P2T: An Electronic Mail System with sender-oriented accountability

António Pais
antonio.pais.p2t@p2t.email
https://p2t.email

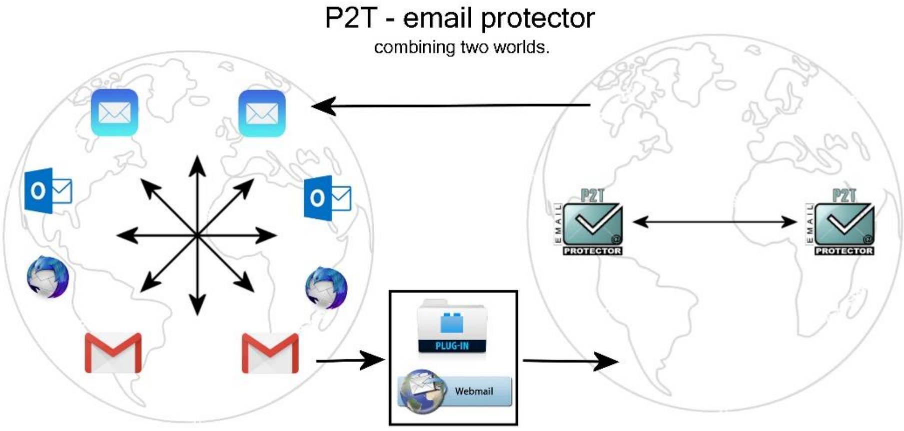
Synopsis. The email service is based on a client-server communications protocol structure created in 1971 and since then its main objective has always been the free and direct sending of messages from a sender to one or more recipients with only the email addresses being required to be known. Due to the fast adoption, it took the security needs for the following years were neglected at the new structure level, opting only to create external layers of solutions to continue to maintain the basic requirement it proposed since its creation. Today, and despite the exponential growth in technology associated with major players whose tools promise 99.99% protection capabilities, even so, after 50 years, email is still considered the largest attack vector for ransomware, phishing and malware in general. It is proposed to create a new email server software to run on a network consisting of a consortium of email service providers with anti-spam features, through a model called "Flow Control by Selection" (FCbyS) and which will operate from a responsibility-oriented perspective for the sending user, thus removing the need to invest in time, human resources and advanced technology to solve a problem created by a third party. The structure will be ensured by a DAO (Decentralized Autonomous Organization) consensus model to allow the constant improvements of the network and server software both in the implementation phase of new requirements and in the security of its constituents.

Compatibility with traditional users will be ensured by means of a gateway that, in addition to its native mode, will provide two more communication alternatives without the need to change known email protocols.

1. Introduction

This white paper describes the methods applied in P2T- email Protector's tools to protect users from email spam using a new concept called by the author as "Flow Control by Selection (FCbyS)". This innovative approach allows the email recipients to get rid of the cost burden problems caused by fraudster third parties. Emails are the number one malware and cybercrime delivery mechanism globally, according to David Bennett, Director of Operations at the Defense Information Systems Agency, the cyber security arm of the United States Defense Department. Cybercrime damages are on route to exceed $10.5 billion globally by the year 2025. This gives it a bigger market capitalization than the current worldwide black market in counterfeit currency and illegal drugs combined. According to the FBI, phishing was the most common type of cybercrime in 2020 (96%) and phishing incidents nearly doubled in frequency, from 114,702 incidents in 2019 to 241,324 incidents in 2020. Complaints were more than 11 times higher in 2020 compared to 2016. The entire world spam volume is already 75% being responsible for ransomware, phishing and other different types of malware making this type of criminal activity as the preferred attack vector. To solve this problem, we created a new and parallel structure with specific and proactive rules. P2T - email Protector, releases technology and financial resources for other important tasks, freeing users from email spam concerns by a fraction of the price of the other market offerings.

The following diagram shows the market positioning



P2T using a new protection model: Flow Control by Selection (FCbyS)

2. The email framework; Current Challenges

In recent years, the quality of cyber-attacks especially via e-mail has become sophisticated with the cyber criminals finding creative ways to by-pass the security and human controls. They constantly change their methods and avenues of attack, making it difficult to detect and easy for the user to give up something valuable. Attackers have also started targeting people from all levels of the organization, their customers and even partners. Simply visiting a poisoned site is all that is needed now to create havoc not only on your computer but also to the associated shares tied to your account. These attacks are typically sent via fraudulent e-mails that seem to come from a legitimate sender. Why the current protection model does not solve the email spam problem?! Because it uses FILTERS (some more complex than others, like filtering content for IP reputation, using heuristic methods, white lists, black lists, grey lists, etc.), and filtering models are reactive models, they're palliatives, unsuitable, because they go quickly obsolete by the amazing spam and botnet technology that exponentially increases almost every day. For this reason, various companies have felt the need to look for alternatives, (Skype, Whatsapp, Slack, Microsoft Teams, Telegram,…) which are less productive, but safer to use for communication purposes and less prone to abuse. So far, all of the alternatives found work well among peers while restricting communication between different market players. But e-mail is still the top choice for workplace communication in both big and small organizations, with an average office worker sending 40 and receiving 121 e-mails per day and we still need to use an e-mail address to sign up for the most varied services on the Internet. Therefore, it is not a surprise that e-mail remains the most exploited security threat in an organization. The P2T - email Protector plays a fundamental role to provide users a secure communication channel with all market players.

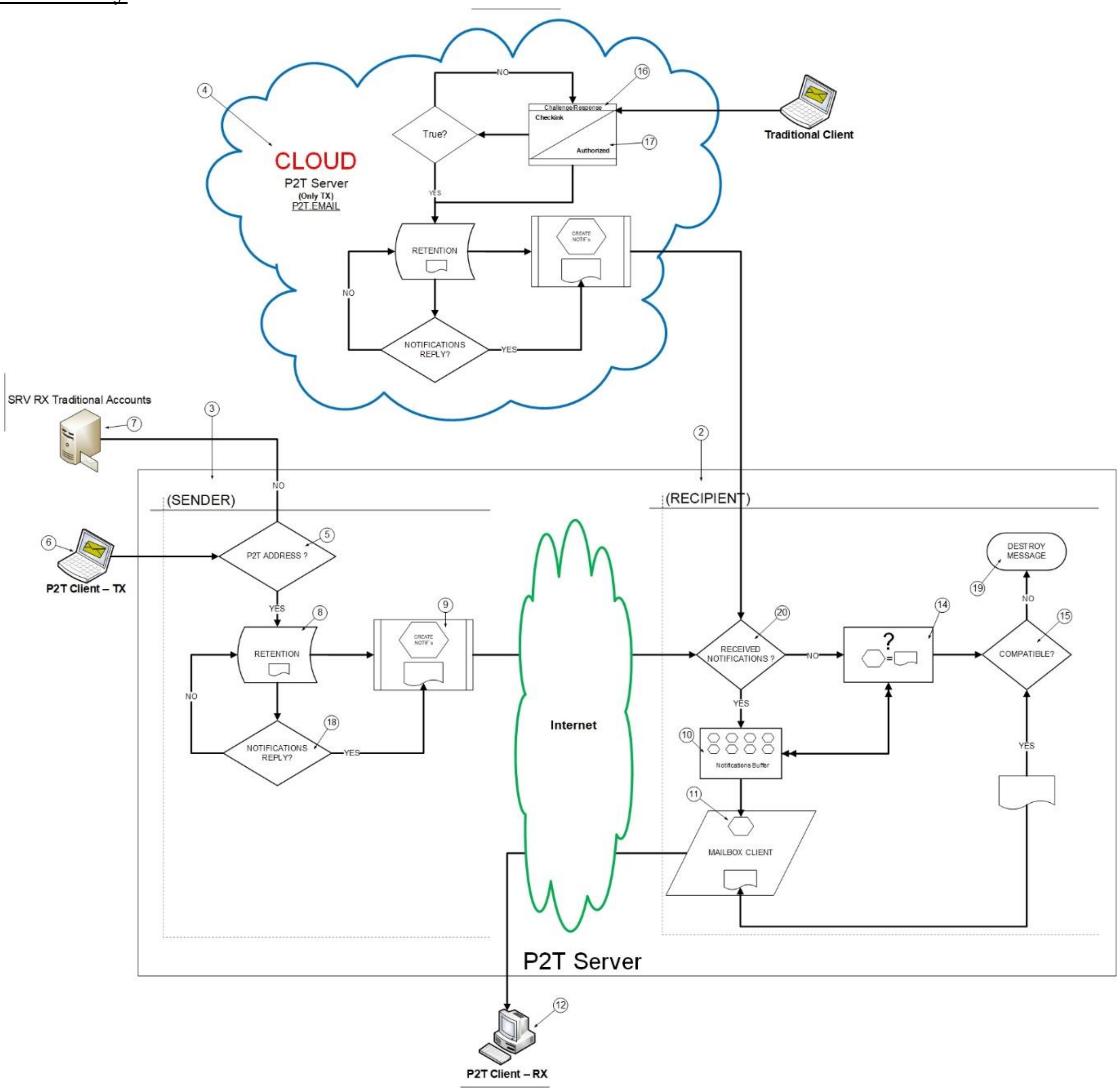
3. Basic Standards

As the volume of attacks on e-mails will only go up and the level of sophistication will only rise in the future, by thinking beyond reactive defense, and approaching e-mail security in a more agile way, organizations can prevent both internal and external e-mail threats. The P2T – email Protector new category of protection uses a preventive model being effective by acting directly on the spam source.

Customer Fit

Adopting a new solution means facing anxiety and inertia from old habits. Customers only go through it when your solution provides important enough value. That's why editing an e-mail, sending it, and receiving it will have minimal impact on your regular behavior. The spam folder no longer exists and the sending folder can be customized and managed. This is the only structural rule change. Managing the OUTBOX rather than the INBOX as it is usual in the traditional setting.

Tool Anatomy



Launching a new email server with more productive internal email management features.

a) Email management responsibility changes from the recipient to the sender side.

b) The recipient server performs a selection process where it will only receive two types of data.
  - Notifications
  - Messages preceded by notifications

c) Build a cloud gateway to ensure compatibility.

d) Create a "plug-in" to support communication.

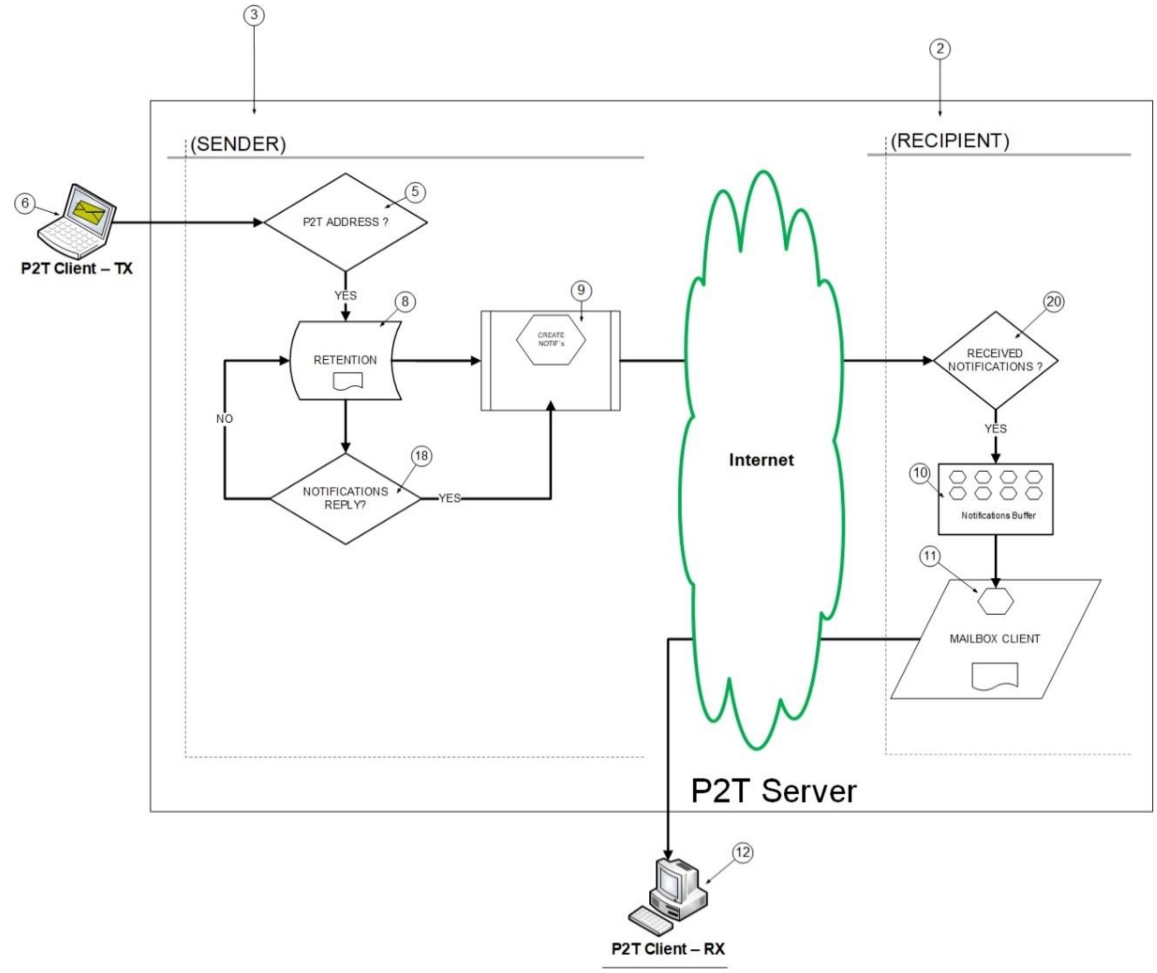
e) All servers will run in proprietary software controlled by the consortium.

4. Membership Community. How P2T (FCbyS) Works

Three likely scenarios:

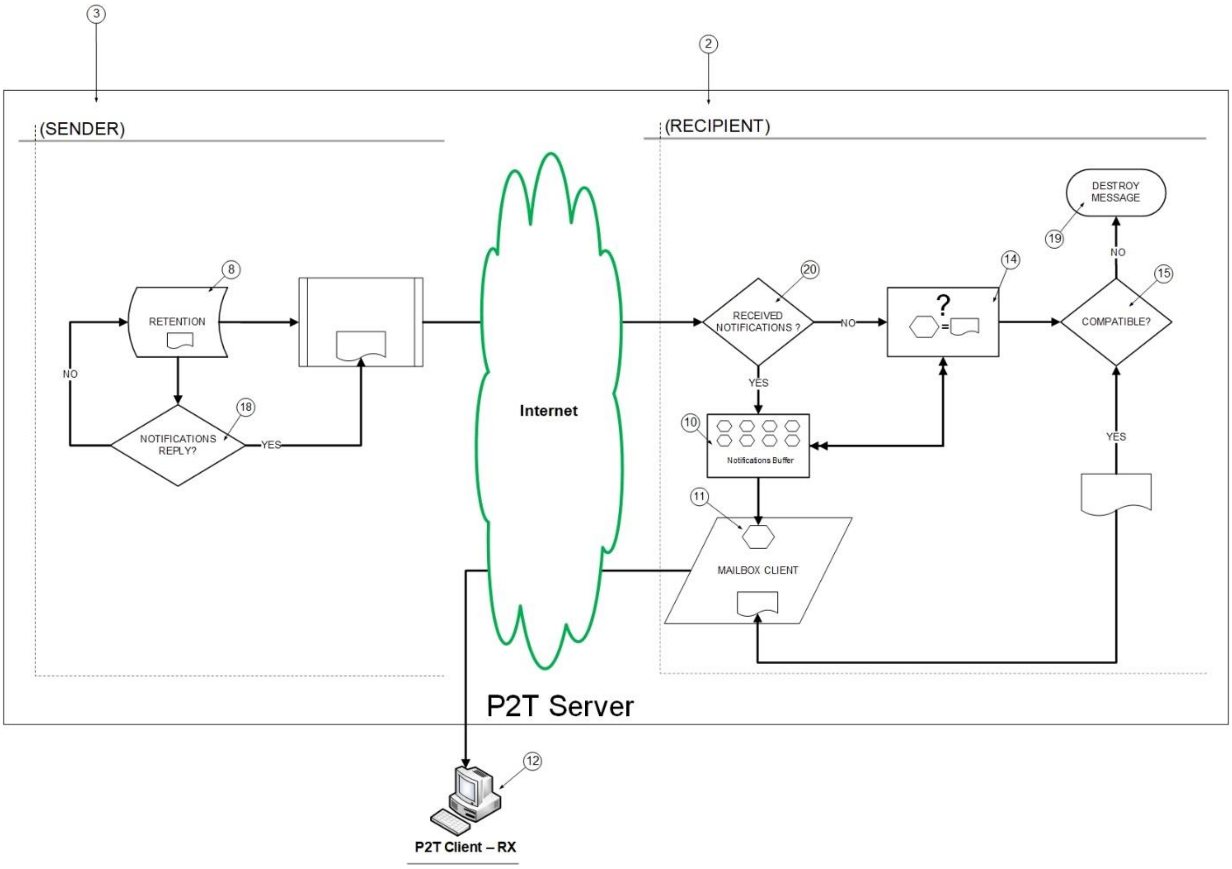
1. Exchanging emails between P2T - email Protector users

<u>Sending Process.</u>



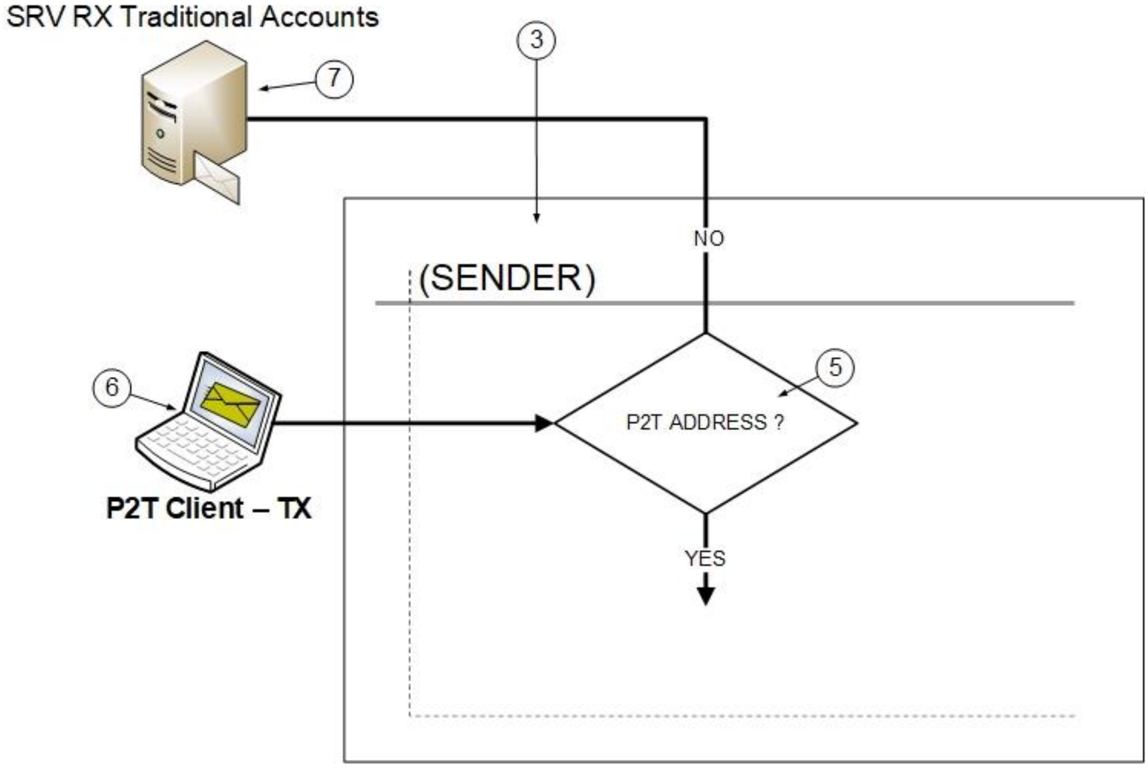
--

Receiving Process.



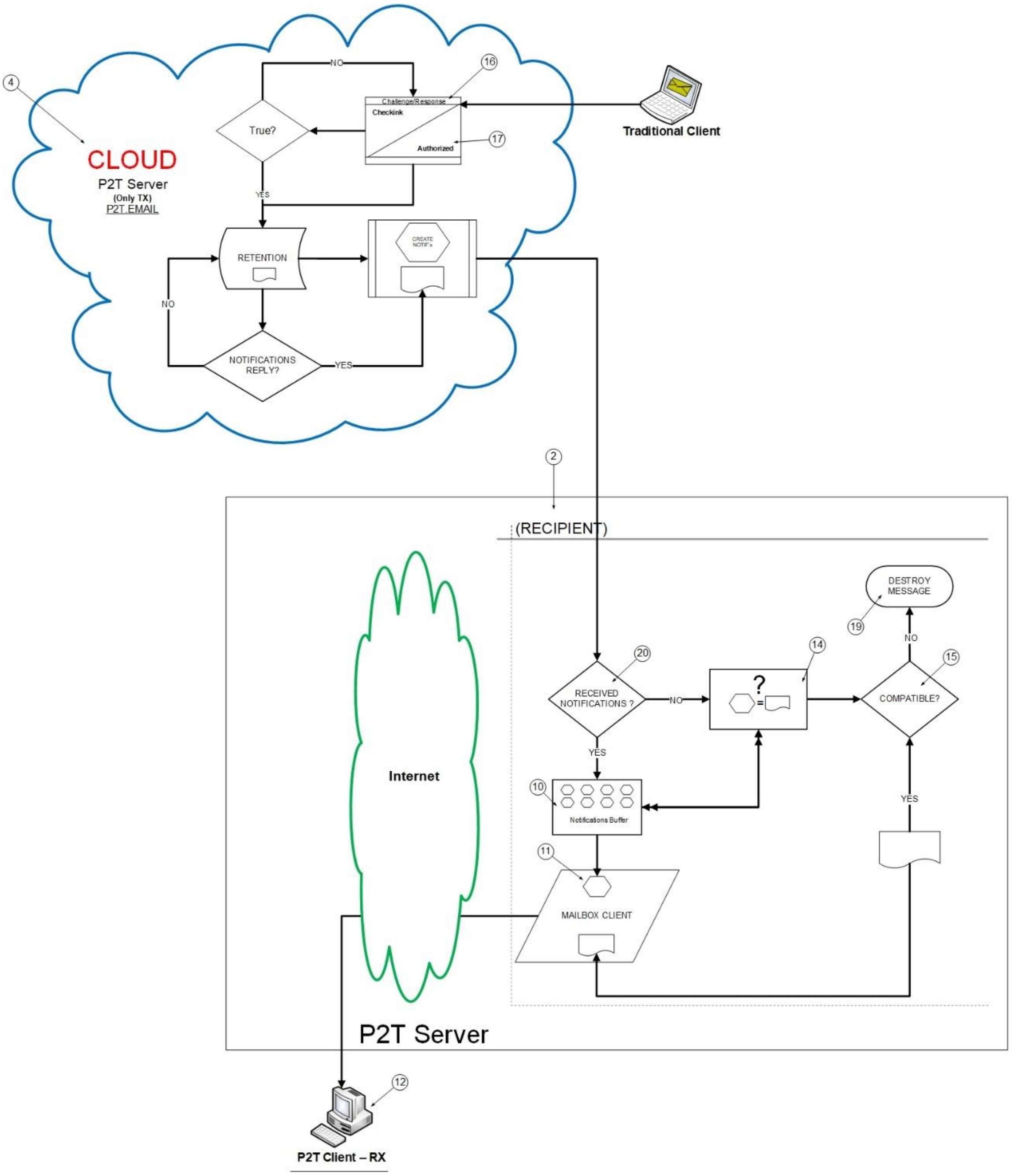
All messages issued are retained on the sender's server. Instead a notification (with the sender and recipient identification, the subject, the reception date and time, the attachments info, and an Ignore/Accept button) will be sent to the recipient's inbox. All messages held on the sender's outbox will be released only when the recipient clicks the "Accept" button. Dealing with all the "message garbage" and the server's capacity is from now on a sender problem.

2. Sending emails to non-P2T users



In this scenario there's no innovation. This process uses the current SMTP communication protocols matching all the market players. The P2T - email Protector's user message goes directly to the recipient’s inbox.

3. Receiving emails from non-P2T users



P2T - email Protector plays a fundamental role to provide users a secure communication channel with all market players. A free "plug-in" will be automatically granted to all P2T - email Protector customers' trusted contacts. By installing the plug-in in their usual email provider the non-P2T users became P2T - email Protector compatible. This feature allows P2T - email Protector users to remain shielded while receiving non-P2T user's communications. The other way for non-P2T users keeping in touch with P2T - email Protector ones is through a webmail service available on our webpage.

The P2T - email Protector client will have the "p2t" sign preceding the "@" e-mail symbol; example: name.p2t@domain. This automation will be created by means of an "alias".

5. The key points

Protection innovative tools;

- Identity dissimulation.

The traditional email template allows the use of a fake ID to avoid tracking. In the non-P2T user case the email recipient has no choice, as the message is already in his/her INBOX.

How big is this problem?? In a survey by Tessian, an email security software company for the enterprise market, they stated that 75% of organizations worldwide experienced some type of phishing attack in 2020. Another 35% experienced spear phishing attacks, and 65% faced Business Email Compromise attacks (BEC.) A BEC is "carried out by compromising legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds," according to the FBI. More colloquially, a BEC occurs when an employee receives what appears to be a genuine email from a senior executive. The email asks them to wire funds to a fake business account or provide personally identifiable information. The Internet Crime Complaint Center actually identifies five kinds of BEC swindles: bogus invoice, CEO fraud, account compromise, attorney impersonation, and data theft. To stem the tide, companies are setting up education and training programs to help staff recognize potential email fraud. Losses from commercial email compromise (BEC) have skyrocketed over the past year. The FBI's Internet Crime Report shows that in 2020, BEC scammers made more than $1.8 billion - more than through any other type of cybercrime.
With the P2T - email Protector model, accepting a notification of a false user will make it impossible to release the retained message because the provided address does not have the desired message. Therefore, the disclosure of an email address may even be encouraged and without the fear of being used by spammers.

- Botnets

In traditional systems users are infected with some variants of malware allowing the generation of automatic bots and the involuntary sending of emails to their address lists. As those bots do not need to pre-notify P2T - email Protector systems, they fill up the mailing lists promptly but the messages will never be delivered causing an instant alarm in the OUTBOX folder. This procedure ends up having preventive and decisive roles in botnet activities.

- Mass mailing

To be safe from the effects of email spam, non-P2T users must invest time, human and financial resources in the protection action. Now, with P2T - email Protector direct mail on the network imposes a heavy burden on the sender to handle unwanted messages! But, on the other hand, professional marketers with P2T - email Protector will have a comprehensive campaign tracking and analytics tool that quickly displays the results. P2T - email Protector eases human, technological, and financial resources for other important tasks.

Less is More;

- Less features needed / More protection granted.

Some existing features suggest additional operating capabilities to converge to more rigorous use, however, this will no longer be necessary in the P2T model. The simplicity of its use translates into a fairer and more accurate use. These are the ones with the greatest impact.

Features	P2T	Google	Exchange	Yahoo	Apple Mail	Thundirbird
undosent	unlimited	30s	30s (owa)	✗	30s	✗
spamfolder	no need	✓	✓	✓	✓	✓
false positives/negatives	no need	✓	✓	✓	✓	✓
hardbounce	no need	✓	✓	✓	✓	✓
spam filtering	no need	✓	✓	✓	✓	✓
delivery/read confirmation	no need	✓	✓	✓	✓	✓
opt-in/opt-out	no need	✓	✓	✓	✓	✓
webmail	✓	Gmail	Outlook	✓	iCloud	✗
botnet threat (email)	✗	✓	✓	✓	✓	✓

6. Storage Capacity

Organizations strive to optimize the use of their data centers, often they feel compelled to create quotas to manage their employees's mailboxes. Regardless of whether the recipient decides to archive an email, let it to read later, create filters to redirect to the spam folder, or even delete, they are all part of a set of incoming messages that were deposited freely on data centers by his/her email server. And, at some point, we have already experienced the boredom of sending a message to a destination and receiving a delivery error "The recipient's mailbox is full and cannot accept messages anymore. Please try again later or send back directly to the recipient." Determining the average size of an e-mail message is difficult because of all the factors that come into play. However, in general, an average email is about 75KB in size. Because 75KB is around 7,000 words in plain text or about 37.5 pages of typewriting, it stands to reason that other factors contribute to the size of an average email; I.messages contain formatting information in addition to mere text. II.rich text emails are often accompanied by a duplicate plain text version of the same message. III.newsletters and marketing emails are often longer, bigger emails and make up a large proportion of incoming mail. IV.attachments heavily skew the average. Although some attachments are small, some may be 10MB or larger. V.photos, animations, audio clips, and other attachments all add to the size. Animated GIFs are particularly size-hungry because every frame is essentially an image. The more frames the GIF has, the larger it is. VI.HTML takes up space. VII.in an email thread that goes back and forth, quoted material may appear several times. VIII.header information that describes the email's route isn't visible, but it counts in the size. Headers have a minimum value of about 1KB, and the maximum value may, in some cases exceed because of each router where this email passes by adding more information.
A P2T notification works like an original message, but without the body and its size content will be equivalent to that of a header. In conclusion, one could say in a simplistic way that 75 P2T notifications roughly account for the size of a single message.

7. Comparing deals

The following table describes the main differences between the current market offer and P2T value proposition:

Market Offer	P2T Value Proposition
Filter capabilities of 99,99%.	100% protection capabilities.
Accountability on the receiver side.	Accountability on the sender side.
Prone to false-positives/negatives.	Flow control by selection.
Permissiveness to BotNet networks.	Incompatible with BotNet networks.
Easy hiding user user ID.	Non-repudiation user ID.
Concern to hide email addresses.	Sharing email addresses.
Bandwidth occupied by unsolicited messages.	Maximized performance. Only authorized email traffic.

8. Conclusion

"*Insanity is doing the same thing over and over again and expecting different results*" The author proposed a paradigm shift to everything that has been offered as a solution over the last 50 years which led to the proposed standard change of filtering models to Flow Control by Selection (FCbyS) offering consequently fairer protection for the recipient. It would be essential to keep the current email communication protocols choosing only to change the way messages would be managed inside the P2T servers which led to create new internal rules for that purpose. This made it incompatible to any abusive user or botnet networks the direct and uncontrolled action of abusing the system. All contents of interest will from now on be the accountability of the sender to manage everything that recipients did not wish to receive, reinforcing the need to remain exposed on the network in order to release them. The reversal of this accountability is the number one pillar of this project's success. Finally, he proposed the need to strengthen security and future improvements with a solution based on consensus by an Autonomous Decentralized Organization (DAO) keeping the trend and technological adaptation for the near future.

9. References

[1] D. J. Bernstein, "Internet mail"
http://cr.yp.to/im2000.html

[2] Andrew Leung - TELUS Corporation, "SPAM – The Current State"
https://sicherheitskultur.at/pdfs/spam.pdf

[3] Tessian - Enterprise Email Security Software
https://www.tessian.com/blog/phishing-statistics-2020/

[4] Steve Morgan, Editor-in-Chief – "Cybercrime Magazine"
https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

[5] FBI - Internet Crime Complaint Center IC3
https://www.ic3.gov/Media/Y2019/PSA190910

Assinado por : **ANTÓNIO MANUEL DE JESUS PAIS**
Num. de Identificação: BI06266364
Data: 2021.05.03 20:41:34+01'00'

CHAVE MÓVEL