte - uobičajeni savjet je ne odgovarati na neželjene poruke, jer napadači mogu jednostavnim odgovorom potvrditi da je adresa elektroničke pošte valjana.[7]

Mnoge zemlje, uključujući Kanadu, Australiju, te Europsku uniju, donijele su zakone koji se bave temom slanja neželjene pošte. EU ima skup smjernica od kojih zemlje članice mogu prilagoditi svoje zakone o elektroničkoj komunikaciji, ali većina zemalja članica propisuje da je prije slanja poruke elektroničke pošte potreban prethodni izričiti pristanak za isključivanje svih daljnjih neželjenih poruka, kako bi se olakšalo primatelju otkrivanje istih. Ukoliko dođe do prekršaja prestupnici mogu primiti novčane i druge kazne. [8]

Okvirna statistika kaže, kao i slika 9., da se svakog dan na globalnoj razini pošalje 14,5 milijardi poruka neželjene pošte, što čini 45% od ukupnog broja poruka elektroničke pošte poslane u jednom danu. 36% sve neželjene pošte čini neki oblik oglašavanja. Najčešća vrsta neželjene pošte povezana je s oglašavanjem. To uključuje promotivni prodajni sadržaj za koji primatelj nije izričito odobrio primanje. Druga najprisutnija vrsta neželjene pošte je sadržaj povezan sa porno industrijom, koji čini 31,7% sve neželjene pošte. Poruke o financijama zauzimaju treće mjesto, čineći oko 26,5% neželjene pošte. Na svakih 12,5 milijuna neželjenih poslanih poruka samo jedna osoba odgovori. To možda ne zvuči previše, dok se ne uzme u obzir da se svakodnevno šalje više od 14 milijardi neželjenih poruka. Čak i samo jednim odgovorom na 12,5 milijuna poslanih poruka, spameri zarade oko 3,5 milijuna dolara tijekom jedne godine. Tom računicom dobili bi da neželjena poruka košta tvrtke oko 20,5 milijardi dolara svake godine.

[7] Anti-spam techniques; dostupno na https://en.wikipedia.org/wiki/Anti-spam_techniques
[8] Email spam; dostupno na https://searchsecurity.techtarget.com/definition/spam



Slika 9. Postotak vrste poruka neželjene pošte

3.1.1. Anti-spam implementacija kroz Ironport

Anti-spam mehanizmi pregledavaju dolaznu elektroničku poštu, kao i odlaznu, na temelju pravila elektroničke pošte kojima se konfigurira:

- Jedan ili više mehanizama za skeniranje, skeniraju poruke putem svojih modula filtriranja,
- Mehanizmi za skeniranje dodjeljuju ocjenu svakoj poruci. Što je rezultat veći, veća je i vjerojatnost da je poruka neželjena,
- Na temelju rezultata svaka se poruka kategorizira kao:
    - Nije neželjena pošta
    - Sumnja se na neželjenu poštu
    - Prepoznata neželjena pošta
- Na temelju rezultata se poduzimaju daljnje mjere.

Radnje poduzete unutar poruka koje su identificirane kao neželjene, a za koje se sumnja da su neželjene ili su prepoznate kao neželjene marketinške poruke, međusobno se ne isključuju. Na primjer, ako se želi odbaciti poruka identificirana kao neželjena poruka, ali karantena sumnja da je to neželjena poruku. Za svako pravilo elektroničke pošte može se odrediti granica za neku kategoriju i odrediti radnja koja će se poduzeti za svaku kategoriju. Razne politike mogu se dodijeliti različitim korisnicima i definirati različiti mehanizmi za pregledavanje, granice definicije neželjene pošte, kao i mjere za postupanje s neželjenom poštu.

Na sljedeći se način mogu konfigurirati mehanizmi za pregledavanje poruka za neželjenu poštu na Ironportu:

1. Na Ironportu je potrebno omogućiti opciju za skeniranje protiv neželjene pošte
2. Konfigurirati da li će se neželjeni sadržaj odložiti lokalno u karantenu na Ironportu-u ili koristiti vanjska karantena
3. Definirati grupe korisnika čije se poruke žele skenirati radi neželjene pošte
4. Konfigurirati pravila za zaštitu od neželjene pošte za grupu korisnika koja je definirana
5. Ukoliko je potrebno da određene poruke zaobiđu Cisco Anti-Spam skeniranje, mogu se kreirati filteri poruka koje zaobilaze anti-spam skeniranje
6. Omogućiti SenderBase Reputation Service bodovanje za svako pravilo ulazne pošte, čak i ako se ne odbijaju konekcije temeljene na rezultatima SenderBase Reputation Service
7. Ako se Ironport ne povezuje izravno s vanjskim pošiljateljima elektroničke pošte, nego umjesto toga prima poruke koje se prenose preko nekog drugog uređaja koji se nalazi mreži, potrebno je provjeriti da li dolazne poruke sadrže izvornu IP adresu pošiljatelja
8. Spriječiti da upozorenja i ostale poruke koje generira sustav ne budu pogrešno identificirane kao neželjene
9. Omogućiti filtriranje URL-ova kako bi se poboljšala zaštita od zlonamjernih URL-ova u porukama (opcionalno)
10. Testirati konfiguraciju
11. Konfigurirati postavke za ažuriranje sustava

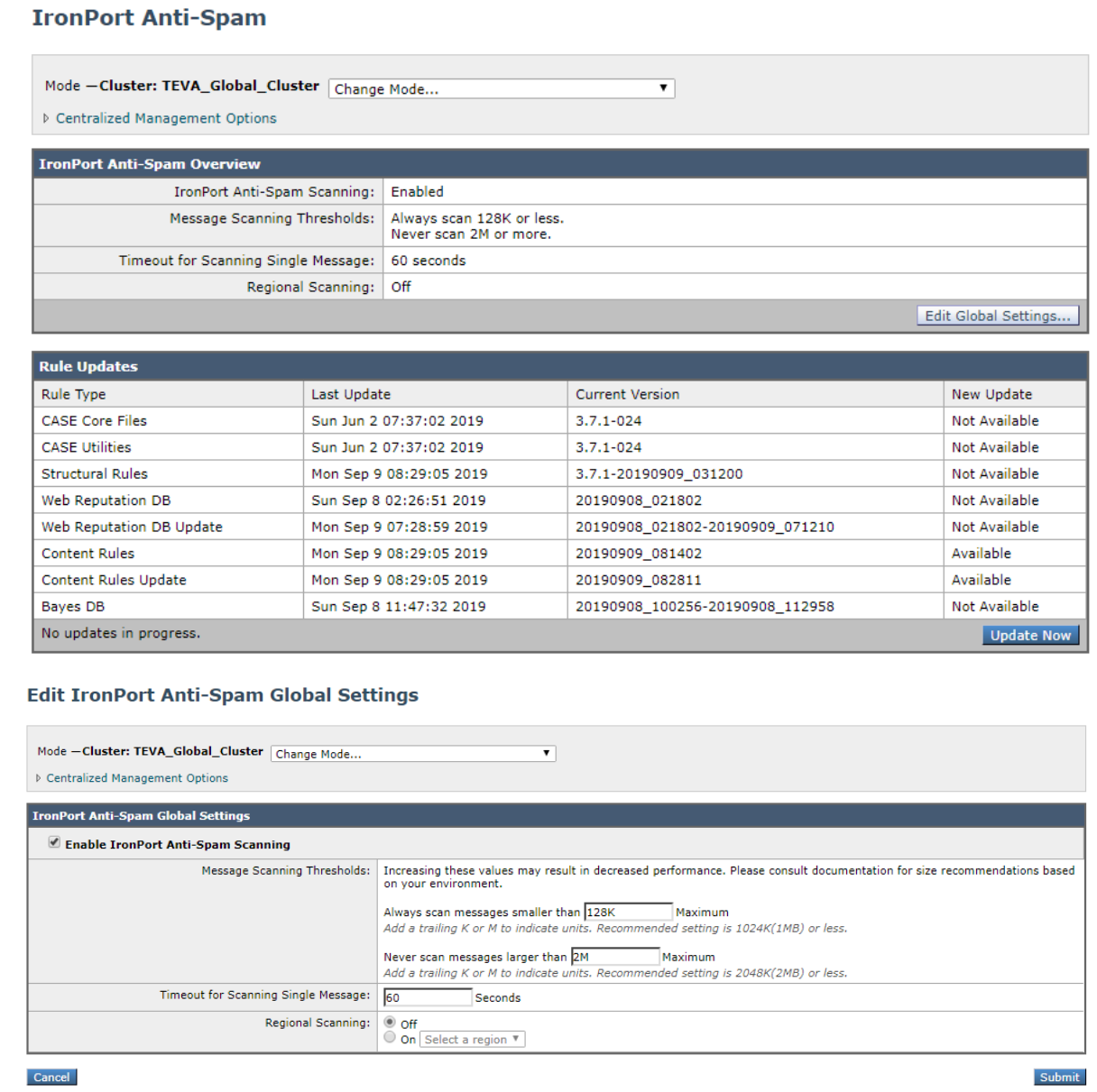
IronPort Anti-Spam obrađuje čitav niz poznatih prijetnji, uključujući neželjenu poštu, krađu identiteta i zombi napade. Da bi prepoznao ove prijetnje, IronPort ispituje cijeli kontekst poruke - njezin sadržaj, način na koji je kreirana poruka, reputaciju pošiljatelja, reputaciju web stranica oglašenih u poruci i druge parametre poruka. IronPort Anti-Spam kombinira podatke o elektroničkoj pošti i podatke o web reputaciji, iskorištavajući svu snagu najveće svjetske mreže

za praćenje elektroničke pošte i web prometa – SenderBase, a time ubrzavaju otkrivanje novih napada čim oni započnu.

Analiza šireg spektra odnosa omogućuje sustavu da uhvati širok raspon prijetnji uz održavanje točnosti. Na primjer, poruka koja ima sadržaj za koji tvrdi da potiče iz legitimne financijske institucije, ali koja je poslana sa sumnjive IP adrese ili sadrži URL smješten na zaraženom računalu, smatrat će se neželjenom. Suprotno tome, poruka farmaceutske tvrtke koja ima pozitivnu reputaciju neće biti označena kao neželjena pošta, čak i ako poruka sadrži riječi usko povezane sa listom zabranjenih riječi od strane administratora.

Konfiguracija IronPort-a za anti-spam pregledavanje (slika 10.):

1. Odabrati Security Services - > Ironport Anti-Spam
2. Ako nije aktiviran IronPort Anti-Spam u čarobnjaku za postavljanje sustava:
    - Odabrati Enable
    - Spustiti se na dno stranice do ugovora i kliknuti Accept za prihvaćanje ugovora
3. Odabrati Edit Global Settings
4. Markirati Enable IronPort Anti-Spam Scanning
5. Potrebno je konfigurirati od kuda će Ironport Anti-Spam početi skenirati poruke, kako bi se optimizirala propusnost dok je u mogućnosti skenirati veći broj poruka koje šalju neželjenu poštu
6. Izvršiti promjene.

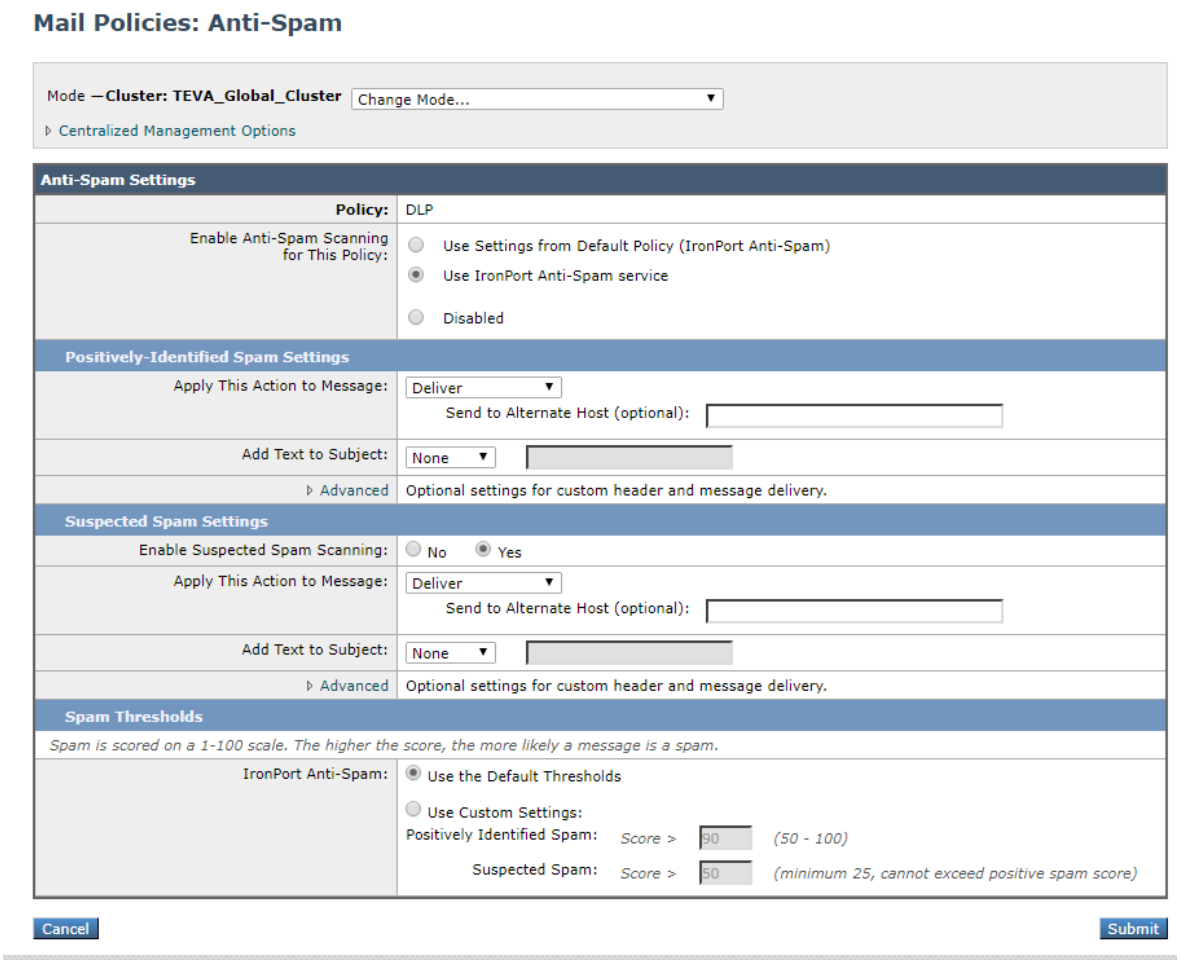


Slika 10. Konfiguracija IronPort-a za anti-spam pregledavanje

Za svako pravilo elektroničke pošte potrebno je odrediti postavke koje određuju koje se poruke smatraju neželjenom i koje će se mjere poduzeti za takve poruke. Također, odrediti gdje će se skenirati poruke u odnosu na koje pravilo se odabere. Mogu se konfigurirati različite postavke za zadana pravila o dolaznoj i odlaznoj pošti. Ako su potrebna različita pravila protiv neželjene pošte za različite korisnike, treba se upotrijebiti više različitih pravila sa različitim postavkama protiv neželjene pošte. Može se omogućiti samo jedno rješenje protiv neželjene pošte po pravilu, nikako se ne može omogućiti više rješenja u istom pravilu.

Postavljanje Anti-spam pravila putem Ironporta (Slika 11.):

1. Pod Mail Policies odabrati Incoming Mail Policies
2. Pod Mail Policies odabrati Outgoing Mail Policies
3. Odabrati opciju Anti-Spam iz izbornika
4. Pod Enable Anti-Spam Scanning for This Policy, odabrati rješenje protiv neželjene pošte koja se želi koristiti za to pravilo. Opcije koje su dostupne ovise o rješenjima za skeniranje protiv neželjene pošte koja je omogućena. Ako se koriste postavke iz zadanog pravila, sve ostale opcije su onemogućene
5. Konfigurirati postavke za identificiranu neželjenu poštu, sumnju na neželjenu poštu i marketinške poruke:
   - Omogućiti Suspected Spam Scanning
   - Odabrati Apply This Action to Message - odaberite općenitu akciju koja će se poduzeti za neželjenu poštu (isporuči, odbij ili karantena)
6. Izvršiti promjene



Slika 11. Postavljanje Anti-spam pravila

Najveća točnost se određuje pragom za identifikaciju neželjene pošte, a prema zadanim postavkama prilično je visoka: poruke s ocjenom između 90 i 100 smatraju se identificiranim

kao neželjena pošta. Inače, zadana ocjena za neželjenu poštu je 50. Poruke s ocjenama ispod sumnjivog praga za neželjenu poštu smatrat će se zakonitim. Poruke iznad sumnjivog praga, ali ispod praga za identifikaciju, smatrat će se neželjenom poštom. Zaštitu od neželjene pošte može se konfigurirati tako da odražava razine tolerancije prema neželjenoj pošti unutar organizacije. Prag za identificiranu neželjenu poštu može se promijeniti u vrijednost između 50 i 99. Može se postaviti prag za sumnju na neželjenu poštu u bilo koju vrijednost između 25 i vrijednost koja je navedena za identificiranu neželjenu poštu.

3.2.Malware napadi

Malware, odnosno zloćudni program, smatra se programom koji je umetnut unutar sustava sa jasnom namjerom za zloupotrebom integriteta ili otimanju korisničkih podataka, kao i ulaska u operacijske sustave. Koristeći nesigurne web stranice, adresa elektroničke pošte je sve što kradljivcu identiteta treba za izmjenu nečije lozinke. Nakon postavljanja nove lozinke korisnik više nema kontrolu, a zloćudni program preuzima račun za svoje potrebe. U tu svrhu spadaju više malicioznih radnji, od krađe identiteta do korištenja tuđeg računala za slanje neželjene pošte. Jedna od mnogih metoda krađe adresa elektroničke pošte koristi zloćudni program koji nadzire web stranice na mjestima gdje je potrebno upisati adresu elektroničke pošte prilikom registracije korisnika. Neki zloćudni programi djeluju tako da prate komunikaciju preko mreže i pokušavaju ukrasti adresu elektroničke pošte. Ako web stranica ne koristi enkripciju podataka, elektronička pošta i lozinka će se poslati vrlo vjerojatno sa vidljivim tekstom putem Interneta. Ako web stranica na koju se korisnik prijavljuje koristi sigurnosni protokol, kao što je HTTPS (eng. Hypertext Transfer Protocol Secure), podaci se kriptiraju dok su u tranzitu i vrlo teško ih je probiti. Nažalost, za većinu uspješno provedenih napada stvarni krivac je sam korisnik zbog svoje naivnosti, slabijeg znanja ili nemara. Drugim riječima, napadači najčešće prevare korisnika, te time nametnu korisniku štetnu radnju koji on izvrši. Danas postoje razne vrste zloćudnih programa, a slijedi lista nekolicine najpoznatijih:

- Virusi - program ili kod koji se sam replicira u drugim datotekama s kojima dolazi u kontakt. Može se nalaziti i zaraziti bilo koji program ili dokument koji podržava makronaredbe, tako da promijeni sadržaj te datoteke te u nju kopira svoj kod,
- Crvi - su računalni programi koji umnožavaju sami sebe. Pri tome koriste računalne mreže da bi se kopirali na druga računala, često bez sudjelovanja čovjeka. Crvi za svoje

djelovanje ne moraju inficirati druge programe, te otežavaju rad mreže, a mogu oštetiti podatke i kompromitirati sigurnost računala,

- Logičke bombe – je vrsta zloćudnog programa koji sam sebe aktivira određenog dana u određeno vrijeme, odnosno onda kada se koriste određeni procesi na računalu. Npr. mogu se aktivirati kada se pokrene određeni program na računalu, tipa Skype,
- Ransomware - je maliciozni kod koji korisniku blokira pristup računalu i od njega zahtjeva plaćanje otkupnine. Visina otkupnine i razlog zašto bi žrtva morala platiti ovisi o tipu virusa,
- Trojanski konji - predstavlja zloćudni program koji se korisniku lažno predstavlja kao koristan program s namjerom da mu korisnik dozvoli instalaciju. On može izmijeniti operacijski sustav na zaraženom računalu, ili u gorem slučaju, omogućiti napadaču potpuno kontrolu nad računalom,
- Špijunski programi - je nadgledanje aktivnosti korisnika računala, te često krađa osjetljivih informacija. Korisnikove aktivnosti obično se nadgledaju kako bi se utvrdile njegove navike,
- Botnet programi - je aplikacija koja izvršava sve naredbe koje primi od tzv. "master" aplikacije. Mreža računala na koje su instalirani Bot programi čini Botnet mrežu. Ovi programi obično se koriste za izvođenje distribuiranih DoS (eng. Denial of Service) napada. [9]

Zloćudni programi su prisutni na raznim mjestima, kao npr.:

- Internetskim stranicama koje služe kao neprovjerena mjesta na kojima se mogu preuzeti programi. Neprovjerena mjesta su nesigurna mjesta sa slabom zaštitom i slabom provjerom,
- Unutar službenih programa koji nisu ažurirani na vrijeme ili koji više nisu podržani od strane administratora. Također, i unutar službenih mjesta za preuzimanje programa jer u načelu se provode ozbiljnije mjere zaštite,
- Unutar malicioznih reklama i linkova zloćudni program se može proširiti i smatra se jednim od najkorištenijih napada.,
- Na vanjskim medijima za pohranu podataka. Trojanski konj može doći i u obliku USB sticka. Napadač negdje ostavi USB stick, Žrtva ga zatim pronađe i misli da je

[9] CCERT-PUBDOC-2008-11-247- Limbo Malware; dostupno na https://www.cert.hr/wp-content/uploads/2008/11/CCERT-PUBDOC-2008-11-247.pdf

to nečiji izgubljeni USB stick. Pokušavajući otkriti kome ga treba vratiti, ili iz znatiželje, žrtva priključuje USB stick u svoje računalo.

Bez sumnje se može reći da je zlćudni program jedan od najraširenijih i najbrže rastućih udara na sigurnost sustava, kao i korisnika. Razloge ovoga trenda treba prvenstveno tražiti u sve profinjenijim metodama kojima se autori zlćudnih programa koriste u njihovoj izradi, kao i u brojnim mutacijama već odavno poznatih primjeraka. Svaki zlćudni program i napadač koji ga prati, a koji želi učiniti uspješan napad pokušava u tišini izvršiti ciljanju akciju. Prijašnji napadači su izvršavali dosta velike i glasne napade, koji bi bili uočljivi i za koje bi se znalo. Zbog takvog napretka napadači više ne moraju biti osobe sa vrhunskim znanjem o računalnim operacijama, već se bilo tko može svrstati u ulogu napadača i pokušati izvesti napad. Bitno je napomenuti da se u zadnjih godinu dana (2018.-2019.) aktivnost zlćudnih programa povećala za 61%.[10] Te informaciju djeluju zabrinjavajuće, i stručnjaci rade na tome da suzbiju svim silama maliciozne aktivnosti.

Najčešće korišteni zlćudni programi koji su se koristili prošle godine u svrhu napada na korisnike i sustave su:

- Emotet - je modularni program koji preuzima ili odbacuje bankarske trojance. Može se isporučiti putem zlonamjernih internetskih poveznica sa kojih se preuzimaju privitci kao. npr. PDF ili Word dokumenti sa makronaredbama,
- WannaCry - je ransomware crypto crv koji koristi EternalBlue zlonamjerni kod koji se širi putem SMB protokola,
- Dridex - je inačica bankarskog programa koja koristi zlonamjerne makronaredbe unutar Microsoft Office programa sa umetnutim zlonamjernim privitcima.

3.2.1. Anti-malware implementacija kroz Ironport

Cisco Ironport uključuje integrirane programe za pregledavanje virusa od strane trećih kompanija kao npr. Sophos ili McAfee. McAfee i Sophos programi sadrže programsku logiku potrebnu za pregledavanje datoteka u određenim točkama, obradu virusa i podudaranja uzoraka s podacima koje pronalaze u datotekama. Također, dešifriraju i pokreću virusni kod unutar okruženja, primjenjuju heurističke tehnike za prepoznavanje novih virusa, te uklanjaju zarazni kod iz legitimnih datoteka. Program se može konfigurirati za pregledavanje poruka vezanim za

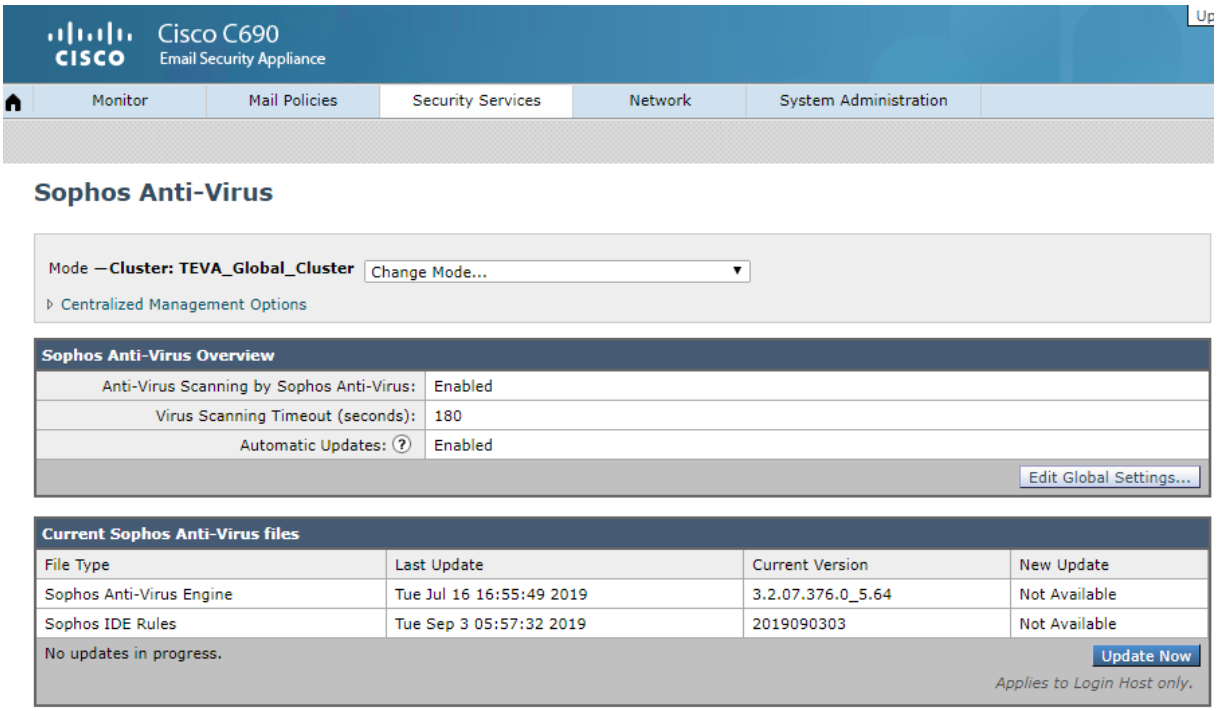
[10] Top 10 Malware January 2019 – CIS; dostupno na https://www.cisecurity.org/blog/top-10-malware-january-2019/

viruse (na temelju podudaranja pravila o dolaznoj ili odlaznoj pošti) i, ako se nađe virus, izvršiti različite radnje unutar poruke. Prema zadanim postavkama omogućeno je pregledavanje virusa za zadana pravila o dolaznoj i odlaznoj pošti. Mogućnostima programa za skeniranje upravlja kombinacija dvaju bitnih komponenti: klasifikator koji zna gdje tražiti, i baza podataka virusa koja zna što tražiti. Program traži viruse u tijelima i prilozima poruka koje je primio sustav, a vrsta datoteke koja se nalazi u privitku pomaže u određivanju načina skeniranja. Na primjer, ako je priložena datoteka poruke izvršna datoteka, program pregledava zaglavlje koje mu kazuje gdje započinje izvršni kod, kao i da li se kod nalazi na mjestu koje mu je i namijenjeno. Ako se radi o MIME datoteci, formatu koji se koristi za slanje poruka, pretražuje se mjesto na kojem se nalazi privitak. Tijekom procesa skeniranja program analizira svaku datoteku, identificira tip virusa i zatim primjenjuje odgovarajuću tehniku.

Može doći do ograničenja kada je u pitanju pregledavanje virusa, jer nije uvijek moguće vratiti datoteku u izvorno stanje. U tom slučaju definira se kako postupati s porukama koje sadrže dodatne priloge koji se ne mogu popraviti. Ove postavke konfiguriraju se na osnovi primatelja koristeći sljedeći oblik zaštite elektroničke pošte: Mail Policies -> Incoming or Outgoing Mail Policies (putem GUI-a) ili policyconfig -> antivirus command (CLI).

Način kako konfigurirati Ironport za pretraživanje virusa:

1. Omogućiti pretraživanje antivirusa na Ironportu
2. Odrediti grupe korisnika čije se poruke žele pretražiti
3. Konfigurirati na koji način karantena namijenjena za viruse obrađuje poruke (opcionalno)
4. Odrediti kako će sustav obraditi poruke sa virusima
5. Konfigurirati pravila za antivirusno pretraživanje za korisničke skupine koje su definirane
6. Poslati poruku elektroničke pošte, kako bi se testirala konfiguracija.



Slika 12. Konfiguracija Sophos antivirusa

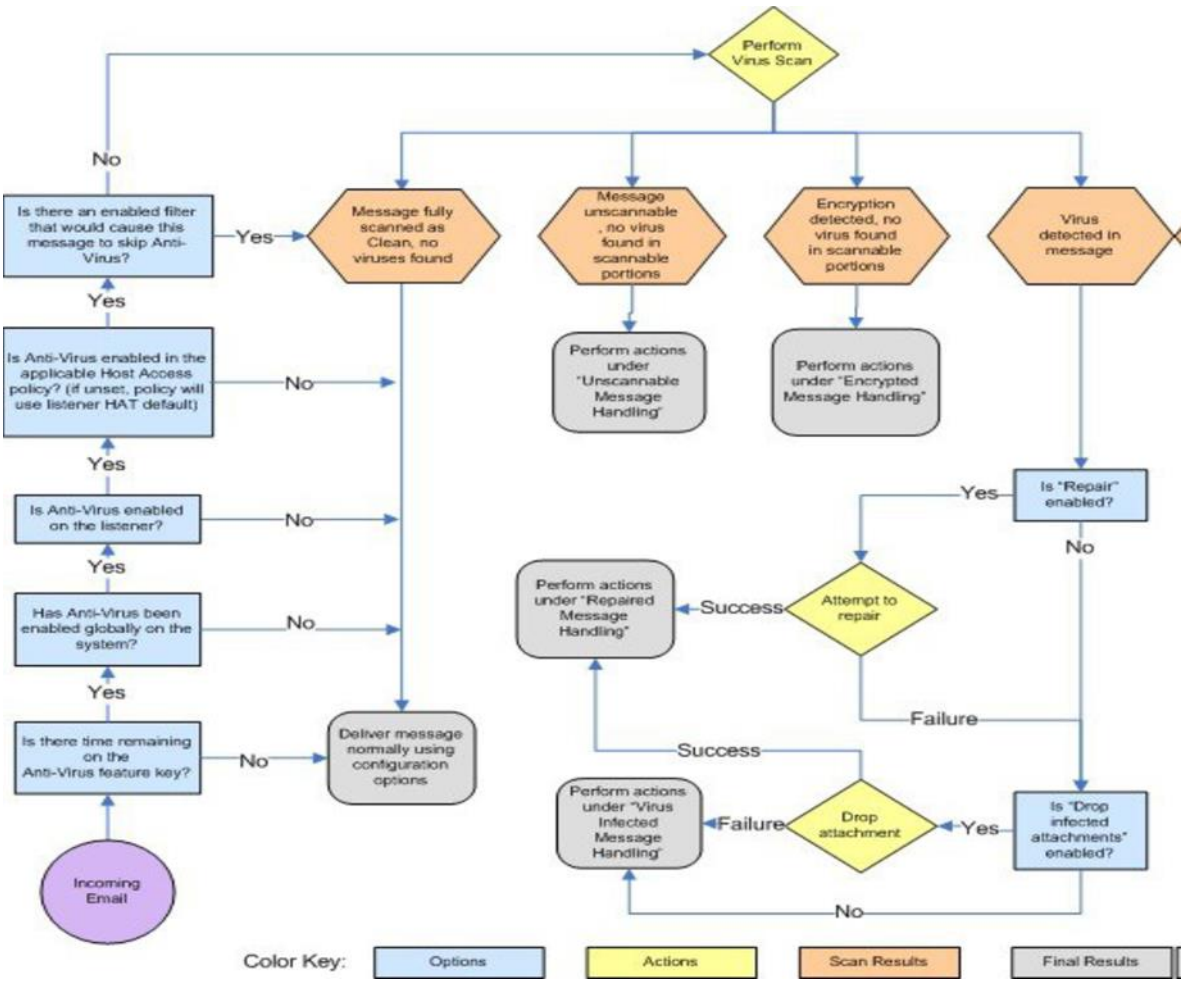
Kada je potrebno konfigurirati postavke kako se odnositi prema porukama elektroničke pošte koje su potencijalno opasne, bitno je odabrati akciju za svaku vrstu poruke za šifrirane, poruke koja se ne može skenirati ili poruke koje sadrže viruse, kako je i prikazano na slici 13. Primjer: poruka se odbacuje, šalje se kao privitak unutar nove poruke, šalje se takva kakva je ili se poruka šalje u karantenu za antivirus. Ako se odluči isporučiti poruku u originalu ili je isporučiti kao privitak novoj poruci, može se dodatno:

- Izmijeniti tema poruke,
- Arhivirati izvorna poruka,
- Poslati generalnu obavijest,
- Poslati poruku alternativnom odredišnom hostu,
- Poslati obavijest o upozorenju.[11]

Kada se označi za karantenu, poruka se nastavlja kretati kroz ostatak protokola elektroničke pošte. Kada poruka dođe do kraja ciklusa, poruka se sprema za jednu ili više karantena, te bude isporučena u jednu od njih. Ako poruka ne stigne do kraja ciklusa, neće biti stavljena u

[11] User Guide for AsyncOS 11.0 for Cisco Email Security Appliances, First Published: 2017-05-31

karantenu. Na primjer, filtriranje sadržaja može uzrokovati odbacivanje ili vraćanje poruke, u tom slučaju poruka neće biti isporučena u karantenu.



Slika 13. Dijagram puta poruke za pretraživanje virusa

3.3.DLP – Data Loss Prevention

DLP (eng. Data Loss Prevention) je skup alata i procesa koji se koriste kako bi se osiguralo da se osjetljivi podaci ne izgube, zloupotrebe, te da neovlašteni korisnici nemaju pravo pristupa istima. Također, bitna je stavka kod otkrivanja i sprečavanja krađe podataka ili neželjenog uništavanja osjetljivih podataka. Organizacije koriste DLP radi zaštite i ispravnog skladištenja svojih osjetljivih podataka i to trebaju raditi u skladu sa propisima. DLP klasificira regulirane, povjerljive i poslovne kritične podatke i identificira kršenje pravila definiranih od strane organizacija ili unutar unaprijed definiranog skupa politika, obično vođenih regulatornim usklađivanjem poput GDPR-a (eng. General Data Protection Regulation). [12]Gubitak podataka smatra se događaj u kojem su izgubljeni važni podaci za organizaciju, a za primjer napada možemo uzeti zloglasni ransomware. Prevencija protiv gubitka podataka usmjerena je na sprječavanje ilegalnog prijenosa podataka izvan granica organizacije. Organizacije najčešće koriste DLP radi:

- Zaštite osobnih podataka u skladu sa relevantnim propisima,
- Zaštite intelektualnog vlasništva kritičnog za organizaciju,
- Osiguranja komunikacije preko mobilnih uređaja, te sigurnosti BYOD (eng. Bring Your Own Device) uređaja,
- Zaštite podataka na udaljenim oblačnim sustavima.[13]

Tri su uobičajena uzroka curenja podataka:

- Prijetnja unutar organizacije - napadač koji je kompromitirao administratorski račun, zloupotrijebio prava pristupa i prebacuje podatke izvan organizacije,
- Ciljani napadi - napadači prodiru kroz sigurnosni perimetar koristeći tehnike poput phishinga, injekcije zlonamjernog programa ili koda za pristup osjetljivim podacima,
- Nenamjerno ili nemarno izlaganje podataka – veliki broj izgubljenih podataka nastaje kao posljedica nemarnih korisnika koji izgube osjetljive podatke.

[12] Ellen Zhang: What is Data Loss Prevention (DLP)? A Definition of Data Loss Prevention; dostupno na https://digitalguardian.com/blog/what-data-loss-prevention-dlp-definition-data-loss-prevention

[13] Data Loss Prevention (DLP) – Imperva; dostupno na https://www.imperva.com/learn/data-security/data-loss-prevention-dlp/

Dobro je koristiti standardne sigurnosne alate za obranu od gubitka i curenja podataka. Na primjer, IDS (eng. Intrusion Detection System) može upozoriti na pokušaje napadača da pristupi osjetljivim podacima. Vatrozid može blokirati pristup sa neovlaštene strane sustavima za pohranu osjetljivih podataka. Rješenja kojima se može spriječiti DLP objašnjena su sljedećim mehanizmima:

- Osiguravanje podataka koji se razmjenjuju - tehnologija instalirana na rubu mrežnog protokola može analizirati promet radi otkrivanja osjetljivih podataka poslanih u suprotnosti sa sigurnosnim pravilima,
- Osiguravanje pohranjenih podataka - pravila o kontroli pristupa, šifriranju i zadržavanju podataka mogu zaštititi arhivirane podatke,
- Identifikacija podataka - ključno je utvrditi treba li podatke zaštititi ili ne,
- Otkrivanje curenja podataka - DLP rješenja i drugi sigurnosni sustavi poput IDS-a identificiraju prijenos podataka koji je sumnjiv.

Gartner procjenjuje da će ukupno DLP tržište doseći 1,3 milijarde dolara u 2020. Zajedno s rastućim trendom curenja podataka, dovelo je do toga da se DLP počeo masivno prihvaćati kao ključna preventivna opcija. Ovo su neki od trendova koji idu na ruku DLP-u kao glavnom alatu za sprečavanje curenja podataka:

- Uloga CISO-a sve više napreduje - sve više tvrtki angažira i zapošljava glavnog inženjera za informacijsku sigurnost (eng. Chief Information Security Officer), koji najčešće odgovaraju izvršnom direktoru. CEO-i žele znati koji je plan za sprječavanje curenja podataka. DLP pruža jasnu poslovnu vrijednost u tom pogledu i pruža CISO-ima sve što je potrebno za izvještaj izvršnog direktora,
- Krađa podataka je u sve većem porastu - cyber kriminalci i zlonamjerni korisnici unutar organizacije ciljaju na osjetljive podatke koje koriste za razne kriminalne akcije,
- Podaci unutar organizacije danas vrijede više – ukradeni podaci često završe na crnom tržištu
- Sve više podataka koji se mogu ukrasti - osjetljivi podaci sada uključuju nematerijalnu imovinu, kao što su modeli zarade i poslovne metodologije.

Čak i mali udar na sigurnosti elektroničke pošte može biti vrlo skup za organizaciju. Organizacije koje se bave provedbom GDPR-a već su započele sa provođenjem oštrih mjera donošenjem ogromnih novčanih kazni za prijestupnike. Smatra se da će u budućnosti te mjere biti i strože. sa tim podacima. Kada korisnik pokuša poslati poruku koja nije u skladu sa pravila,

program mora pokrenuti jednu ili više radnji na temelju pravila koja su odabrana. Pravila uključuju:

- Upozorenje korisnika,
- Kriptiranje poruke elektroničke pošte,
- Micanje privitaka iz poruke,
- Slanje kopije elektroničke poruke administratorima.

Dobar program može pružiti veliki broj različitih sigurnosnih rješenja. Neki od programa i alata koji se mogu koristiti za kontrolu pristupa određenim podacima i način na koji se njima upravlja su:

- Symantec Data Loss Prevention – ovaj program se koristi za nadgledanje sumnjivog ponašanja, posebno programa instaliranih od strane korisnika. Također može prepoznati i zaustaviti programe da pristupaju zaštićenim informacijama, kao i spriječiti bilo kakve prijenose podataka koji nisu u skladu za regulativom,
- McAfee Total Protection for Data Loss Prevention - ide korak dalje od većine istražujući na koje načine su podaci mogli procuriti u nedostatku internih pravila i propisa. To je prikladno za organizacije koje možda nemaju konkretna korporativna pravila.
- Check Point Data Loss Prevention - cilj mu je educirati korisnike o riziku gubitka podataka i pomoći im da odgovore na incidente što je brže moguće. To se postiže praćenjem korištenja podataka na svim servisima, pri elektroničkoj pošti, pretraživanju weba i dijeljenju datoteka.

Rizici od curenja podataka u brojkama:

- 26% organizacija smatra da će njihove tvrtke biti usklađene sa GDPR regulativom,
- 22% organizacija smatra da je GDPR njihov glavni prioritet,
- 14% organizacija ima 50% ili više korisnika koji su izloženi velikom riziku u kontekstu curenja osobnih podataka,
- 4% godišnjeg prihoda ili 20 milijuna eura, ovisno koji je iznos veći potencijalna je maksimalna kazna u slučaju incidenta. [14]

[14] Krešimir Vinšćak: Symantec DLP: štitite li povjerljive i osobne podatke u vašoj organizaciji?; dostupno na: https://veracompadria.com/hr/symantec-dlp-stitite-li-povjerljive-i-osobne-podatke-u-vasoj-organizaciji/

Studija iz 2019. otkrila je da žrtve cyber kriminala i curenja podataka ne samo da gube trenutne i potencijalne kupce, već postoji velika vjerojatnost da će izgubiti i potencijalne ulagače. Studija je utvrdila da će 69% ulagača teže uložiti u organizaciju koja je pretrpjela jedno ili više curenja podataka izvan organizacije. Pri tome se vidi da i samo curenje podataka može imati katastrofalne posljedice za bilo koju organizaciju.

3.3.1.DLP implementacija kroz Ironport

Kada netko unutar organizacije pošalje primatelju poruku van organizacije, Ironport određuje koja se pravila o odlaznoj pošti primjenjuju na pošiljatelja ili primatelja te poruke, bazirano na temelju pravila koja su definirana. Ironport procjenjuje sadržaj poruke koristeći DLP pravila koja su navedena u toj politici odlazne pošte. Konkretno, on skenira sadržaj poruke (uključujući zaglavlja i privitke) i traži tekst koji se podudara s riječima i izrazima, kao i unaprijed definiranim podacima (poput brojeva socijalnog osiguranja, bankovnog računa) koji su prepoznati kao osjetljiv sadržaj u primjenjivoj DLP politici. Ironport također ocjenjuje kontekst nedopuštenog sadržaja kako bi umanjio lažna podudaranja. Ako sadržaj poruke odgovara više od jednom DLP pravilu, primjenjuje se prvo podudaranje DLP pravila sa liste, temeljeno na redoslijedu koji je naveden. Ako pravila o odlaznoj pošti imaju više DLP pravila koja koriste iste kriterije za određivanje kršenja sadržaja, sva pravila koriste rezultat jedinstvenog skeniranja sadržaja. Kad se u poruci pojavi potencijalno osjetljiv sadržaj, dodjeljuje se ocjena o faktoru rizika između 0 i 100 za potencijalno narušavanje sigurnosti. Ovaj rezultat ukazuje na vjerojatnost da poruka sadrži kršenje DLP-a. Ironport zatim dodjeljuje razinu ozbiljnosti situacije (kritična ili niska) koja je definirana prema ocjeni faktora rizika, te provodi mjere prema razini ozbiljnosti koja je određena unutar stvorenih DLP pravilima.

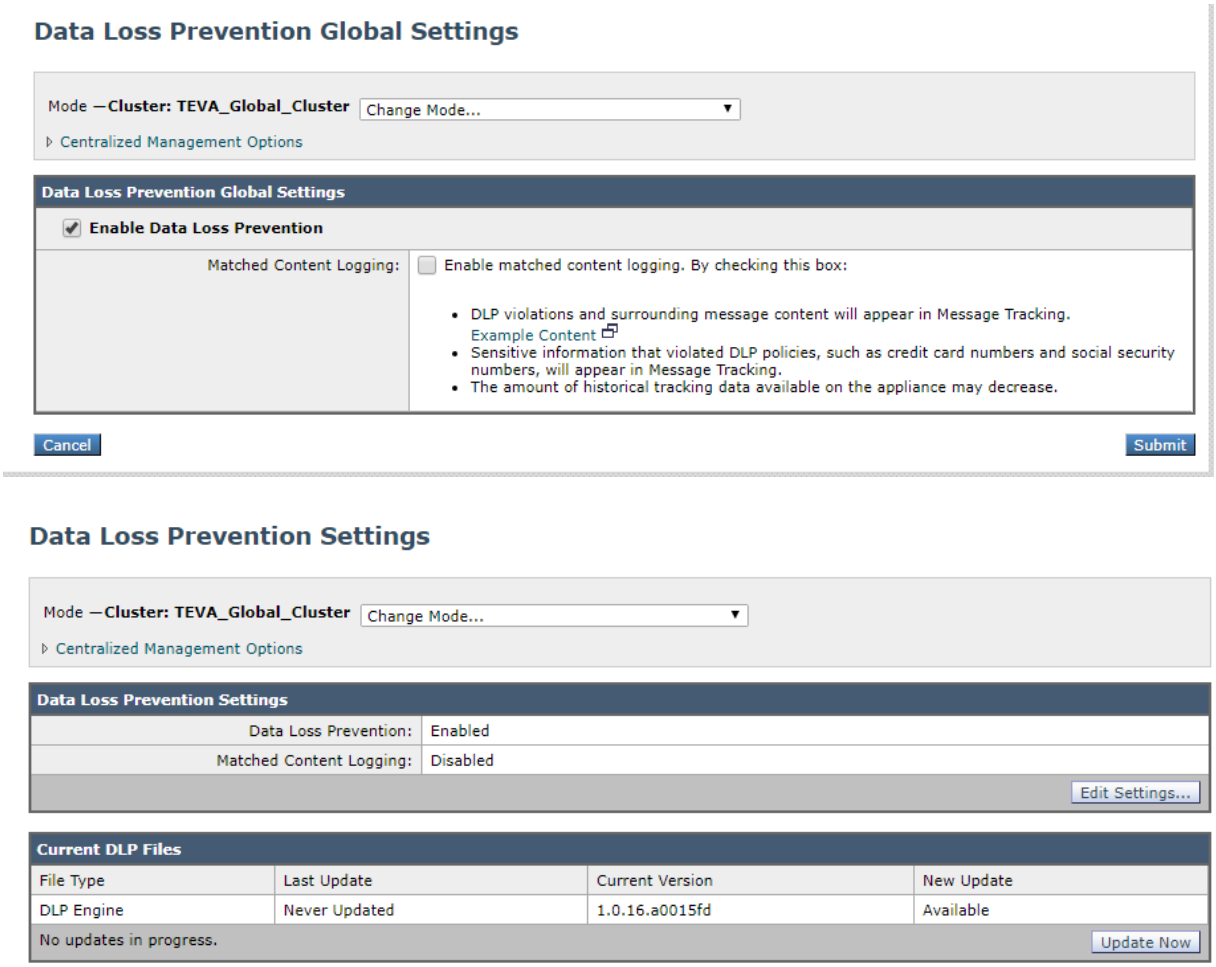
DLP se može konfigurirati na sljedeći način:

1. Omogućiti DLP kao opciju
2. Definirati odgovarajuće radnje za poruke u kojima su pronađena kršenja pravila ili se sumnja na njih. Na primjer, staviti takve poruke u karantenu
3. Stvoriti DLP pravila koja identificiraju sadržaj koji ne smije biti poslan elektroničkom poštom izvan organizacije ili odrediti koje će se radnje poduzeti za svako kršenje pravila
4. Postaviti redoslijed DLP pravila kako bi se odredilo koje se DLP pravilo koristi za procjenu kada bi se sadržaj mogao podudarati s više DLP pravila

5. Provjeriti jesu li kreirana pravila za odlaznu poštu za svaku skupinu pošiljatelja ili primatelja čije će se poruke skenirati u slučaju kršenja DLP-a
6. Navesti koja se DLP pravila primjenjuju na koje pošiljatelje ili primatelje dodjeljivanjem DLP pravila za odlaznu poštu
7. Konfigurirati postavke za pohranu i pristup osjetljivim DLP informacijama.

DLP se mora omogućiti na Ironportu, kako bi se aktivno počeo primjenjivati, prema slici 14.:

1. Odabrati opciju Security Services > Data Loss Prevention -> Enable
2. Prihvatiti sve postavke iz ugovora
3. Pod Data Loss Prevention Global Settings, odabrati Enable Data Loss Prevention
4. Izvršiti promjene.



Slika 14. Konfiguracija DLP-a

DLP pravila uključuju:

- skup uvjeta koji određuju sadrži li odlazna poruka osjetljive podatke,
- radnje koje treba poduzeti kada poruka sadrži takve podatke.

Za jednostavnije kreiranje DLP pravila, Ironport koristi veliku zbirku unaprijed definiranih predložaka pravila. Kategorije predložaka uključuju:

- Usklađivanje propisa - predlošci koji identificiraju poruke i privitke koji sadrže osobne podatke, podatke o karticama ili druge zaštićene podatke,
- Zaštita privatnosti – predlošci koji identificiraju poruke i privitke koji sadrže financijske račune, porezne evidencije ili osobne iskaznice,
- Zaštita intelektualnog vlasništva – predlošci koji identificiraju vrste dokumenta koji su na cijeni i koji mogu sadržavati intelektualno vlasništvo koje bi organizacija željela zaštititi,
- Predložak prilagođen za organizaciju – omogućuje kreirati vlastita pravila od početka, koristeći unaprijed definirane sadržaje koji se podudaraju sa kriterijima za prepoznavanje kršenja sigurnosti koje je odredila organizacija.

Ovako se mogu kreirati DLP pravila koristeći unaprijed definirane predloške (slika 15.):

1. Odabrati Mail Policies > DLP Policy Manager
2. Odabrati Add DLP Policy
3. Kliknuti na naziv kategorije kako bi se prikazao popis dostupnih predložaka DLP pravila
4. Odabrati Add za DLP predložak koji je potreban
5. Promijeniti predefinirano ime i opis predloška (opcionalno)
6. Primijeniti DLP pravila samo na poruke s određenim primateljima, pošiljateljem, vrstama privitaka ili prethodno dodanim oznakama poruka,
7. Potrebno odabrati mjeru koja se treba poduzeti za svako ozbiljnije kršenje sigurnosti, na način da se odabere Edit Scale
8. Izvrši promjene.

DLP Policy Manager

Mode —**Cluster: TEVA_Global_Cluster** Change Mode...

▷ Centralized Management Options

Active DLP Policies for Outgoing Mail

Add DLP Policy...

Order	DLP Policy	Duplicate	Delete
1	Teva Financial Reports		
2	Mergers and Acquisitions		
3	Teva Employee Details		

Edit Policy Order...

Advanced Settings

Custom DLP Dictionaries: (for use in Custom Policies only)	None Available

DLP Policy Manager: Add DLP Policy

Mode —**Cluster: TEVA_Global_Cluster** Change Mode...

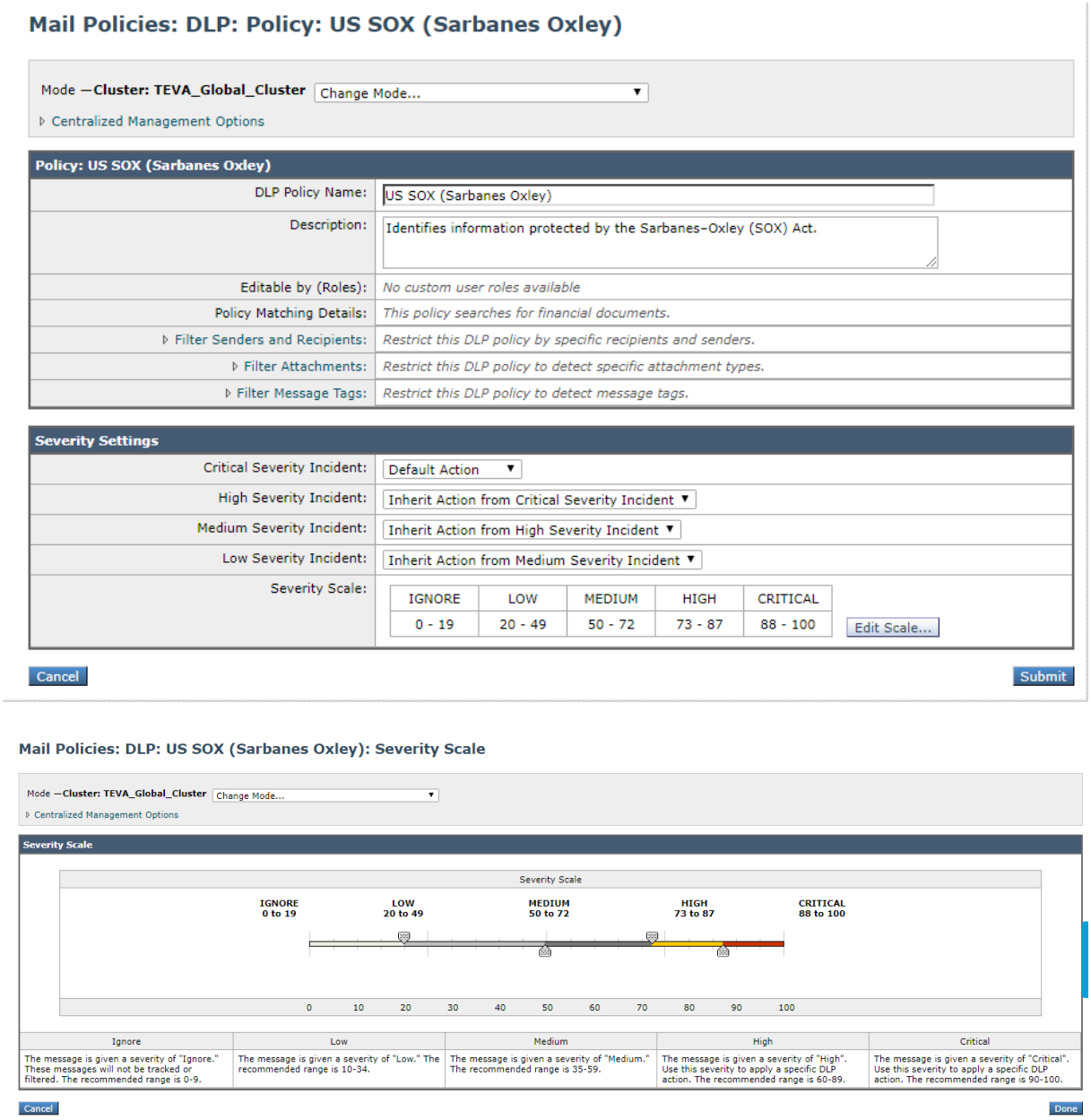
▷ Centralized Management Options

Add DLP Policy from Templates

Display Settings: Expand All Categories | Display Policy Descriptions

▽ Regulatory Compliance	
Add	**Canada PIPEDA (Personal Information Protection and Electronic Documents Act)**
Add	**PCI-DSS (Payment Card Industry Data Security Standard)**
Add	**US FERPA (Family Educational Rights and Privacy Act)** *Customization recommended.*
Add	**US GLBA (Gramm Leach Bliley Act)** *Customization recommended.*
Add	**US HIPAA and HITECH** *Customization recommended.*
Add	**US HIPAA and HITECH (Low Threshold)** *Customization recommended.*
Add	**US SOX (Sarbanes Oxley)**
▷ US State Regulatory Compliance	
▷ Acceptable Use	
▷ Privacy Protection	
▽ Intellectual Property Protection	
Add	**File Types (Design Documents)** *Customization recommended.*
Add	**File Types (Publishing Documents)** *Customization recommended.*
▷ Company Confidential	
▽ Custom Policy	
Add	**Custom Policy** (Advanced) This option is considered advanced and should be used only in rare cases when the policy templates above do not meet unique requirements of your network environment.

« Back



Slika 15. Konfiguriranje DLP sa unaprijed definiranim predlošcima

Ironport dolazi s setom unaprijed definiranih rječnika (eng. Dictionaries), ali mogu se kreirati i prilagođeni DLP rječnici, kako bi se odredili pojmovi za skeniranja DLP-a. Prilagođeni DLP rječnik može se kreirati na nekoliko načina:

- Izravno dodavanje prilagođenih DLP rječnika,
- Kreiranje DLP rječnika kao tekstualna datoteka,
- Izvoz DLP rječnika s drugog uređaja za zaštitu elektroničke pošte.

Izravno dodavanje prilagođenih DLP rječnika (slika 16.):

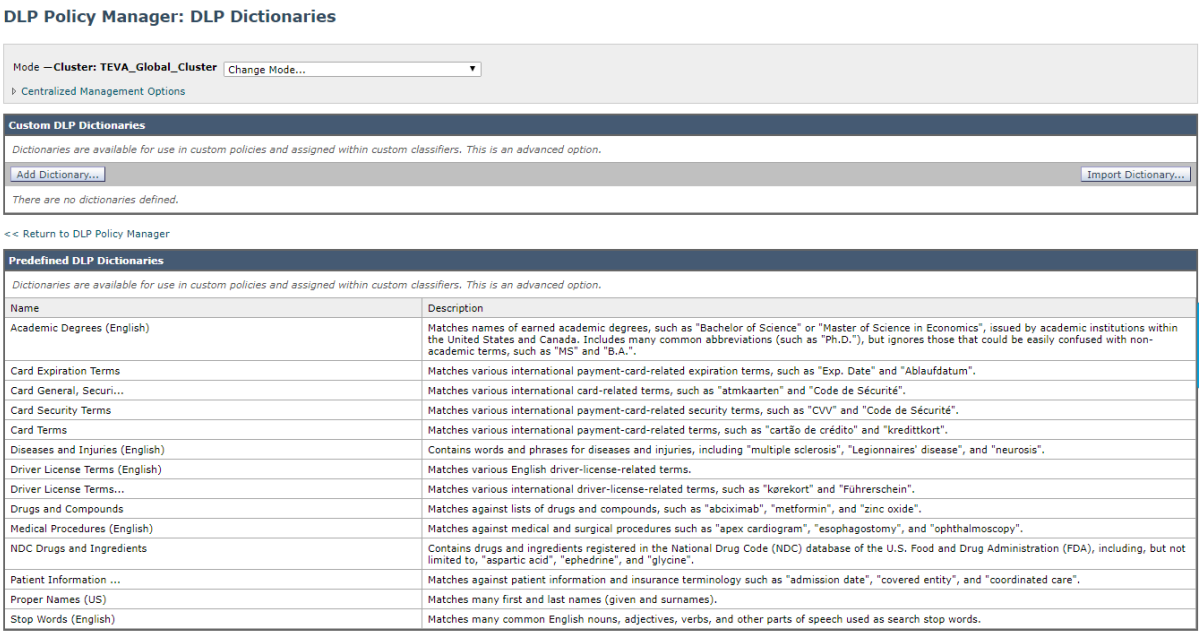
1. Odabrati Mail Policies > DLP Policy Manager
2. Pod Advanced Settings odabrati Custom DLP Dictionaries
3. Odabrati Add Dictionary
4. Upisati ime prilagođenog rječnika
5. Potrebno upisati nove stavke u rječnik (riječi i izraze) pod popis pojmova.
6. Odabrati Add i izvršiti promjene.

Kreiranje DLP rječnika kao tekstualna datoteka – može se stvoriti vlastiti rječnik kao tekstualnu datoteku na lokalnom računalu i uvesti ga na Ironport.

Izvoz DLP rječnika s drugog uređaja za zaštitu elektroničke pošte:

1. Odabrati Mail Policies > DLP Policy Manager,
2. Pod Advanced Settings odabrati Custom DLP Dictionaries,
3. Odabrati Export Dictionary,
4. Upisati ime datoteke za rječnik,
5. Odabrati gdje se treba spremiti rječnik na lokalnom računalu ili u konfiguracijskom imeniku na Ironportu,
6. Odabrati kodiranje datoteke
7. Izvrši promjene

Uvoz DLP rječnika se izvodi na gotovo isti način kao i izvoz, jednina razlika je u tome što se u 3. koraku odabire opcija Import Dictionary, te se dalje slijede ostali koraci.



Slika 16. DLP rječnik

3.4.Phishing napadi

Phishing napadi uvelike se zasnivaju na primjeni elektroničke pošte, i u stalnom su porastu. Prilikom phishing napada, napadači pokušavaju priskrbiti povjerljive korisničke podatke, koji im omogućavaju izravno ili neizravno ostvarivanje nekakve koristi. U većini slučajeva napadači uspješno dolaze do zaporki, PIN-ova kreditnih kartica te ostalih povjerljivih podataka koji napadaču daju pravo pristupa sustavu ili organizaciji. Phishing napad se temelji na tehnikama socijalnog inženjeringa (eng. Social engineering), čime se zloupotrebljava neznanje korisnika. Napadači pokušavaju stvoriti lažne poruke elektroničke pošte i korisnika navesti da nesvjesno preda vlastite povjerljive podatke. Probleme predstavljaju i razne ranjivosti koje se nalaze unutar Web preglednika i klijenata elektroničke pošte, te one u spoju sa naprednim tehnikama napada predstavljaju snažan alat u napadačevim zamislima. Phishing napadi se sastoje od tri faze:

- Razvijanje i organiziranje napada – faza u kojoj se prikupljaju sve relevantne informacije o meti napada koja se želi napasti, te se proučavaju sigurnosni propusti,
- Izvlačenje povjerljivih podataka – faza u kojoj se prikupljaju sve relevantne informacije o žrtvi napada,
- Izvršavanje napada – faza u kojoj se napad počinje sprovoditi u djelo, te se šalju zaražene poruke elektroničke pošte prema meti napada, koristeći ukradene adrese elektroničke pošte.

Kao i kod svakih napada postoje razne tehnike za njihovo ostvarivanje:

- Man in the Middle napadi – napad u kojem napadač ulazi u komunikaciju između klijenta i poslužitelja tako da ih uvjeri da klijent i poslužitelj komuniciraju direktno dok napadač u stvari preuzima cijelu komunikaciju bez znanja ostalih sudionika komunikacije,
- Maskiranje URL adresa – smatra se jednom od najkorištenijih tehnika. URL adrese koje se nalaze unutar poruke elektroničke pošte, uz pomoć specijaliziranih programa, preusmjeravaju se na maliciozne Web stranice, koje korisnik zbog malih izmjena ne može prepoznati kao lažne,
- Cross Site Scripting - tehnika kojom napadač u korisničkom web pregledniku izvodi podmetnuti programski kod, što mu omogućuje prikupljanje različitih osjetljivih podataka dostupnih pregledniku,

- Tabnabbing - tehnika pri kojoj se pokušava zamijeniti pozadinska kartica zlonamjernim dokumentom. Ova akcija također mijenja adresnu traku na pozadinskoj kartici, ali napadač se nada da će žrtva biti manje pažljiva i slijepo će unijeti svoju lozinku ili druge osjetljive podatke kada se vrati na karticu.

Zaštiti se od phishing napada nije laka misija, s obzirom na njegove mehanizme. Tehničke segmente potrebno je eliminirati odgovarajućim sigurnosnim provjerama koje će onemogućiti izvršavanje napada (sigurno programiranje, redovita instalacija sigurnosnih zakrpi), dok je probleme socijalnog inženjeringa moguće smanjiti preventivnom edukacijom i podizanjem svijesti korisnika. Pružanje pravovremenih informacija i održavanje edukacija trebao bi biti glavni motiv za sprječavanje potencijalnih napada. Korisnici mogu prepoznati phishing napad na elektroničku poštu prema sljedećim parametrima:

- Ucjene ili nagrade – napadač koristi priliku isprovocirati sreću korisnika i privući ga lažirajući link koji nudi nagradu. Prilikom ucjenjivanja najčešće se napada na korisnički račun,
- Gramatičke greške – s obzirom da se napadači žure i ne mare puno za pravopis, često se može vidjeti prilikom phishing napada da npr. linkovi sadrže gramatičke pogreške. Samim time može se zaključiti da nije validan link ili adresa jer ozbiljne organizacije nemaju problema sa gramatikom,
- Imitacija poznatih organizacija ili adresa – jedan od najčešćih parametara za prepoznavanje phishing napada. Pokušaj prevare u sitnim izmjenama unutar adrese elektroničke pošte, u vidu promijene samo jednog slova, ili rasporeda unutar adrese. [15]

Poruke elektroničke pošte vrlo je lako lažirati, što napadači vrlo često koriste kako bi zavarali korisnike i povećali učinkovitost svojih napada. Digitalnim potpisivanjem poruka moguće je znatno podići razinu sigurnosti sustava elektroničke pošte. Korištenjem asimetrične kriptografije i certifikata osigurava se autentičnost, integritet i povjerljivost poruke što je temeljni sigurnosni zahtjev kod modernih informacijskih sustava.

S obzirom, da postoji više vrsta phishing napada, ovo je lista najčešćih:

1. Deceptive phishing - Najčešći oblik phishing napada kod kojeg se napadači predstavljaju kao legitimna organizacija te traže od žrtava da predaju svoje osobne podatke

[15] ZAŠTITA OD PHISHINGA; dostupno na https://www.t.ht.hr/drustvena-odgovornost/modal-phishing/

2. Spear phishing - Oblik phishing napada kod kojeg se poruke kroje posebno za svaku žrtvu na temelju prethodno prikupljenih podataka o žrtvi
3. Whailing - Phishing napad kojim se ciljaju ljudi na vodećim pozicijama unutar tvrtke kako bi se putem njihovih podataka ostvario pristup većoj količini povjerljivih podataka
4. SMSiSHing - Vrsta napada kod kojeg se koriste SMS poruke kako bi se došlo do osjetljivih podataka.[16]

[16] DESET NAJČEŠĆIH VRSTA PHISHING NAPADA – Cert.hr; dostupno na https://www.cert.hr/deset-najcescih-vrsta-phishing-napada/

4.Autentikacija elektroničke pošte

4.1.SPF – Sender Policy Framework

SPF (eng. Sender Policy Framework) protokol je koji se zasniva na objavljivanju MX zapisa koji predstavlja neko računalo sa kojeg će se slati elektronička pošta za danu domenu. Da bi sve funkcioniralo potreban nam je DNS poslužitelj kojim se obavlja usmjeravanje korisničkih zahtjeva. MX zapis DNS poslužitelja registrira računalo koje prima elektroničku poštu za danu domenu. SPF protokol je dizajniran tako da se nadograđuje na SMTP protokol iz razloga što SMTP protokol ne uključuje jasan mehanizam autentikacije korisnika. Kroz najjednostavniji primjer može se objasniti na koji način se SPF protokol koristi u praksi (slika 17.). Naime, kako bi poruka elektroničke pošta bila poslana na siguran način prvo se mora objaviti SPF zapis na DNS poslužitelju, jer se time definira ovlašteni poslužitelji za slanje elektroničke pošte za danu domenu. Poslužitelj elektroničke pošte koji prima poruku, također mora podržavati SPF protokol, te kada primi poruku elektroničke pošte s domene sa koje je poruka poslana, odgovara slanjem DNS SPF upita. Time se vrši provjera da li je adresa s koje je poruka stigla ovlaštena slati poruke elektroničke pošte za tu domenu, te ako postoji SPF zapis koji ukazuje da je stvarno tome tako, poslužitelj elektroničke pošte prihvaća zaprimljenu poruku. U suprotnom, pošta se odbacuje. SPF protokol prije svega štiti adresu koja se nalazi u Return-Path zaglavlju poruke. Ta adresa ne mora biti jednaka adresi koja se nalazi u From zaglavlju, ali predstavlja adresu na koju se vraća poruka u slučaju da poruka nije isporučena. [17]

Važan aspekt koji treba razumjeti kod SPF protokola je taj da se on ne validira s From zaglavlja, već u Return-Path zaglavlju poruke kako bi potvrdio autentičnost poslužitelja sa kojeg je poruka poslana. Return-Path je adresa elektroničke pošte koju poslužitelji koji primaju poruku upotrebljavaju za obavještavanje poslužitelja sa kojih je poruka poslana o problemima s isporukom. Tako da poruka elektroničke pošte može zaobići SPF protokol bez obzira na to što je From adresa lažna. Problem je u tome što primatelji vide ono što je došlo i što piše u From adresi unutar klijenta elektroničke pošte. Nadalje, čak i ako poruka uspije zaobići SPF protokol, ne postoji garancija da se neće isporučiti. Konačna odluka o isporuci ovisi o poslužitelju koji prima poruku. Kad je riječ o provjeri adrese koja se šalje sa From zaglavlja, DMARC je relativno novi standard dizajniran za rješavanje ovog nedostatka u SPF protokolu. SPF protokol neće riješiti sve probleme sa isporukom poruke, ali služi kao dodatni sigurnosni sloj koji u

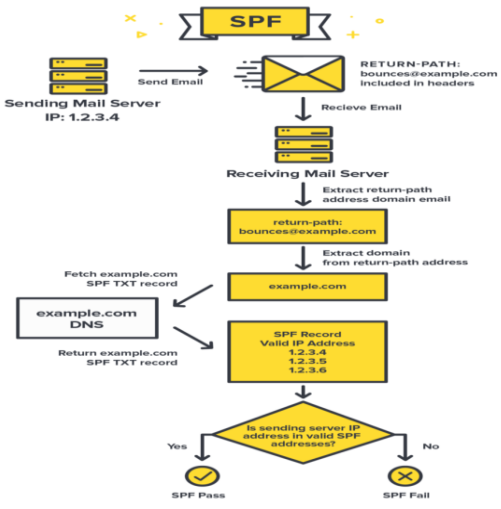
[17] CCERT-PUBDOC-2006-02-148 Sender Policy Framework; dostupno na https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-02-148.pdf

kombinaciji s DKIM-om i DMARC-om može poboljšati razinu isporuke poruka i spriječiti zloupotrebu istih. No o njima će biti više govora u nastavku rada.

SPF protokol ima nekoliko mana:

- SPF zapisi se teško mogu ažurirati ukoliko organizacija promijeni pružatelja usluge,
- Čak i ako poruka bude blokirana od strane SPF-a, ne znači nužno da će neće biti isporučena u korisnikov pretinac,
- Kada se poruka prosljeđuje, SPF protokol se prekida,
- SPF ne štiti organizaciju od napada koji su koncipirani na način da se krivotvori From zaglavlje adrese pošiljatelja.

Većina sustava zahtjeva samo TXT zapis u DNS-u za implementaciju SPF protokola. TXT zapis objedinjuje više vrijednosti unutar kratkog tekstualnog zapisa. Davatelj usluge može zatražiti da administrator unutar organizacije sam dodjeli TXT zapis, koji se onda kao cijeli tekstualni zapis kopira u SPF zapis. Najčešća pogreška prilikom postavljanja SPF-a je ako postoji više SPF TXT zapisa unutar DNS-a. Time se radi veliki problem prema poslužitelju koji neće znati koji je SPF TXT konačan i ispravan. Rezultat takve konfiguracije je neuspjela autentikacija SPF-a na poslužitelju. Stoga, kad god postoji potreba za dodavanjem podataka potrebnih za konfiguraciju SPF-a, potrebno je prvo provjeriti da ne postoji SPF TXT zapis.



Slika 17. Shema SPF protokola

4.1.1.SPF zapisi

Termin SPF zapis odnosi se na DNS zapis koji označava IP adrese računala ovlaštenih za slanje elektroničke pošte za danu domenu. Domena ne smije imati višestruke SPF zapise koji bi prilikom autorizacijskog zahtjeva rezultirali odabirom više od jednog zapisa. Domena koja implementira SPF protokol definira proizvoljni broj mehanizama koji se koriste za određivanje skupa računala ovlaštenih za slanje elektroničke pošte za danu domenu. Mehanizmi se koriste i za definiranje određenih aspekata sigurnosne politike elektroničke pošte. Iako nije pravilo, najbolje je konfigurirati SPF zapis sa malim slovima.

Prvi korak za kreiranje SPF zapisa je prikupiti sve IP adrese sa kojih će biti poslane poruke elektroničke pošte. Za uspješnu implementaciju SPF-a prvo se mora identificirati koji će se poslužitelji elektroničke pošte koristiti za slanje elektroničke pošte za postojeću domenu. To mogu biti poslužitelji unutar organizacije ili poslužitelji od trenutnog ISP-a. SPF zapis se mora kreirati za svaku domenu, bez obzira na to da li domena služi za aktivno slanje poruke elektroničke pošte.

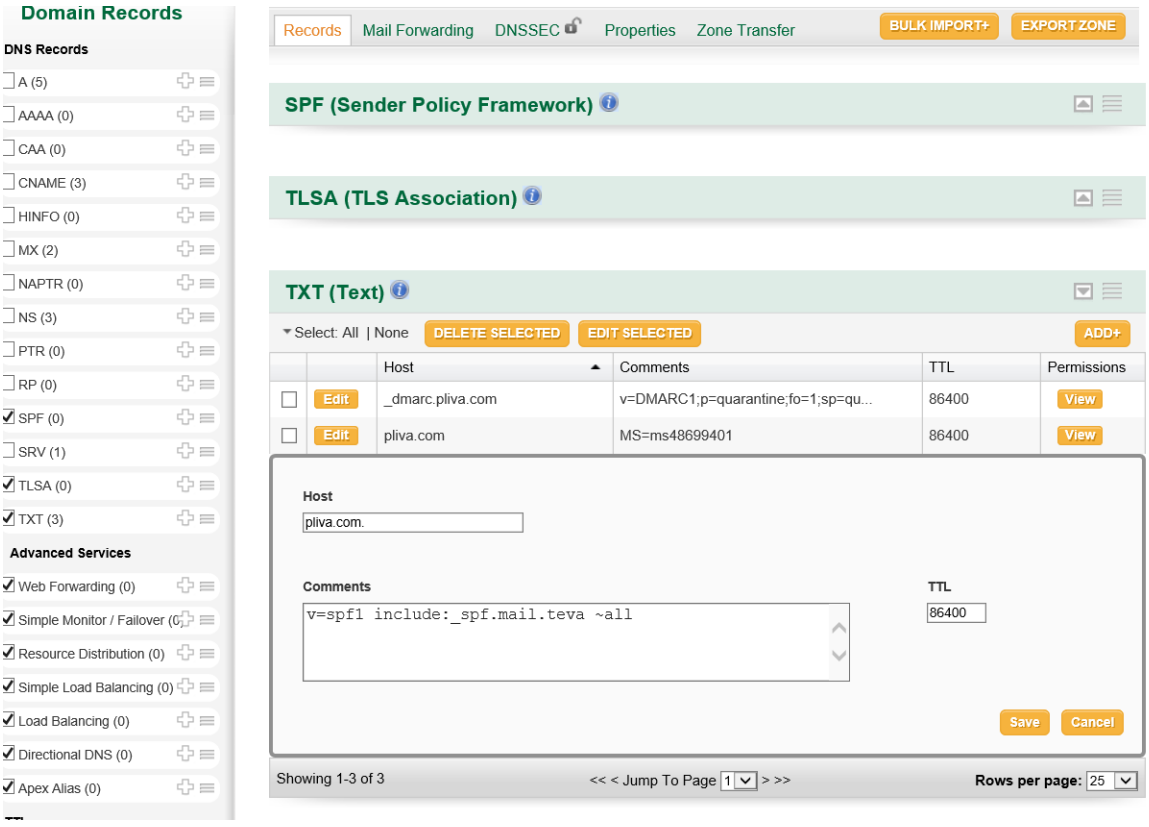
Drugi korak je kreiranje samog SPF zapisa. Započinje se sa odabirom verzije SPF protokola i tim se dijelom definira SPF zapis. SPF zapis uvijek mora započeti brojem verzije npr. v=spf1. Nakon što je postavljena verzija SPF protokola, potrebno je dodati i IP adrese koje su autorizirane za slanje poruka u ime domene npr. v=spf1 ip4:34.243.61.237. Također, može se i postaviti opcija „uključi“ (eng. Include) za bilo koju organizaciju koja može biti autorizirana za slanje poruka u ime druge organizacije npr. include:thirdpartydomain.com. Potrebno je uskladiti se sa drugom organizacijom i biti svjesni koje domene se koriste kao vrijednost za opciju „uključi“. Nakon što su implementirane sve IP adrese i kreirani svi parametri, zapis bi se trebao završiti sa oznakom ~all ili –all. Ako neovlašteni poslužitelj pošalje poruku elektroničke pošte u ime domene, poduzimaju se mjere prema objavljenim pravilima npr. može se odbiti elektronička pošta ili označiti kao neželjena pošta. Bitno je imati na umu da SPF zapis ne može imati više od 255 znakova i može imati najviše 10 oznaka. Nakon što je zapis definiran, mogao bi izgledati ovako (slika 19.):

v=spf1 ip4:34.243.61.237 ip6:2a05:d018:e3:8c00:bb71:dea8:8b83:851e include:thirdpartydomain.com –all

Treći korak obuhvaća objavljivanje SPF zapisa u DNS-u. SPF zapis se objavljuje kroz DNS manager, koji koristi administrator koji je dobio pripadajuća prava za korištenje, od strane DNS

sustava, ili se može koristiti usluga DNS pružatelja usluge. Primjer i koraci korištenja DNS managera, pogledati sliku 18.:

- Potrebno je prijaviti se na domenu,
- Otvoriti DNS konzolu za ažuriranje DNS zapisa na domeni,
- Odabrati domenu na kojoj će se modificirati zapis,
- Otvoriti DNS manager,
- Kreirati novi TXT zapis u TXT polju,
- Unutar Host polja postaviti ime domene,
- Unutar TXT Value polja upisati SPF zapis,
- Specificirati TTL (eng. Time To Live), upisati 3600 ili ostaviti kako je i odabrano,
- Odabrati Add record kako bi se objavio SPF zapis unutar DNS-a. [18]



Slika 18. Primjer TXT zapisa unutar DNS-a

[18] Everything you need to know about SPF – DMARC Analyzer; dostupno na https://www.dmarcanalyzer.com/spf/

Četvrti korak služi za testiranje SPF zapisa preko alata za provjeru SPF zapisa. Postavljanje SPF zapisa bitan je dio tehničkih postavki. SPF zapis je ispravno konfiguriran kada:

- alat za provjeru SPF zapisa uspješno pronađe SPF zapis,
- SPF zapis ne premašuje maksimalni broj od 10 upita (eng. Lookups),
- su konfigurirane IP adrese stvarne adrese sa kojih se šalju poruke elektroničke pošte.

Mehanizmi kao prefiks mogu imati jednu od ovih oznaka:

- + (pass) – dopuštaju se sve adrese elektroničke pošte. + se može i izostaviti, npr. + mx je isto što i mx,
- - (hardfail) - sve adrese elektroničke pošte za koje se sumnja da su krivotvorene ili neželjene se odbacuju i ne isporučuju,
- ~ (softfail) - adrese se prihvaćaju / prikazuju korisniku, ali su označene upozorenjem kao sumnjive,
- ? (neutral) – sve adrese su dopuštene.

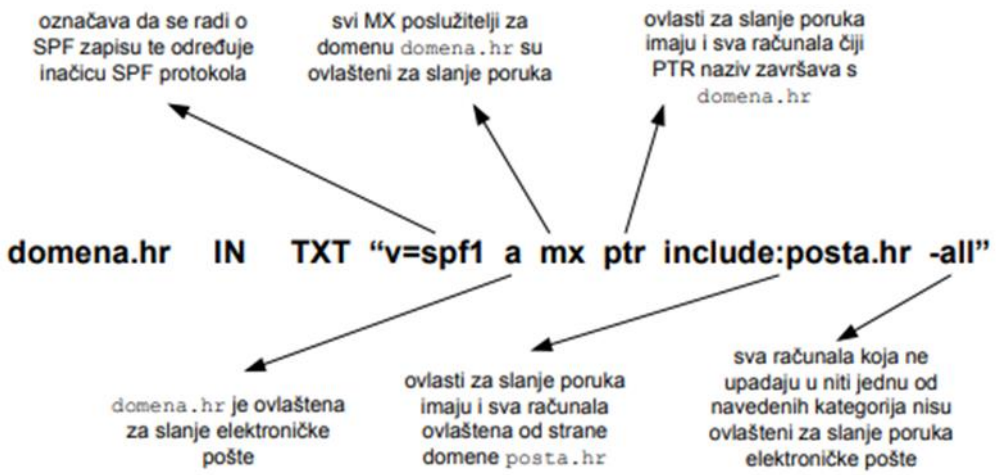
Popis mehanizama je sljedeći:

- All - obično se postavlja na kraju. Npr. v=spf1 mx –all tim zapisom dopuštamo svim MX zapisima na domeni da šalju poruke u ime te domene, a sve ostalo se zabranjuje,
- IPv4 – uključuje raspon IPv4 mreža. /32 subnet je postavljen kao zdani. Npr. v=spf1 ip4:192.168.0.1/16 –all tim zapisom dopuštamo bilo IP adresu između 192.168.0.1 i 192.168.255.255,
- IPv6 – uključuje raspon IPv6 mreža. /126 subnet je postavljen kao zadani,
- A – svi A zapisi sa domene su testirani, i ako su IP adrese sa klijenta pronađene među njima smatramo ih urednima. Za konekcije preko IPv6 koriste se AAAA zapisi. Također, ukoliko domena nije konfigurirana, koristi se zadana domena. Npr. v=spf1 a -all ili za postavljenu domenu example.com v=spf1 a:example.com –all,
- MX - prilikom korištenja MX zapisa provjeravaju se svi odgovarajući A zapisi. Ukoliko se tražena IP adresa nađe, mehanizam MX se evaluira kao istinit. Npr. v=spf1 mx/24 mx:offsite.domain.com/24 -all MX mehanizam prima poruku na jednu IP adresu, ali šalje poruku na drugu adresu koja je u istom mrežnom rasponu,
- PTR – pomoću PTR upita pretražuju se imena računala od strane klijenta. Najmanje jedan A zapis vezan za PTR upit mora biti usklađen sa ispravnom IP adresom klijenta. Npr. v=spf1 ptr:otherdomain.com –all Bilo koji poslužitelj čije ime računala završava na otherdomain.com je označen,

- Exists – Izvršava se A upit na domeni, ukoliko je rezultat pronađen, konekciju smatramo uspješnom. Npr. v=spf1 exists:example.com –all ako domena example.com odgovori na upit, konekcija je uspješna, u suprotnom ju smatramo neuspješnom,
- Include - koristi se u slučaju da se za slanje elektroničke pošte koriste poslužitelji koji se nalaze na drugoj domeni. Npr. v=spf1 include:example.com –all.

Domena može definirati i modifikatore, koji su opcionalni i može se pojaviti samo jednom po zapisu:

- Redirect - SPF zapis za domenu može zamijeniti trenutni zapis. Npr. v=spf1 redirect=example.com Ukoliko nema SPF zapisa za domenu example.com, prikazuje se greška: rezultat je nepoznat,
- Explanation – netko tko oglašava SPF može odrediti niz objašnjenja koji pošiljatelji vide.



Slika 19. Primjer SPF zapisa

4.1.2.SPF implementacija kroz Ironport

Ironport podržava Sender Policy Framwork verifikaciju. Budući da SPF provjere zahtijevaju raščlanjivanje i procjenu, one direktno mogu utjecati na izvedbu Ironporta. Također, treba imati na umu da SPF provjere povećavaju opterećenje DNS infrastrukture.

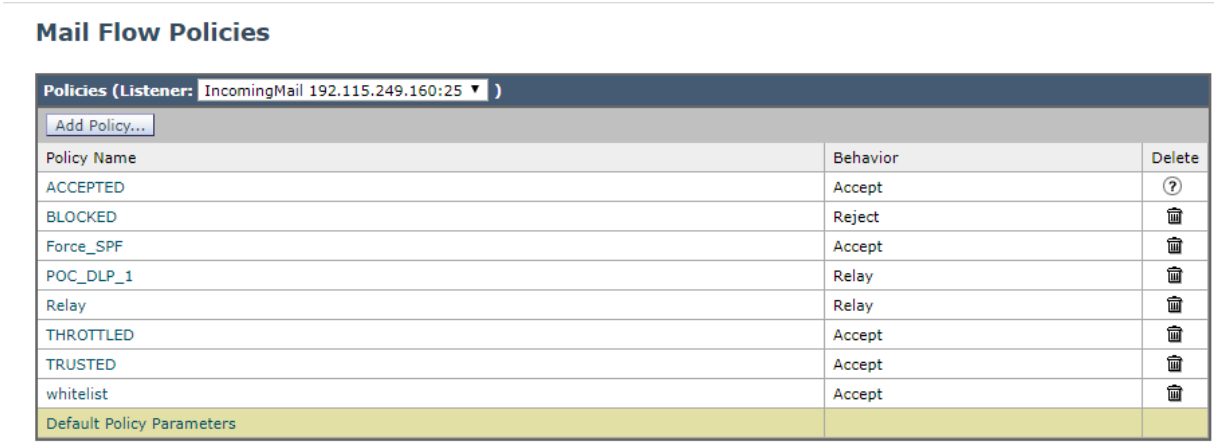
Kako provjeriti dolazne poruke pomoću SPF protokola?

1. Kreirati prilagođeno pravilo za protok elektroničke pošte za provjeru dolaznih poruka pomoću SPF protokola

2. Konfigurirati pravilo za protok elektroničke pošte za provjeru dolaznih poruka pomoću SPF protokola
3. Definirati radnju koju Ironport izvršava na provjerenim porukama
4. Pridružiti radnju grupama određenih pošiljatelja ili primatelja
5. Testirati rezultate poruka (opcionalno).[19]

Da bi se koristio SPF protokol, mora se omogućiti SPF pravilo za protok elektroničke pošte na dolaznom slušatelju (Slika 20.):

1. Odabrati Mail Policies > Mail Flow Policy
2. Odabrati Default Policy Parameters
3. Pod zadanim parametrima pravila, provjeriti opciju Security Features
4. Unutar SPF/SIDF Verification sekcije, odabrati On
5. Podesiti razinu sukladnosti (zadano je kompatibilno sa SIDF-om). Ova opcija omogućava da se odredi koji se standard provjere korist, SPF ili SIDF.

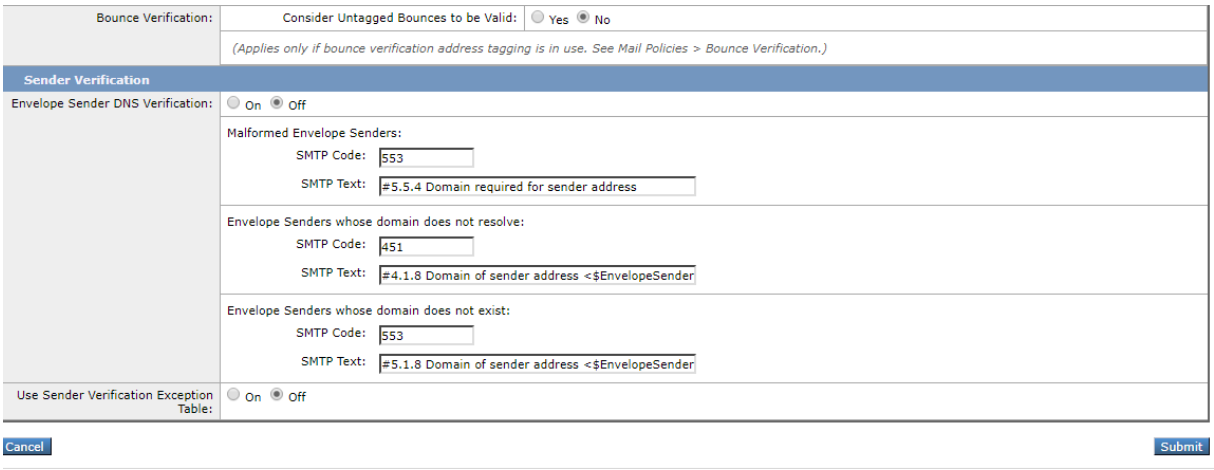


[19] User Guide for AsyncOS 11.0 for Cisco Email Security Appliances, First Published: 2017-05-31

Mail Flow Policy: Defaults - IncomingMail 192.115.249.160:25

Default Settings		
Connections:	Max. Messages Per Connection:	10
	Max. Recipients Per Message:	50
	Max. Message Size:	10485760 *(add a trailing K for kilobytes; M for megabytes)*
	Max. Concurrent Connections From a Single IP:	10
SMTP:	Custom SMTP Banner Code:	220
	Custom SMTP Banner Text:	
	Custom SMTP Reject Banner Code:	554
	Custom SMTP Reject Banner Text:	
	Override SMTP Banner Hostname:	◉ Use Hostname from Interface ○
Mail Flow Limits		
Rate Limit for Hosts:	Max. Recipients Per Hour:	◉ Unlimited ○
	Max. Recipients Per Hour Code:	452
	Max. Recipients Per Hour Text:	Too many recipients received this hour
▷ Rate Limit for Envelope Senders:	Settings to define maximum recipients for envelope sender, per time interval.	
Flow Control:	Use SenderBase for Flow Control:	◉ On ○ Off
	Group by Similarity of IP Addresses:	*This Feature can only be used if Senderbase Flow Control is off.*
		◉ Off ○ *(significant bits 0-32)*

Directory Harvest Attack Prevention (DHAP):	Max. Invalid Recipients Per Hour:	○ Unlimited ◉ 25
	Drop Connection if DHAP threshold is Reached within an SMTP Conversation:	◉ On ○ Off
	Max. Invalid Recipients Per Hour Code:	550
	Max. Invalid Recipients Per Hour Text:	Too many invalid recipients
Security Features		
Spam Detection:	◉ On ○ Off	
Virus Protection:	◉ On ○ Off	
Encryption and Authentication:	TLS:	◉ Off ○ Preferred ○ Required ☐ Verify Client Certificate
	SMTP Authentication:	◉ Off ○ Preferred ○ Required
	If Both TLS and SMTP Authentication are enabled:	☐ Require TLS To Offer SMTP Authentication
Domain Key/DKIM Signing:	○ On ◉ Off	
DKIM Verification:	○ On ◉ Off	
	Use DKIM Verification Profile:	DEFAULT ▾
S/MIME Decryption/Verification:	○ On ◉ Off	
	Signature After Processing:	◉ Preserve ○ Remove
S/MIME Public Key Harvesting:	S/MIME Public Key Harvesting:	◉ Disable ○ Enable
	Harvest Certificates on Verification Failure:	◉ Disable ○ Enable
	Store Updated Certificate:	○ Disable ◉ Enable
SPF/SIDF Verification:	◉ On ○ Off	
	Conformance Level:	SPF ▾
	Downgrade PRA verification result if 'Resent-Sender:' or 'Resent-From:' were used:	○ No ○ Yes
	HELO Test:	○ Off ○ On
DMARC Verification	○ On ◉ Off	
	Use DMARC Verification Profile:	DEFAULT ▾
	DMARC Feedback Reports: ⓘ	* *DMARC reporting message must be DMARC compliant.* * *Recommended: Enable TLS encryption for domains that will receive reports. Go to Mail Policies > Destination Controls.* ☐ Send aggregate feedback reports



Slika 20. SPF pravilo za protok elektroničke pošte

Ironport podržava više upravljačkih postavki za svaku razinu sukladnosti SPF/SIDF. Kada se konfiguriraju zadane postavke slušateljevog HAT-a (eng. Host Access Table), može se odabrati razina slušateljeve SPF/SIDF sukladnosti i SMTP radnje (ACCEPT ili REJECT) koje Ironport izvodi na temelju rezultata provjere SPF / SIDF. Može se definirati i SMTP odgovor koji Ironport šalje kada se odbije poruke. Ovisno o razini sukladnosti, Ironport vrši provjeru identiteta HELO, MAIL FROM OF ili PRA identiteta. Može se odrediti da li se nastavlja sesija (ACCEPT) ili prekida sesija (REJECT) za svaki od sljedećih rezultata provjere SPF / SIDF za svaku provjeru identiteta:

- None - provjera se ne može provesti zbog nedostatka informacija,
- Neutral - vlasnik domene ne potvrđuje da je li korisnik ovlašten koristiti dani identitet,
- SoftFail - vlasnik domene vjeruje da korisnik nije ovlašten koristiti dani identitet, ali ne želi dati konačnu izjavu,
- Fail – korisnik nije ovlašten slati poštu s navedenim identitetom,
- TempError - tijekom provjere došlo je do prolazne pogreške,
- PermError - tijekom provjere došlo je do trajne pogreške.

Kad se dobije verificirana pošta SPF protokola, možda će biti potrebno poduzeti različite radnje ovisno o rezultatima provjere SPF-a. Ova pravila za poruku i filtrirani sadržaj mogu odrediti status ovjerene pošte SPF protokola i izvesti radnje nad porukama na temelju rezultata provjere:

- spf-status - ovo pravilo za filtriranje određuje radnje na temelju statusa SPF protokola. Za svaku važeću povratnu vrijednost SPF protokola mogu se koristiti različite radnje,

- spf-passed - ovo pravilo za filtriranje generalizira SPF rezultate kao Boolean vrijednost. spf-status se može koristiti kada se žele dobiti detaljniji rezultati, a spf-passed kada se želi stvoriti jednostavan logički rezultat.

4.2.DKIM – DomainKeys Identified Mail

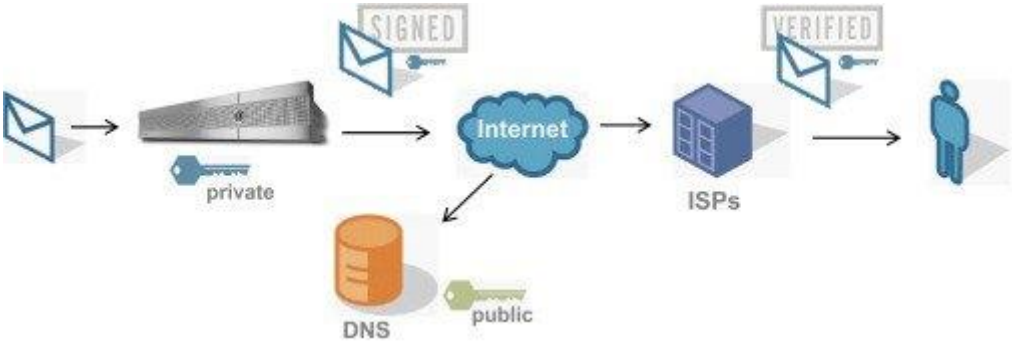
DKIM (eng. DomainKeys Identified Mail) je protokol koji omogućava organizaciji da preuzme odgovornost za prijenos poruke na siguran i zaštićen način. Takva poruka omogućena je uz pomoć kriptografske provjere autentičnosti. DKIM je najbolje opisati u tri koraka koja su zaslužna za njegovu konfiguracijom, pogledati sliku 21. Prvo, pošiljatelj odlučuje koje elemente elektroničke pošte želi uključiti u postupak potpisivanja. Može se odlučiti uključiti cijelu poruku (zaglavlje i tijelo) ili se samo usredotočiti na jedno ili više polja zaglavlja elektroničke pošte. Elementi koji se odluče uključiti postupak potpisivanja DKIM-a moraju ostati nepromijenjeni u tranzitu, jer DKIM potpis neće uspjeti proći provjeru autentičnosti. Na primjer, ako je poruka elektroničke pošte proslijeđena s npr. Example.com na Example2.com, Example.com može dodati redak teksta na vrh elektroničke pošte. U tom trenutku, tijelo poruke je promijenjeno i, ako je tijelo uključeno u postupak potpisivanja DKIM-a, DKIM autentikacija neće biti uspješna za proslijeđenu poruku elektroničke pošte. Međutim, ako je u potpisu DKIM-a uključen samo element zaglavlja, poput polja "From", a poruka je proslijeđena sa domene Example.com na Example2.com, provjera autentičnosti DKIM-a će biti uspješna, jer dio poruke koji je promijenjen nije potpisan od strane DKIM-a.

Drugi korak je zadužen za proces kriptiranja. Pošiljatelj konfigurira svoju platformu za elektroničku poštu, na način da automatski stvori hash od dijelova elektroničke pošte koji žele potpisati. Proces hashiranja pretvara čitljivi tekst u jedinstveni tekstualni niz. Prije slanja poruke elektroničke pošte taj se niz šifrira pomoću privatnog ključa. Privatni ključ dodjeljuje se jedinstvenoj kombinaciji domene i selektora, omogućujući više legitimnih privatnih ključeva za istu domenu, što je važno zbog sigurnosti. Samo pošiljatelj ima pristup privatnom ključu. Nakon što je postupak šifriranja dovršen poruka elektroničke pošte se šalje.

U trećem koraku odrađuje se provjera potpisa DKIM-a uz pomoć javnog ključa. Davatelj usluga elektroničke pošte prima poruku elektroničke pošte, te se vidi da ima DKIM potpis i otkriva koja je kombinacija "domena / selektor" potpisala postupak šifriranja. Da bi potvrdio potpis, davatelj usluga pokrenut će DNS upit kako bi pronašao javni ključ za tu kombinaciju domena / selektor. Javni ključ ima jedinstvenu karakteristiku da se jedini može podudarati sa privatnim

ključem koji je potpisao poruku elektroničke pošte, također poznat kao "keypair match“. Takva mogućnost pružatelju usluga elektroničke pošte omogućuje dešifriranje potpisa DKIM-a u izvorni hash niz. Zatim se uzimaju elementi poruke koju potpisuje DKIM i generira vlastiti hash od tih elemenata. Na samom kraju, davatelj usluga uspoređuje hash koji je generirao s dešifriranim hash-om iz potpisa DKIM-a. Ako se podudaraju, zna se da:

- DKIM domena doista "posjeduje" poruku elektroničke pošte, jer u protivnom postupak dešifriranja ne bi funkcionirao,
- Elementi poruke potpisani od strane DKIM-a nisu u promijenjeni u tranzitu, u slučaju da su promijenjeni hash-evi se ne bi podudarali



Slika 21. Shema DKIM protokola

DKIM protokol koristi naziv domene kao identifikator kako bi se referirao na identitet odgovorne osobe ili organizacije. Unutar DKIM protokola taj se identifikator naziva SDID (eng. Signing Domain IDentifier) i nalazi se u polju zaglavlja DKIM potpisa npr. d = example.com. Bitno je znati da, isti identitet može imati više identifikatora. Ugled domene je dodatna osnova za procjenu da li se vjeruje poruci koja se isporučuje, te vlasnik SDID-a potvrđuje da prihvaća odgovornost za poruku. DKIM je zamišljen kao dodana vrijednost za elektroničku poštu.

Za DKIM protokol, SDID potvrđuje valjanost ključa, a nikako ne treća strana. Upravljanje ključevima DKIM-a omogućeno je dodavanjem informacija o zapisima u postojeći DNS sustav. Ovaj pristup ima značajne operativne prednosti. Prvo, izbjegava se stvaranje nove globalne infrastrukture, a drugo za tehnički aspekt DNS-a se već zna da je učinkovit. Svaka nova usluga morala bi proći kroz period postupnog sazrijevanja, s potencijalno problematičnim ponašanjima u ranoj fazi. DKIM dodaje mogućnost krajnje provjere autentičnosti postojećoj infrastrukturi

za prijenos elektroničke pošte DKIM protokol dopušta da se bilo koji naziv domene koristi kao SDID i podržava više opcija za različite algoritme. Kod DKIM-a potpisnik izričito navodi zaglavlja koja su potpisana, poput From, Date, i Subject polja. Odabirom minimalnog skupa zaglavlja koji je potreban, potpis će vjerojatno biti i znatno snažniji. Nakon potpisivanja poruke, administrator može na putu prijenosa poruke provjeriti potpis kako bi utvrdio da je vlasnik SDID-a preuzeo odgovornost za tu poruku. Primatelj poruke može provjeriti potpis tako da izravno zatraži od DNS-a domenu potpisnika, kako bi pronašli odgovarajući javni ključ. Na taj način potvrđuje se da je poruku potpisala strana koja posjeduje privatni ključ za SDID.

4.2.1.Elementi DKIM-a

Ako se javni ključ objavi javno, svatko može dešifrirati i čitati šifrirane podatke, ali ih nitko ne može mijenjati (za vrijeme tranzita). Za šifriranje vlastite izmijenjene kopije potreban je privatni ključ. Potpis ne šifrira podatke, već samo hashira zbroj podataka. Primjer:

- A = zbroj hash kopija podataka,
- B = dešifrira potpis koristeći javni ključ domene / DNS-a,
- Ako je A = B, kopija nepromijenjena.[20]

DKIM zahtijeva generiranje parova javnih i privatnih ključeva i pravilno postavljanje javnog ključa u DNS zapise, kao i postavljanje privatnog ključa unutar poslužitelja za razmjenu poruka e-pošte. Primjer DKIM potpisa:

DKIM-Signature: v=1; a=rsa-sha256; d=example.net; s=brisbane;

c=relaxed/simple; q=dns/txt; l=1234; t=1117574938; x=1118006938;

h=from:to:subject:date:keywords:keywords;

bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;

b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZ

VoG4ZHRNiYzR

Oznake iz ovog primjera mogu se prevesti kao:

- v – verzija,

[20] DKIM Email Security Standard; dostupno na https://www.cyberpunk.rs/dkim-email-security-standard

- a – algoritam potpisivanja,
- d – domena,
- s – selektor (koji se javni ključ koristi),
- c - algoritmi za kanonizaciju zaglavlja i tijela poruke,
- q – zadana metoda upita,
- l - duljina kanoniziranog dijela tijela koji je potpisan,
- t – timestamp potpisa,
- x – vrijeme istjecanja,
- h - popis potpisanih polja zaglavlja, ponavlja se za polja koja se javljaju više puta,
- bh – zbroj hasheva kanoniziranog tijela poruke. Koristi se za brzu provjeru ako poruka ne prihvati DKIM,
- b - potpis podataka (uključuje zaglavlja i tijelo).

DKIM protokol definira dva algoritma kanonizacije za tijelo poruke:

- simple - čini vrlo malo, samo skida prazne crte na kraju tijela,
- relaxed – briše prazne crte, a zatim zamjenjuje bilo koju karticu sa jednakim razmakom.

DKIM protokol također definira dva algoritma kanonizacije za zaglavlja poruke:

- simple – ne radi promjene. Tako da zaglavlja moraju biti identična, bajt po bajt, da bi se podudarali,
- relaxed - pretvara sva imena zaglavlja u mala slova, razotkriva zaglavlje, tako da svaki pojedinačni redak zamjenjuje i uklanja svaki zaostali prostor u svakom retku.

Neki od rezultata koji se mogu prikazati prilikom testiranja DKIM protokola su:

- pass - poruka je potpisana, potpis ili potpisi su prihvatljivi i prošli su sve verifikacijske provjere,
- fail - poruka je potpisana i potpis ili potpisi su prihvatljivi, ali nisu zadovoljili verifikacijske provjere. Poruka je potpisana i potpis je pravilno oblikovan, ali ne podudara se s potpisom poslužitelja koji šalje. Potencijalni pokazatelj da je poruka izmijenjena negdje na putu,
- none – poruka nije potpisana, odnosno poruka bez DKIM potpisa,
- policy - poruka je potpisana, ali potpis ili potpisi nisu prihvatljivi. Poruka je potpisana i pravilno oblikovana, ali nije zadovoljila zahtjevima na strani primatelja,

- neutral - poruka je potpisana, ali potpis ili potpisi sadrže sintaksičke pogreške ili ih nije bilo moguće drugačije obraditi. Potpisana poruka, ali nije pravilno formirana. Vjerojatno je došlo do pogreške u konfiguraciji na strani pošiljatelja,
- temperror - poruka se ne može verificirati zbog pogreške koja je vjerojatno prolazne prirode, poput privremene nemogućnosti dohvaćanja javnog ključa. Naknadni pokušaj može proizvesti ispravnu verifikaciju. Ukoliko se problem ponavlja može sugerirati na pogreške u vezi s DNS-om,
- permerror - poruka se ne može provjeriti zbog pogreške koja je nepopravljiva, npr. obavezno polje zaglavlja koje fali. Nedostaje potpis unutar primljene poruke. Naznaka loše oblikovanog zaglavlja ili je promijenjen nakon slanja.

4.2.2.DKIM implementacija kroz ironport

DKIM se sastoje od dva glavna dijela: potpisivanja i provjere, a Ironport podržava oba postupka. Također se može omogućiti odbacivanje poruka i odgodu isporučivanja prije DKIM potpisivanja. Potpisivanje DKIM-a u Ironport-u provodi se putem profila domena i omogućuje slanjem elektroničke pošte. Profili domena povezuje domenu s ključnim podacima o domeni (ključ za potpis). Budući da se elektronička pošta šalje preko Ironporta putem pravila protoka elektroničke pošte, pošiljateljeva adresa elektroničke pošte, koja odgovara bilo kojem profilu domene, je potpisana ključem za potpis koji je naveden u profilu domene. Dakle, ako se omogući DKIM potpisivanje, koristi se i DKIM potpis. DKIM se može implementirati preko CLI naredbe domainkeysconfig ili putem GUI-a Mail Policies > Domain Profiles i Mail Policies > Signing Keys. Potpisivanje DKIM-a funkcionira na sljedeći način: vlasnik domene generira dva ključa - javni ključ pohranjen u javnom DNS-u (DNS TXT zapis povezan s tom domenom) i privatni ključ koji je pohranjen na uređaju, koristi se za potpisivanje elektroničke pošte koja je poslana sa te domene. Dok se poruke talože na slušatelja koji se koristi za slanje poruka, Ironport provjerava postoje li konfigurirani profili domena. Ako su na Ironportu konfigurirani profili domena, poruka se skenira tražeći valjanu adresu pošiljatelja, kao i From zaglavlje. Ukoliko su oba parametra prisutna, Sender zaglavlje se uvijek koristi za potpisivanje DKIM-a, ali i From zaglavlje također mora biti uključeno iako se ne koristi za potpisivanje DKIM-a. Ako je prisutno samo Sender zaglavlje, profili DKIM potpisivanja ne odgovaraju.

Ključ za potpis je privatni ključ pohranjen unutar sustava. Prilikom stvaranja ključa za potpis određuje se veličina ključa. Veći ključevi su sigurniji, međutim veći ključevi također mogu utjecati na performanse. Ironport podržava ključeve od 512 bita do 2048 bita. Ključevi veličine

768 do 1024 bita smatraju se sigurnijim i danas ih koristi većina pošiljatelja. Ključevi temeljeni na većim dimenzijama mogu utjecati na performanse i nisu podržani ključevi veličine iznad 2048 bita.[21] Nakon što se ključ potpiše, dostupan je za upotrebu u profilima domena i pojavit će se unutar liste popisa ključeva za potpis. Nakon što se ključ za potpis poveže sa profilom domene, može se stvoriti DNS tekstualni zapis koji sadrži javni ključ. To se odrađuje putem Generate polja unutar DNS Text Record opcije pri listi sa profilima domene. Ili putem CLI naredbe domainkeysconfig -> profiles -> dnstxt. Javni ključ se može pronaći i odabirom Signing Keys -> View (Slika 22.).

Signing Keys

Signing Keys — Items per page: 20

Add Key... | Clear All Keys | Import Keys...

Displaying 1 — 20 of 21 items. Page 1 of 2 « Previous | 1 | 2 | Next »

Name ▲	Key Size (Bits)	Public Key	Domain Profiles	All Delete
POC	1024	View	POC test_maildomain_com	☐
actavis_bg	2048	View		☐
actavis_co_nz	2048	View	actavis_co_nz	☐
actavis_com_mt	2048	View		☐
actavis_dk	2048	View		☐
actavis_is	2048	View		☐
actavis_ru	2048	View		☐
actavis_se	2048	View		☐
elmor_com_ve	2048	View		☐
frx_com	2048	View		☐
mail_teva	2048	View		☐
nicobrand_com	2048	View		☐
ratiopharm_fi	2048	View		☐
specifar_gr	2048	View		☐
sudocrem_com	2048	View		☐
test	2048	View		☐
test3	2048	View		☐
test4	2048	View		☐
test5	2048	View	test3	☐
teva-romania_ro	2048	View		☐

Displaying 1 — 20 of 21 items. Page 1 of 2 « Previous | 1 | 2 | Next »

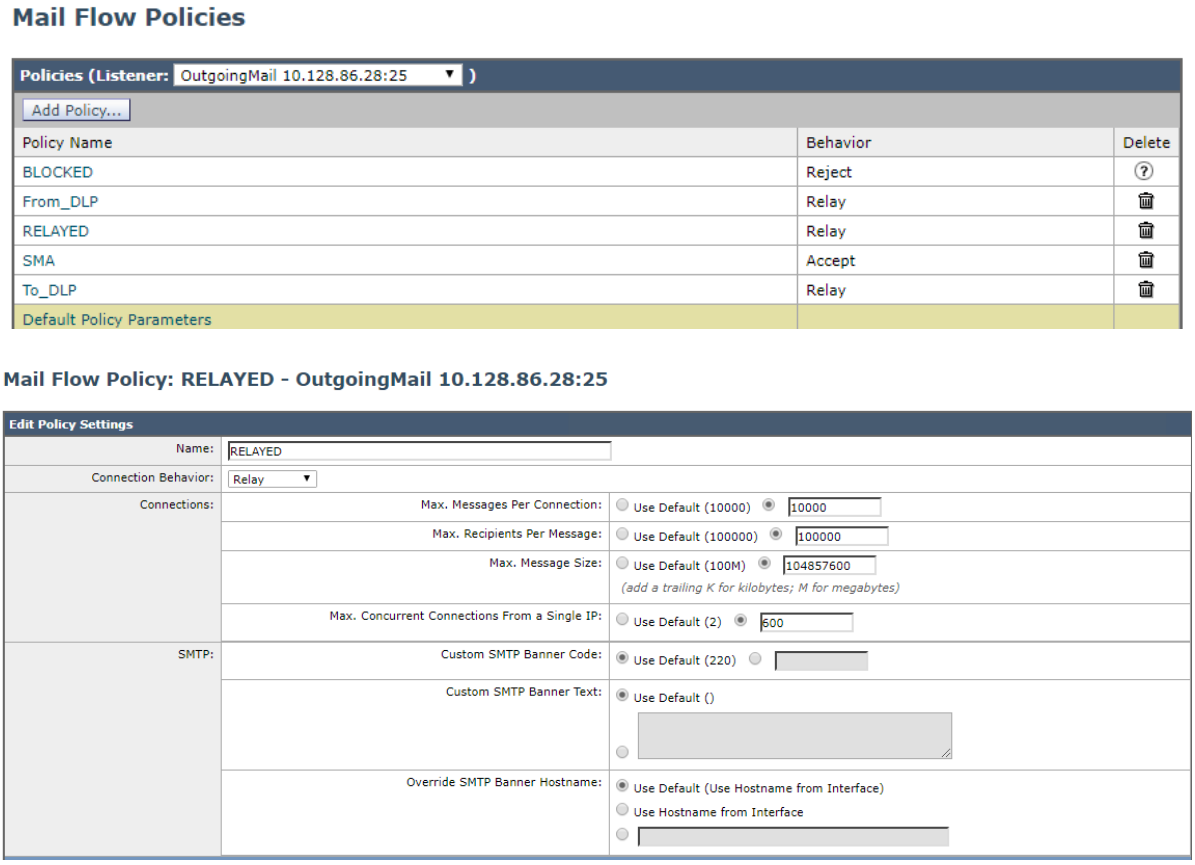
Export Keys... | Delete

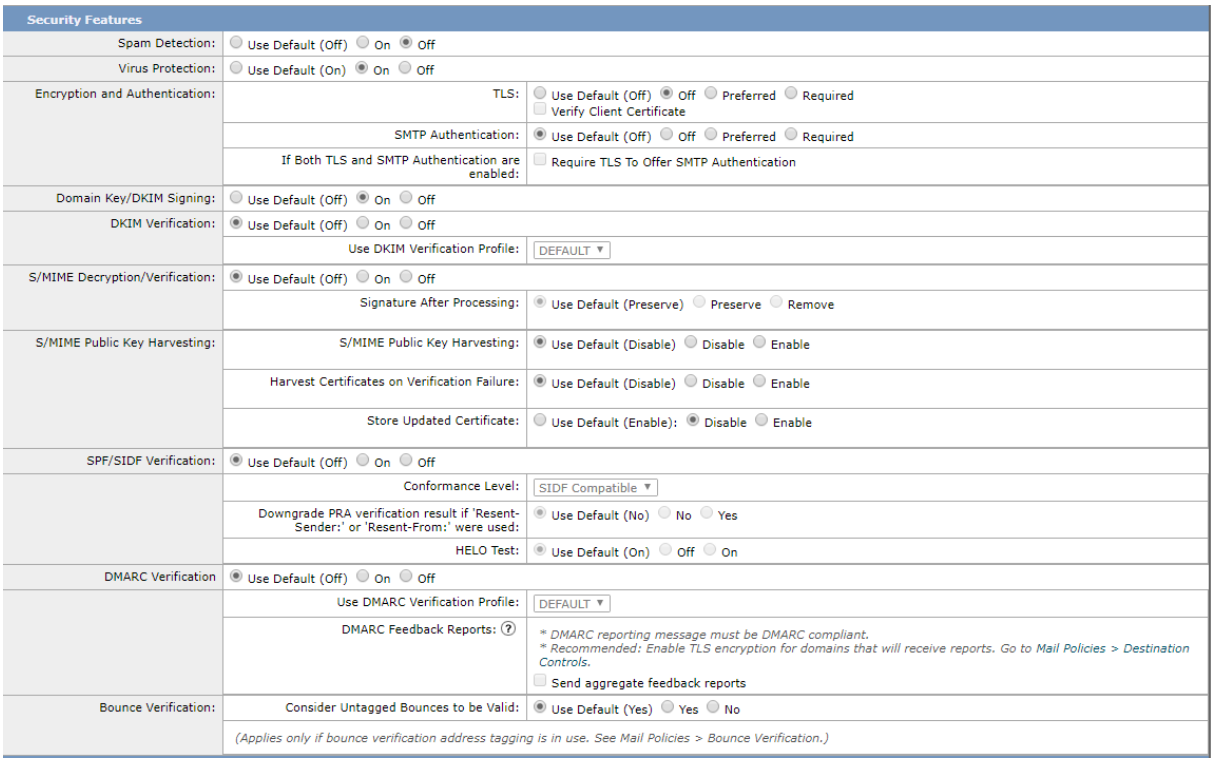
[21] User Guide for AsyncOS 11.0 for Cisco Email Security Appliances, First Published: 2017-05-31

Slika 22. Primjer DKIM ključa za potpisivanje

Potpisivanje DKIM-a za odlaznu poštu omogućeno je sljedećim koracima (Slika 23.):

1. Pod Mail Flow Policies odabrati RELAYED politiku protoka pošte (odlaznu)
2. Pod Security Features omogućiti DKIM Signing odabirom opcije On
3. Izvršiti promjene





Slika 23. Potpisivanje DKIM-a za odlaznu poštu

Osim potpisivanja odlaznih poruka, preporučuje se i potpisivanje poruka o odbacivanju i odgodi isporuke. Time se upozorava primatelje da su te iste poruke koje dobivaju od strane organizacije legitimne. Da bi se omogućilo potpisivanje DKIM-a za poruke odbacivanja i odgode, koristi se profil koji je povezan s javnim slušateljem. Može se pronaći pod opcijom Hard Bounce and Delay Warning Messages -> omogućiti Use Domain Key Signing for Bounce and Delay Messages.

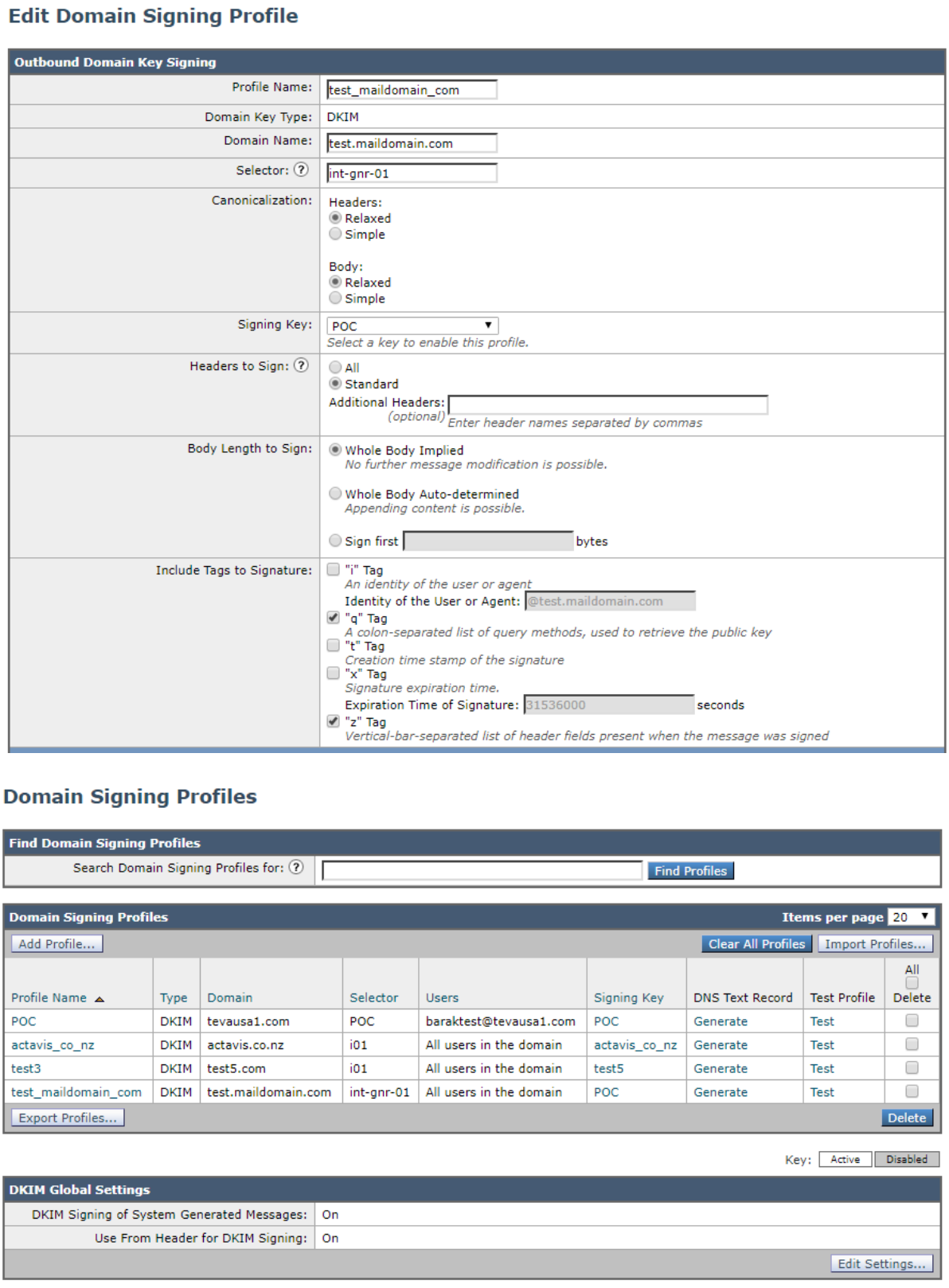
Konfiguriranje DKIM potpisivanja u koracima:

1. Kreirati novi ili uvesti postojeći privatni ključ,
2. Kreirati profil domene i pridružite ključ profilu domene,
3. Kreirati DNS tekstualni zapis,
4. Omogućiti potpisivanje DKIM-a za odlaznu poštu,
5. Omogućiti potpisivanje DKIM-a za poruke o odbacivanju i odgodi,
6. Poslati testnu poruku. Poruka poslana s domene koja odgovara profilu domene biti će potpisana DKIM-om

Prema slici 24., kreiranje novog profila domene za potpisivanje DKIM-a:

1. Odabrati Mail Policies > Signing Profiles

2. Pod Domain Signing Profiles odabrati Add Profile
3. Upisati ime profila
4. Pod Domain Key Type odabrati DKIM, te provjeriti dodatne postavke
5. Upisati ime domene
6. Postaviti selektor. Selektori su proizvoljna imena koja su predodređena za "_domeinkey." imenski prostor, koji se koristi za podršku višestrukih istodobnih javnih ključeva po domeni koja šalje poruke.
7. Odabrati kanonizaciju za zaglavlje (Relaxed ili Simple)
8. Odabrati kanonizaciju za tijelo poruke (Relaxed ili Simple)
9. Odabrati ključ za potpis. Da bi na popisu imali ključeve za potpis, mora se kreirati (ili uvesti) najmanje jedan ključ za potpis
10. Odabrati popis zaglavlja za potpis. Može se odabrati između sljedećih zaglavlja:
11. All – Ironport potpisuje sva zaglavlja prisutna u trenutku potpisivanja. Potpisuju se sva zaglavlja ako se ne očekuje da će se zaglavlja dodavati ili uklanjati u tranzitu,
12. Standard – se odabiru ako se očekuje da će zaglavlja biti dodana ili uklonjena u tranzitu
13. Navesti kako potpisati tijelo poruke. Može se odabrati potpis tijela poruke i koliko bajtova treba potpisati.
14. U polju zaglavlja potpisa poruke odabrati oznake koje se žele uključiti. Podaci pohranjeni u ovim oznakama koriste se za provjeru potpisa poruke
15. Upisati korisnike (adrese elektroničke pošte) koji će koristiti profil domene za potpisivanje
16. Izvršiti promjene



Slika 24. Kreiranje novog profila domene za potpisivanje DKIM-a

Kreiranje novog ključa za potpis (na gotovo isti način se i konfigurira već postojeći ključ):

1. Odabrati Mail Policies > Signing Keys
2. Odabrati Add Key
3. Upisati ime ključa
4. Odabrati Generate i kolika će biti veličina ključa
5. Izvršiti promjene

Kreiranje DNS tekstualnog zapisa (Slika 25.):

1. Odabrati Mail Policies > Signing Profiles
2. Pod Domain Signing Profiles u DNS Text Record retku, odabrati Generate za odgovarajući profil domene
3. Označiti atribute koji se žele uključiti u DNS tekstualni zapis
4. Odabrati Generate Again da bi se ponovo generirao ključ sa izmjenama
5. Odabrati Done

Slika 25. Kreiranje DNS tekstualnog zapisa

Pomoću globalnih postavki DKIM protokola može se odabrati da li sustav potpisuje poruke generirane s DKIM potpisom. Ironport će potpisati sljedeće poruke: Cisco IronPort Spam Quarantine notifikacije, obavijesti koje generiraju filtar sadržaja i poruke vezane za konfiguraciju. Također, pomoću globalnih postavki DKIM protokola se može upotrijebiti From zaglavlje za DKIM potpisivanje.

1. Odabrati Mail Policies > Signing Profiles
2. Pod DKIM Global Settings odabrati Edit Settings
3. Ovisno o zahtjevima, potrebno je konfigurirati sljedeće stavke:
4. DKIM potpisivanje poruka generiranih u sustavu
5. Koristiti From zaglavlje za DKIM potpisivanje
6. Izvršiti promjene

Za kraj je potrebno još verificirati dolazne poruke koristeći DKIM:

1. Kreirati profil za verifikaciju poruka koristeći DKIM
2. Odrediti prilagođeno pravilo protoka elektroničke pošte za provjeru dolaznih poruka pomoću DKIM-a
3. Odrediti prilagođeno pravilo protoka elektroničke pošte za potvrdu dolaznih poruka pomoću DKIM-a
4. Odrediti što će Ironport poduzeti sa provjerenim porukama
5. Na temelju prethodnog koraka pridružiti poruke grupama određenih pošiljatelja ili primatelja.

5.DMARC – Domain based Message Authentication, Reporting and Conformance

DMARC (eng. Domain based Message Authentication, Reporting and Conformance) protokol definira skalabilni mehanizam pomoću kojeg organizacija koja šalje poruku elektroničke pošte može izraziti preferencije na razini domene za provjeru valjanosti, selekciju i izvještaje, a organizacija koja prima elektroničku poštu može te postavke koristiti za poboljšanje rukovanja poruka elektroničke pošte. DMARC protokol je dizajniran tako da primateljima poruke elektroničke pošte omogućava bolju kontrolu temeljenu prema reputaciji domene pošiljatelja. Omogućuje strani koja šalje poruku razne opcije za objavljivanje politika za poboljšanje učinkovitosti protiv neželjene pošte i krađe identiteta, samim time gradeći bolju reputaciju domene. DMARC za cilj ima:

- Mora biti skalabilan,
- Smanjiti krađe identiteta,
- Primijeniti pravila za pošiljatelja,
- Pružiti izvještaje o autentikaciji.[22]

Kako bi DMARC mogao funkcionirati, domena sa koje se šalje poruka mora objaviti SPF i DKIM zapis. Nakon postavljanja SPF i DKIM zapisa, DMARC se može konfigurirati dodavanjem parametara u TXT zapise domene (na isti način na koji se objavljuju SPF i DKIM zapisi). TXT zapis bi trebao biti konfiguriran na sljedeći način: "_dmarc.example_domain.com."

[22] What is a DMARC record and how do I create it on DNS server? – SonicWall; dostupno na https://www.sonicwall.com/support/knowledge-base/what-is-a-dmarc-record-and-how-do-i-create-it-on-dns-server/170504796167071/

5.1.DMARC zahtjevi

DMARC zahtjevi određuju na koji način će se postavi jasni ciljevi za poboljšanje autentikacije, poboljšanu sigurnost, detaljno odabrane zahtjeve, te stavkama koje su dokumentirane kao opcije koje su izvan kruga djelovanja DMARC-a. Jasni ciljevi mogu biti:

- Dopustiti vlasnicima domena da provjere autentičnost sa svoje strane,
- Minimizirati složenost implementacije za pošiljatelje, i za primatelje, kao i utjecaj na rukovanje i isporuku legitimnih poruka,
- Smanjiti količinu uspješno isporučenih lažnih poruka elektroničke pošte,
- Dopustiti vlasnicima domene da lakše kontroliraju greške autentikacije.

DMARC protokol nastoji izbjeći potrebu za trećim stranama ili unaprijed definiranom sporazumu za slanje poruka između pošiljatelja i primatelja. S takvim zahtjevom održavaju se pozitivni aspekti trenutne infrastrukture elektroničke pošte. Iako DMARC nema potrebu za uključivanjem pošiljatelja trećih strana (vanjske organizacije ovlaštene za slanje u ime operatora) u proces slanja poruka elektroničkom poštom, on ih striktno niti ne isključuje. U principu, treće strane mogu pružiti uslugu zajedno s DMARC-om, ako za to postoji potreba. DMARC je osmišljen da spriječi napadače da šalju poruke za koje tvrde da dolaze od legitimnih pošiljatelja, posebno pošiljatelja transakcijskih poruka elektroničke pošte npr. unutar bankarskog sustava. Jedan od glavnih napada ove vrste lažirane pošte je krađa identiteta. Dakle, DMARC je značajno informiran o stalnim naporima za uvođenje snažnih i učinkovitih anti-phishing mjera unutar organizacije. Iako se DMARC može koristiti samo za borbu protiv specifičnih oblika napada na domenu, jasno je da DMARC može biti koristan u stvaranju sigurnih i pouzdanih protoka poruka. DMARC se ne trudi riješiti sve probleme nastale lažiranjem porukama elektroničke pošte.

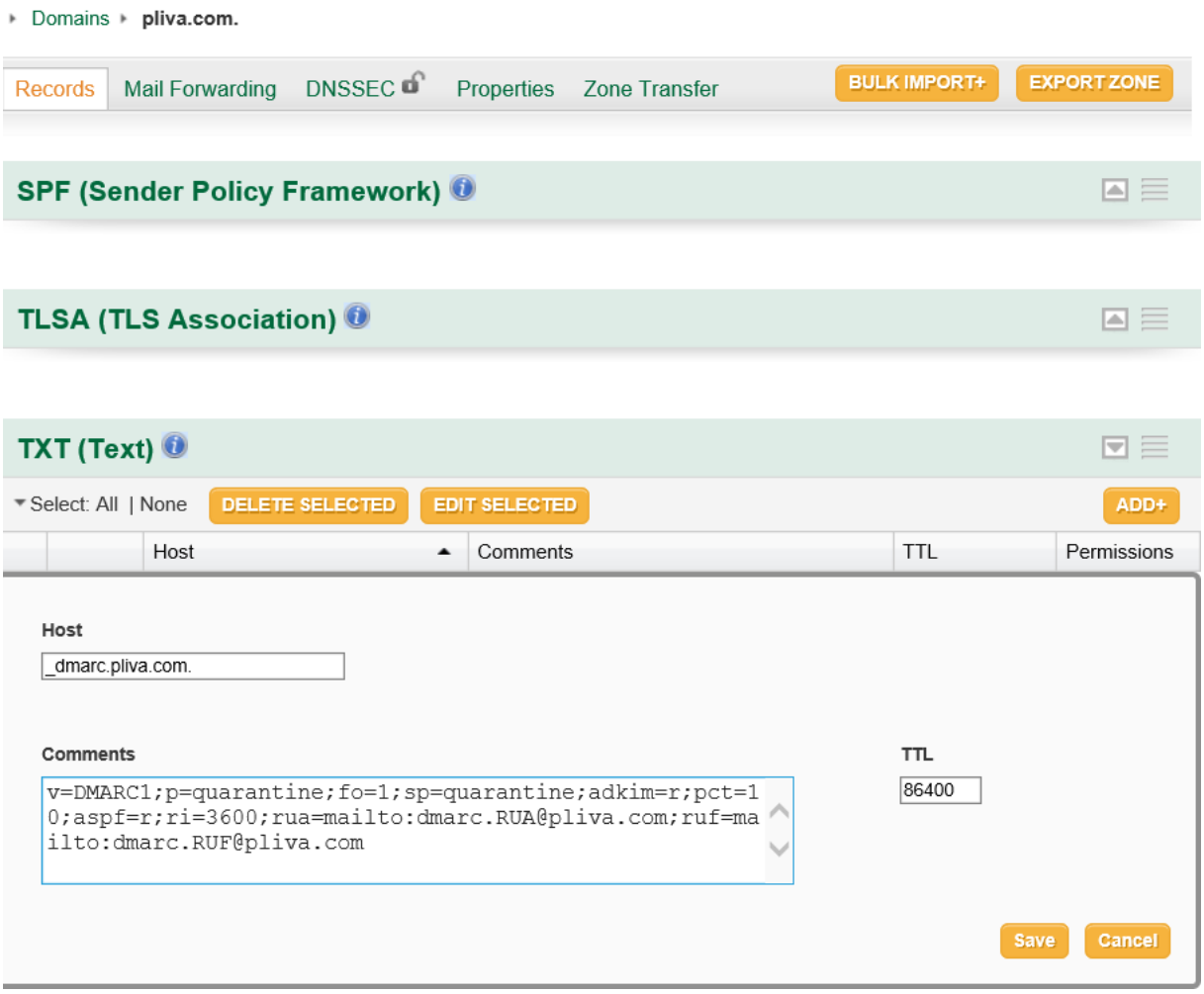
Tehnologije koje služe za provjeru identiteta poruke elektroničke pošte potvrđuju različite aspekte pojedine poruke. DKIM protokol ovjerava domenu koja je postavila potpis poruci, dok SPF protokol može potvrditi identitet bilo koje domene. From zaglavlje je odabran kao središnji identitet DMARC-a, jer je to obavezno polje zaglavlja poruke i stoga je zajamčeno da će biti prisutno u kompatibilnim porukama. From, kao začetnik poruke, krajnjim korisnicima prikazuje dio ili cijeli sadržaj samog zaglavlja. Stoga je From polje segment koji krajnji korisnici koriste za prepoznavanje izvora poruke, te samim time postaje glavni cilj za zlouporabu. Mnogi davatelji usluga elektroničke pošte, zahtijevaju da se pošiljatelju provjeri

autentičnošću prije nego što se poruka elektroničke pošte može generirati. Dakle, ovaj mehanizam krajnjem primatelju pruža snažne dokaze da je poruku doista stvorio pošiljatelj s kojim je povezan, te da su pružene sve mjere zaštite koje su propisane. Unutar DMARC-a pošiljatelji mogu odrediti „strogi“ (eng. strict) ili „opušteni“ (eng. relaxed) način rada u smislu prisiljavanja provjera identifikatora. . U „strogom“ načinu rada, svi identifikatori iz sustava za provjeru autentičnosti na kojima se zasniva DMARC moraju se podudarati sa From zaglavljem. U „opuštenom“ načinu rada verificirane domene moraju se podudarati. „Opušteni“ način je automatski zadani način rada. DMARC dopušta „strogo“ ili „opušteno“ poravnavanje identifikatora na temelju rezultata provjere identiteta. (nisu povezani sa DKIM-ovim načinima kanonizacije.) U „opuštenom“ načinu, verificirane domene, obje DKIM autorizirane domene za potpisivanje moraju biti jednake kako bi se identifikatori smatrali usklađenima. U „strogom“ načinu rada smatra se da se točnim podudaranjem oba potpuno kvalificirana imena domene (engl. FQDNs) dobije usklađivanje identifikatora. Usklađivanje identifikatora je potrebno jer poruka može imati valjani potpis s bilo koje domene, uključujući i ne valjane domene. Stoga, čak ni valjani potpis nije dovoljan da smatra autorovu domenu ispravnom. Treba biti oprezan i znati da jedna jedina poruka elektroničke pošte može sadržavati više potpisa DKIM-a, a smatra se da je DMARC „prolazna“ točka ako je bilo koji potpis DKIM-a validan i potvrđen.

5.2.DMARC politike

DMARC pravila objavljuju vlasnici domena, a primjenjuju ih primatelji pošte. Vlasnik domene oglašava participaciju jedne ili više domena unutar DMARC-a pridruživanjem DNS TXT zapisa tim domenama. Pritom, vlasnici domena određuju posebne zahtjeve prema primateljima pošte, u vezi s raspoređivanjem poruka za koje se smatra da su iz jedne od domena vlasnika domene, te pružanje povratnih informacija o tim porukama. Vlasnik domene može odlučiti ne sudjelovati u DMARC procjeni od strane primatelja pošte. Na primjer, ako se rezultati provjere autorizacije ne bi podudarali sa dijelom konfiguracije DMARC-a za određenu domenu, tada vlasnik domene ne objavljuje SPF zapis određen prema pravilima, koji rezultira potvrdom SPF-a. Primatelj pošte koji implementira DMARC mora se maksimalno potruditi da se pridržava objavljenih pravila DMARC-a od strane vlasnika domene ukoliko poruka ne prođe unutar DMARC testa. Budući da razmjena elektroničke pošte može biti kompliciranа, primatelji pošte mogu odstupiti od objavljenih pravila vlasnika domene tijekom obrade poruka, te navesti razlog odstupanja vlasniku domene putem izvještaja o povratnim informacijama. DMARC postavke vlasnika domene pohranjuju se kao DNS TXT zapisi u pod domene nazvane "_dmarc". Na

primjer, vlasnik domene "pliva.com" objavljuje postavke DMARC-a u TXT zapisu kao "_dmarc.pliva.com". Slično tome, primatelj poruke koji šalje upit za postavke DMARC-a u vezano za poruku elektroničke pošte sa domene „pliva.com“ izdao bi TXT upit DNS-u za pod domenu „_dmarc.pliva.com“. DMARC podaci smješteni unutar DNS-a nakon konfiguracije nazivati će se DMARC zapis, vidi sliku 26. Korištenje DNS-a, kao usluge zaslužne za upite, pruža prednosti kao što su dobro uspostavljena infrastruktura, administracija i razina upravljanja, i zbog toga ne mora se stvarati nova infrastruktura.



Slika 26. Primjer DNS TXT zapisa za DMARC

Samo se oznake koje su dopuštene od strane DMARC-a dodaju u registar, dok se nepoznate oznake moraju zanemariti. Kao obavezne DMARC oznake uvode se sljedeće oznake:

- v - oznaka verzije koja identificira zapis koji je preuzet kao DMARC zapis. Vrijednost mora biti DMARC1 i biti navedena prva u DMARC zapisu

- p - označava traženo pravilo koje se primjenjuje nad porukom elektroničke pošte ukoliko ne uspije proći provjeru autentičnosti DMARC-a. Pravilo se primjenjuje na primarnu domenu i sve njene pod domene. Postoje tri vrste pravila:
    - None – znači da administratori elektroničke pošte neće poduzimati nikakve radnje sa porukama koje ne odgovaraju DMARC-u,
    - Quarantine – znači da sve poruke elektroničke pošte koje ne prođu DMARC kontrolu, administratori tretiraju kao sumnjive. Poruke elektroničke pošte se mogu staviti u karantenu koje čuvaju poruke unutar mape bezvrijedne pošte.
    - Reject – znači da administrator može odbaciti sve poruke elektroničke pošte koje ne prođu DMARC kontrolu.[23]

Ovo su opcionalne, ali ipak preporučene DMARC oznake:

- rua=mailto:address@example.com - oznaka koja administratorima daje do znanja gdje žele poslati izvještaj. Ti izvještaji pružaju uvid u zdravlje sustava elektroničke pošte,
- fo - oznaka koja administratorima pruža informacije o uzrocima zašto poruka elektroničke pošte nije uspjela proći SPF ili DKIM kontrolu. Dostupne su četiri opcije:
    - 0 – zadana opcija. Generira DMARC izvještaje o kvaru ako svi temeljni mehanizmi za provjeru autentičnosti (SPF i DKIM) ne daju potvrdan rezultat usklađenosti (pass),
    - 1 – generira DMARC izvještaj o kvaru ako je neki mehanizam provjere autentičnosti (SPF ili DKIM) proizveo nešto drugo nego usklađeni rezultat "prolaska",
    - d – generira DKIM izvještaj o pogrešci ako je poruka imala potpis koji nije uspio proći procjenu,
    - s - generira SPF izvještaj o pogrešci ako poruka nije uspjela proći SPF procjenu.

Opcionalne DMARC oznake:

- sp - oznaka se koristi kako bi prikazala traženo pravilo za sve pod domene ukoliko elektronička pošta ne izvršava provjere autentičnosti DMARC-a. Najučinkovitija je kada vlasnik domene želi odrediti različita pravila za primarnu domenu i sve pod domene,

[23]M. Kucherawy, Ed. :Domain-based Message Authentication, Reporting and Conformance (DMARC); dostupno na https://dmarc.org/draft-dmarc-base-00-01.html

- adkim - označava „strogo“ ili „opušteno“ podudaranje DKIM identifikatora. „Opušteno“ je postavljeno kao zadano,
- aspf - označava „strogo“ ili „opušteno“ podudaranje SPF identifikatora. „Opušteno“ je postavljeno kao zadano,
- pct - postotak poruka na koje se odnosi DMARC politika. Ova oznaka omogućuje način postupnog provođenja i testiranja utjecaja postavljenih pravila. Koriste se brojevi od 1-100, s time da je 100 postavljen kao zadani broj,
- ruf=mailto:address@example.com - oznaka koja administratorima omogućava da znaju gdje će se slati forenzički izvještaji. Forenzički izvještaji su detaljni i predviđeni su da administratorima budu isporučeni odmah nakon otkrivanja pogreške pri provjere autentičnosti DMARC-a.

6.Implementacija DMARC protokola kroz programska rješenja

Programska rješenja asistiraju jednoj ili više komponenti povezanih s DMARC protokolom i pomažu u sprečavanju malicioznih aktivnosti koje ugrožavaju zaposlenike ili klijente organizacije. DMARC programe koriste IT odjeli za konfiguriranje elektroničke pošte unutar organizacije, uključujući sve domene unutar organizacije. Utvrđivanjem DMARC protokola i nametanjem provjere autentičnosti DMARC-a pomoću ovih programa može se otkriti i blokirati sumnjiva aktivnost elektroničke pošte dizajnirana da se prikaže kao legalna poruka s jedne ili više registriranih adresa organizacije. DMARC program često se integrira sa sigurnosnim programom za prolaz elektroničke pošte, te neki programi u kategoriji sigurnog prolaza elektroničke pošte mogu sadržavati značajke povezane s DMARC sukladnošću. Savjetovanja o kibernetičkoj sigurnosti može pomoći menadžmentu organizacije da shvati važnost primjene DMARC protokola, zajedno s drugim sigurnosnim mjerama za zaštitu organizacije i klijenata od napada. Da bi program imao svrhu i koristio sve mogućnosti DMARC-a mora:

- Sadržavati znanje o SKF i DKIM protokolima i njihovim usklađivanjima,
- Skenirati adrese i poruke elektroničke pošte kako bi potvrdile DMARC protokol,
- Pomoći prilikom konfiguracije postavki za slanje poruka u skladu sa DMARC-om,
- Integrirati se sa programima koji blokiraju slanje lažnih poruka elektroničke pošte putem registriranih imena domena

Neki od trenutno najpoznatijih DMARC programskih rješenja su:

- Cisco Ironport - automatizira postupak provjere autentičnosti DMARC poruke elektroničke pošte i omogućava uvid u administraciju vlastite i vanjske pošiljatelje elektroničke pošte konfiguriranu na domeni. Informacije automatski povezuju u izvještaj koji se lako čita, u kojem se navodi tko šalje poruke elektroničke pošte u vaše ime i jesu li u skladu sa DMARC protokolom.
- EasyDMARC - je All-In-1 rješenje za sigurnost domene i infrastrukture elektroničke pošte. Njihovi alati pomažu prepoznati postojeće probleme i ispravno konfiguriraju domenu kako bi zaštitili organizaciju od napada krađe identiteta i povećali dostupnost elektroničke pošte,
- GoDMARC - jedan je od najboljih sigurnosnih programa koji sprječavaju krađu identiteta blokiranjem neovlaštenih poruka elektroničke pošte prije nego stignu do organizacije i njezinih zaposlenika,

- DMARC Analyzer - bori se protiv krađe identiteta i zlouporabe domena. Pomoću ovog programskog rješenja može se jednostavno implementirati DMARC protokol za sve domene u organizaciji, omogućavajući da se što prije krene prema DMARC pravilima odbacivanja neželjenih poruka.

6.1.DMARC implementacija kroz Ironport

Unutar ovog dijela rada, biti će ponajviše govora o načinu implementacije DMARC protokola kroz Ironport platformu. Ironport dopušta:

- Provjeru dolaznih poruka elektroničkih pošte pomoću DMARC protokola,
- Definirati profile za nadjačavanje pravila vlasnika domena,
- Slanje izvještaja vlasnicima domena sa povratnim informacijama, što pomaže u jačanju provjere njihove autentičnosti,
- Slanje izvještaja o pogreškama isporuke poruka vlasnicima domena ako veličina DMARC izvještaja prelazi 10 MB ili veličinu navedenu u RUA oznaci DMARC zapisa. Ironport neće izvršiti DMARC provjeru poruka s domena koje imaju nepravilno oblikovane DMARC zapise.

Sljedeće opisuje kako Ironport provodi provjeru DMARC protokola:

1. Slušatelj konfiguriran na Ironportu prima SMTP konekciju,
2. Ironport provodi SPF i DKIM provjeru prema poruci,
3. Ironport iz DNS-a dohvaća DMARC zapis za domenu pošiljatelja:
    - Ukoliko zapis nije pronađen, Ironport preskače DMARC provjeru i nastavlja sa obradom,
    - Ukoliko DNS upit ne uspije, Ironport poduzima mjere na temelju specificiranog profila DMARC provjere
4. Ovisno o rezultatima DKIM i SPF provjera, Ironport provodi DMARC provjeru nad porukom,
5. Ovisno o rezultatu DMARC provjere i specificiranom profilu DMARC provjere, Ironport može prihvatiti, staviti u karantenu ili odbiti poruku,
6. Ironport šalje odgovarajući SMTP odgovor i nastavlja obradu.

Dolazne poruke se mogu verificirati pomoću DMARC protokola, na sljedeći način:

1. Kreirati novi profil za potvrdu DMARC-a ili izmijeniti zadani profil za potvrdu DMARC-a
2. Konfigurirati globalne postavke DMARC-a
3. Konfigurirati pravila za protok pošte kako bi potvrdili dolazne poruke pomoću DMARC-a
4. Konfigurirati adresu za DMARC-ov izvještaj o povratnim informacijama
5. Pregledati izvještaj o verifikaciji i dolaznoj pošti DMARC-a, kao i poruke koje nisu uspjele proći DMARC provjeru.

Profil provjere DMARC-a je popis parametara koje pravila protoka elektroničke pošte Ironport-a koriste za provjeru DMARC-a. Na primjer, može se kreirati striktni profil koji odbacuje sve neusklađene poruke s određene domene, te manje striktni profil koji prebacuje sve poruke koje nisu u skladu s domenom u karantenu. Profil provjere DMARC sastoji se od sljedećih informacija:

- Ime za profil verifikacije,
- Poruka koja javlja što se treba poduzeti kad je pravilo u DMARC zapisu odbaci,
- Poruka koja javlja što se treba poduzeti kad je pravilo u DMARC zapisu karantena,
- Poruka koja javlja što se treba poduzeti slučaju privremenog neuspjeha verifikacije,
- Poruka koja javlja što se treba poduzeti slučaju trajnog neuspjeha verifikacije.[24]

Procedura kojom se može kreirati profil provjere DMARC protokola (Slika 27.) je:

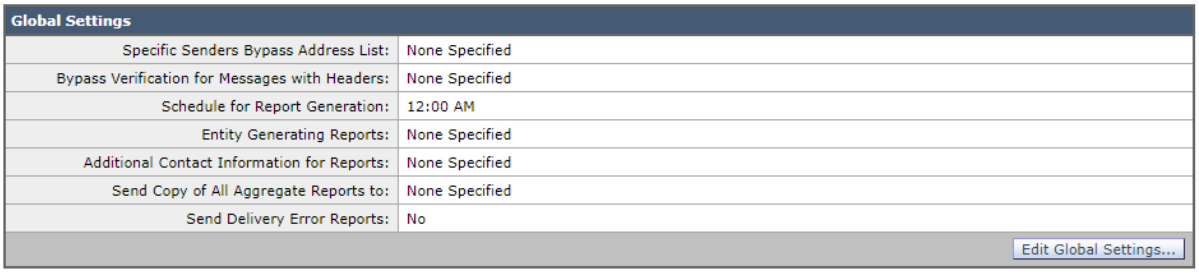
1. Odabrati Mail Policies > DMARC
2. Odabrati Add Profile
3. Upisati ime profila
4. Odrediti radnju koju Ironport poduzima kada se pravilo u DMARC zapisu odbaci, npr:
    - No Action – Ironport ne poduzima ništa protiv poruka koje nisu uspjele proći provjeru DMARC-a,
    - Quarantine – Ironport šalje poruke koje nisu uspjele proći provjeru DMARC-a u karantenu,

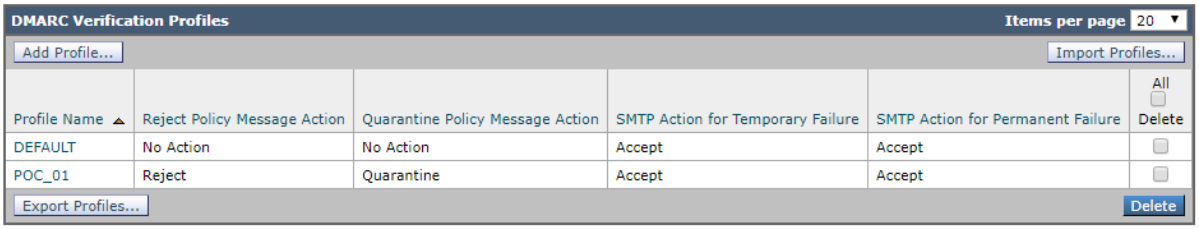
[24] User Guide for AsyncOS 11.0 for Cisco Email Security Appliances, First Published: 2017-05-31

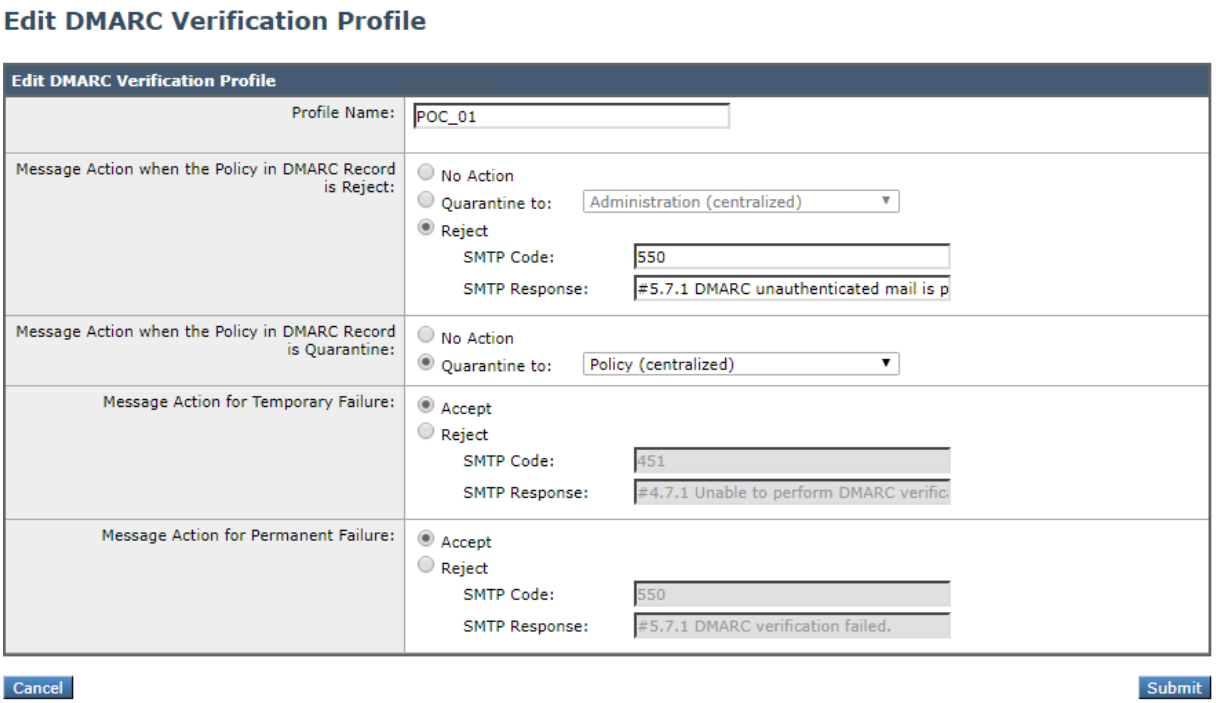
- Reject – Ironport odbacuje sve poruke koje nisu uspjele proći provjeru DMARC-a i vraća zadani SMTP odgovor: 550 and #5.7.1 DMARC unauthenticated mail is prohibited

5. Odrediti radnju koju Ironport poduzima kada je pravilo u DMARC zapisu karantena,
6. Odrediti radnju koju Ironport poduzima kada je rezultat privremeni neuspjeh verifikacije DMARC-a, npr:
    - Accept – Ironport prihvaća poruke koje rezultiraju privremenim neuspjehom tijekom provjere DMARC-a,
    - Reject – Ironport odbacuje poruke koje rezultiraju privremenim neuspjehom tijekom provjere DMARC-a i vraća zadani SMTP odgovor: 451 and #4.7.1 Unable to perform DMARC verification
7. Odrediti radnju koju Ironport poduzima kada je rezultat trajni neuspjeh verifikacije DMARC-a, npr:
    - Accept – Ironport prihvaća poruke koje rezultiraju trajnim neuspjehom tijekom provjere DMARC-a,
    - Reject - Ironport odbacuje poruke koje rezultiraju privremenim neuspjehom tijekom provjere DMARC-a i vraća zadani SMTP odgovor: 550 and #5.7.1 DMARC verification failed
8. Izvršiti promjene

DMARC







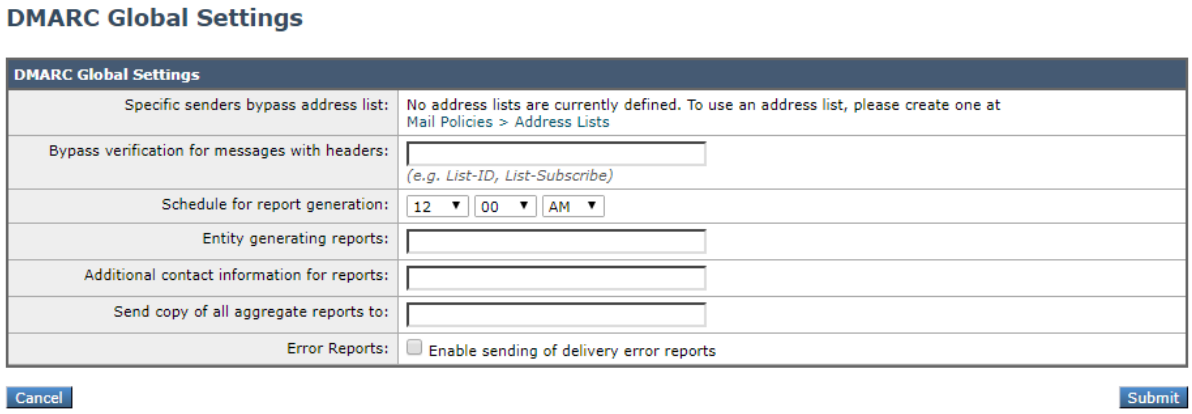
Slika 27. Konfiguracija profil provjere DMARC protokola

Globalne postavke DMARC protokola konfiguriraju se kroz Ironport (Slika 28.):

1. Odabrati Mail Policies > DMARC
2. Odabrati Edit Global Settings
3. Promijeniti postavke koje su definirane sljedećim parametrima:
    - Specifični pošiljatelji zaobilaze adresnu listu – preskače se DMARC provjera poruka od stane određenih pošiljatelja,
    - Zaobilazi se provjera za poruke s zaglavljima – preskače se DMARC provjera poruka koje sadrže određena zaglavlja. Na primjer, ova opcija se kod pouzdanih pošiljatelja,
    - Raspored generiranja izvještaja - vrijeme kada se odlučuje da Ironport generira DMARC izvještaj. Na primjer, za generiranje izvještaja može se odabrati vrijeme izvan radnog vremena kako bi se izbjegao utjecaj na protok pošte,
    - Izvještavanja entiteta - Entitet generira DMARC izvještaje. Tim putem se pomaže vlasnicima domena koji primaju DMARC izvještaje da identificiraju entitet koji je generirao izvještaj,
    - Poslati kopiju svih izvještaja - Poslati kopiju određenim korisnicima, npr. internim korisnicima koji obavljaju analizu izvještaja

- Izvještaj o pogreškama – poslati izvještaj o pogreškama u isporuci vlasnicima domene ako je DMARC izvještaj veći od 10 MB.

4. Izvršiti promjene



Slika 28. Globalne postavke DMARC protokola

Konfiguriranje provjere DMARC protokola vezanim za pravila protoka pošte:

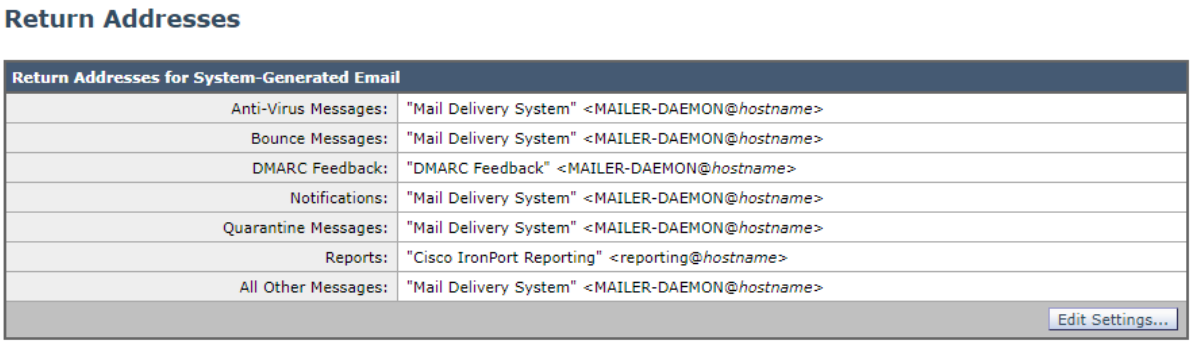
1. Odabrati Mail Policies > Mail Flow Policies
2. Odabrati pravila dolazne pošte za slušatelja na kojem se želi izvršiti provjera
3. Pod Security Features omogućiti DMARC Verification - > On
4. Odabrati profil za provjeru DMARC protokola
5. Omogućiti slanje izvještaja o povratnim informacijama DMARC protokola
6. Izvršiti promjene

Verifikacijske log poruke dodaju se u logove elektroničke pošte tijekom sljedećih faza provjere DMARC protokola:

- Pokušaj provjere DMARC protokola prema poruci,
- DMARC potvrda je završena,
- Podaci o potvrdi DMARC protokola, uključujući rezultate usklađenosti DKIM i SPF protokola,
- Provjera DMARC protokola prema poruci se preskače,
- DMARC zapis je dohvaćen i analiziran,
- Isporuka izvještaja DMARC protokola za domenu nije uspjela,
- Uspješno je isporučen izvještaj o pogrešci,
- Isporuka izvještaja o pogrešci za domenu nije uspjela

Konfiguracija povratne adrese za izvještaje o povratnim informacijama DMARC protokola (slika 29.):

1. Odabrati System Administration > Return Addresses
2. Odabrati Edit Settings
3. Napisati povratnu adresu za izvještaj o povratnim informacijama DMARC-a
4. Izvršiti promjenu.



Slika 29. Konfiguracija povratne adrese za DMARC protokol

7.Zaključak

Da bi se poruka elektroničke pošte poslala i isporučila na zatraženu lokaciju, potrebo je slijediti različite parametre za različite protokole. Infrastruktura elektroničke pošte mora biti robusna i jasno definirana, počevši od klijenata koji služe za skladištenje poruka elektroničke pošte, preko administratora koji sudjeluju u nadgledanju protoka pošte, sve do poslužitelja, te ostalih mehanizama koji su uključeni u proces razmjene elektroničke pošte. U ovom radu razrađeni su svi relevantni protokoli koji služe za sigurnu i pouzdanu razmjenu poruka elektroničke pošte. Prikazani protokoli nisu jednosmjerni, oni služe Svaki protokol ima svoje dobre i loše strane i jasno prikazuju u kojem slučaju se mora odabrati koji protokol. U većini slučajeva vežu se jedan na drugog i tako zatvaraju krug u procesu razmjene elektroničke pošte. Glavni i odgovorni za razmjenu poruka elektroničke pošte je SMTP protokol kojim se šalju naredbe između klijenta i poslužitelja i time se preciziraju primatelj i pošiljatelj. S obzirom da se SMTP protokol smatra push protokolom, odnosno njime se šalje poruka, ali nije moguće sa pošiljatelja preuzeti poruku. I tu u pomoć priskače jedan od protokola koji služe za primanje elektroničke pošte sa poslužitelja, POP3 ili IMAP. Oba protokola načelo imaju istu svrhu, ali s obzirom na razvoj elektroničke pošte, koriste se u različitim slučajevima. POP 3 je izuzetno jednostavan protokol za konfiguriranje i održavanje, ali mana mu je što porukama elektroničke pošte nije moguće pristupiti na drugim uređajima. Iz toga razloga, ovaj protokol se sve manje koristi, a njegovu uslugu preuzima IMAP. IMAP protokol svoju širinu dobiva zbog autentikacije kojom se omogućuje pristup pretincima elektroničke pošte samo ovlaštenim korisnicima, a enkripcijom se štite podaci koji se šalju putem mreže. Glavna prednost nad POP3 protokolom je mogućnost istovremenog pristupa istom poštanskom pretincu sa različitih uređaja, te nakon svakog povezivanja klijenta sa IMAP poslužiteljem, sinkroniziraju sve promjene.

Kako je elektronička pošta postala interesantan komunikacijski kanal za širenje neželjene pošte, zlonamjernih programa ili phishing napada, a sa ciljem priskrbljivanja osjetljivih informacija, prevare ili zarade, sigurnosni mehanizmi za zaštitu domena moraju biti opće prihvatljivi. Kroz rad smo prošli kroz četiri najvažnija oblika napada na korporativnu sigurnost, kao i na sigurnost korisnika. U praksi nije isključeno da organizacija bude napadnuta od svih napada u isto ili slično vrijeme, drugim riječima napadi mogu biti međusobno povezani. Spam napadi, odnosno napadi neželjenom poštom šalju se kako bi se širile lažne obavijesti, bez prethodnog odobrenja korisnika za primanje takvih poruka. Popularan je način napada zbog toga jer ne predstavlja preveliki trošak implementacije i teško ih je otkriti, a usporedbi sa drugim napadima nagomilane poruke mogu zagušiti slobodni prostor, te onemogućiti primanje novih poruka

elektroničke pošte. Na Ironportu se trebaju postaviti mehanizmi za skeniranje koji daju ocjenu svakoj poruci i na temelju tih rezultata se određuje da li je poruka uistinu neželjena i što će se učiniti sa njom. Za razliku od spam napada, zlоćudni programi imaju namjeru ukrasti korisničke podatke i probiti se u operacijske sustave unutar organizacije. Obrana od takvih napada je korištene sigurnosnih protokola, kao npr. HTTPS iz razloga jer podaci se kopiraju za vrijeme tranzita i čini ih teško dohvatljivim. Unutar Ironporta je potrebno postaviti pregledavanje virusa za zadana pravila pri dolaznoj i odlaznoj pošti, i time se skenira svaka datoteka, identificira tip virusa i sukladno tome primjenjuje se odgovarajuća tehnika. Phishing napadi stvaraju dosta problema unutar organizacije zbog svoga načina interpretacije. Naime, phishing napadi većinom su bazirani na socijalnom inženjeringu i na lukav način pokušavaju doprijeti do korisnika, koristeći njihovu lakovjernost i neznanje. Kako bi se to spriječilo najbolji mehanizmi su osiguravanje pravovjernih informacija, održavanje stalnih edukacija, kao i podizanjem svijesti korisnika. DLP se koristi kao proces koji se koristi kao dodatni sloj koji osigurava da se osjetljivi podaci ne izgube, zloupotrebe, te da neovlašteni korisnici nemaju pravo pristupa tim podacima. Ironport određuje koja se pravila o odlaznoj pošti primjenjuju na pošiljatelja ili primatelja poruke elektroničke pošte, bazirano na temelju pravila koja su definirana.

Kolaboracija između protokola za zaštitu domene je obavezna i svrsishodna. Iako SPF i DKIM protokoli mogu biti samostalni, da bi DMARC imao svoju funkcionalnost, domena sa koje se šalje poruka mora imati objavljeni SPF i DKIM zapis. SPF se smatra protokolom koji je zamišljen da se nadograđuje na SMTP protokol, a tome je razlog taj što SMTP protokol nema jasan mehanizam autentikacije korisnika. Najjasniji zadatak SPF protokola zasigurno je taj da on štiti adresu koja se nalazi u Return-Path zaglavlju poruke, te time pokušava donekle zaštiti poruku. S obzirom da i u slučaju da poruka uspije pronaći način da zaobiđe SPF protokol, ne postoji jamstvo da se poruka neće isporučiti. U tom slučaju pomoć SPF protokolu pruža DMARC koji je dizajniran za rješavanje toga nedostatka unutar SPF protokola. Također, kao najčešća greška koja se događa prilikom implementacije SPF protokola smatra se ako postoji više SPF TXT zapisa unutar DNS-a, i na to treba dodatno pripaziti svaki administrator. Time se stvara problem prema poslužitelju jer će on teško znati koji je SPF TXT ispravan. Mozak SPF protokola su SPF zapisi koji se kreiraju za svaku domenu elektroničke pošte, i definiraju određene aspekte sigurnosne politike elektroničke pošte. Dok se DKIM protokol smatra kompliciranim za implementaciju, mišljenje unutar ovog rada je da je iznimno koristan za prijenos poruka elektroničke pošte na siguran i zaštićen način. Pošiljatelji moraju odlučiti što

će sve biti uključeno u postupku potpisivanja elektroničke pošte, te će oni ostati nepromijenjeni u tranzitu. DKIM protokol ovjerava domenu koja je postavila potpis poruci, dok SPF protokol može potvrditi identitet bilo koje domene Također, druga bitna stavka pri DKIM protokolu je proces kriptiranja uz pomoć privatnog ključa koji se izdaje za potrebnu domenu, i naravno samo pošiljatelj ima pristup tome ključu. I cijeli proces se završava sa provjerom potpisa DKIM-a uz pomoć javnog ključa i DNS-a. Potpisivanje DKIM-a u Ironport-u provodi se putem profila domena i omogućuje slanjem elektroničke pošte. Profili domena povezuje domenu s ključnim podacima o domeni. DMARC protokol se smatra novijim protokolom i uzima najbitnije i najkorisnije tehničke mogućnosti SPF i DKIM protokola. Baziran je na način da primatelji poruke elektroničke pošte imaju bolju kontrolu na temelju reputaciji domene pošiljatelja. DMARC koristi zahtjeve i politike koje oglašavaju vlasnici domena, a koriste ih primatelji elektroničke pošte. DMARC se konfigurira na način da se dodaju parametri u TXT zapise domene, ali tek nakon postavljanja SPF i DKIM zapisa. DMARC protokol u principu želi spriječiti napadače da šalju poruke elektroničke pošte za koje se tvrdi da dolaze od legitimnih pošiljatelja. Premda se DMARC protokol u načelu koristi za borbu protiv specifičnih oblika napada na domenu, očito je da DMARC može biti iskoristiv i u stvaranju sigurnih i pouzdanih protoka poruka.

U zadnjoj fazi rada objašnjeni su i prikazani programi koji se mogu koristiti za implementaciju DMARC protokola, njihove glavne karakteristike, te način na koji sprečavaju maliciozne aktivnosti unutar organizacije.

Literatura

[1] Email Security with Cisco IronPort (Networking Technology: Security) 1st Edition

[2] RFC 7489 - Domain-based Message Authentication, Reporting, and Conformance (DMARC). datatracker.ietf.org.

[3] Kucherawy, M.; Zwicky, E. (15 July 2013). "Domain-based Message Authentication, Reporting and Conformance (DMARC) [draft 01]". IETF. Appendix A.3, Sender Header Field. Retrieved 24 May 2016.

[4] Techaai Team, Ekyaku Ruth, Tech Ham: Your Guide To Email Security 2017: What You Should Know About Email Security 2017

[5] User Guide for AsyncOS 11.0 for Cisco Email Security Appliances, First Published: 2017-05-31

[6] M. Kucherawy, Ed. :Domain-based Message Authentication, Reporting and Conformance (DMARC); https://dmarc.org/draft-dmarc-base-00-01.html

[7] DKIM Email Security Standard; https://www.cyberpunk.rs/dkim-email-security-standard

[8] Everything you need to know about SPF – DMARC Analyzer; https://www.dmarcanalyzer.com/spf/

[9] CCERT-PUBDOC-2008-11-247- Limbo Malware; https://www.cert.hr/wp-content/uploads/2008/11/CCERT-PUBDOC-2008-11-247.pdf

[10] Data Loss Prevention (DLP) – Imperva; https://www.imperva.com/learn/data-security/data-loss-prevention-dlp/

[11] CCERT-PUBDOC-2006-05-159 SMTP protokol; dostupno na https://www.cert.hr/wp-content/uploads/2006/08/CCERT-PUBDOC-2006-05-159.pdf

Popis kratica

SMTP	*Simple Message Transfer Protocol*	Jednostavni protokol za prijenos poruka
POP3	*Post Office Protocol*	Protokol poštanskog alata
IMAP	*Internet Message Access Protocol*	Protokol za pristup porukama sa Interneta
TCP	*Transmission Control Protocol*	Protokol kontrole prijenosa
IP	*Internet Protocol*	Internetski protokol
DNS	*Domain name service*	Domenski sustav imena
MX	*Mail Exchanger*	Izmjenjivač pošte
TLS	*Transport Layer Security*	Sigurnost transportnog sloja
SSL	*Secure Sockets Layer*	Sloj osiguranih priključaka
URL	*Uniform Resource Locator*	Usklađeni lokator sadržaja
IDS	*Intrusion Detection System*	Sustav za otkrivanje upada
SPF	*Sender Policy Framework*	Okvir politike pošiljatelja
TXT	*Text*	Tekst
HAT	*Host Access Table*	Tablica pristupa domaćinu
DKIM	*DomainKeys Identified Mail*	Identificirana poštanska adresa
DMARC	*Domain-based Message Authentication, Reporting & Conformance*	Autentifikacija, izvješćivanje i sukladnost na temelju domene

Popis slika

„Pod punom odgovornošću pismeno potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada“.

U Zagrebu, 11.09.2019.