Managed Anti-Spoofing

LGA Security Management

What is anti-spoofing?

Anti-spoofing is a technique used to identify, quarantine or drop forged emails that have a false sender address. Phishing attacks and spam emails can spoof the email header to mislead the recipient about the sender of the email.

Why is having an anti-spoofing solution important for your company?

Hackers can easily forge the email of, for example, one of your vendors, asking you to make payment for an unauthorised transaction. If you are not careful, there is a chance that you might fall for it and make the payment. Therefore, without anti-spoofing, you are easily opening yourself up to business email compromise attacks, which can lead to serious business losses.

How does the anti-spoofing solution work?

Spoofed emails are mitigated through the implementation of 3 key email security protocols, SPF, DKIM and DMARC, which will be configured in the domain name server (DNS) and email server.

When a sender sends you an email, the email will be sent through the sending email server to the receiving email server where the sent email will be signed using a private key. Next, the email will go to the sending organisation's DNS server, which stores the published SPF record, DKIM public key and DMARC. The email will be cross checked against the stored records. If the email passes the 3 policy checks, this means the email is from a legitimate source and will be sent to your inbox. If one of policy check fails, the email will either be quarantined or rejected.

ABOUT LGA

LGA Telecom Pte Ltd is an established Managed Security Services Provider, and an industry pioneer that has helped shape Singapore's Internet ecosystem back in 1995. Over 25 years, We have been delivering resilient enterprise solutions that ensure un-interrupted business operations. Today, LGA offers comprehensive managed security services and solutions that identify, alert and mitigate technological vulnerabilities, threats and potential breaches to the network and systems. Enterprises and government agencies rely and trust LGA for their security needs beyond connectivity.

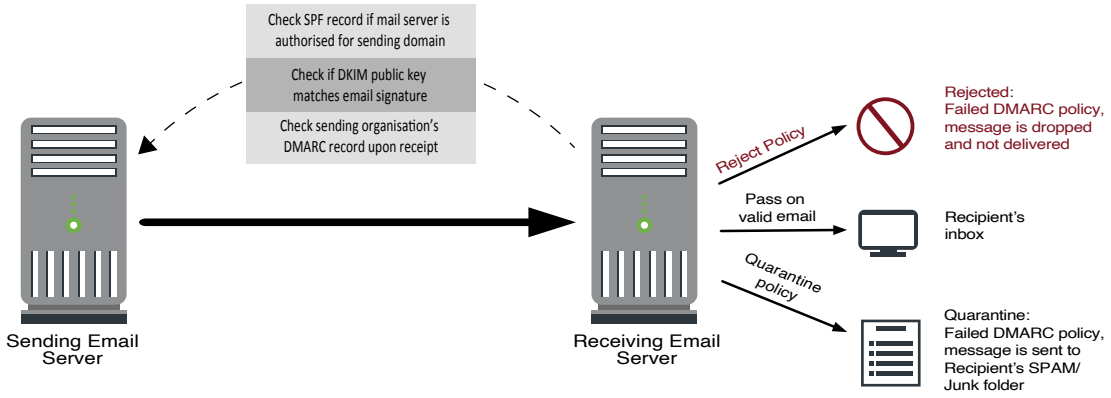

Figure: How the anti-spoofing solution work

Managed Anti-Spoofing

How can LGA's managed anti-spoofing solution help you?

LGA helps you to realise the full potential of existing technology through implementing an anti-spoofing solution based on current email authentication standards to protect your inbox. We help you to:

- Set up and configure SPF, DKIM and DMARC in your DNS server
- Block and quarantine suspicious emails from reaching your inbox
- Administer and mitigate spoofed emails and false positives
- Monitor your domains 24/7 for spoofing attacks
- Gain visibility into spoofing attacks through a personalised portal and DMARC report
- Optimise your anti-spoofing policies and interpret insights into spoofing activities

LGA managed anti-spoofing solution FAQ

1. We already have anti-spoofing in our current setup. Why do we need this?

   There are many methods to protect your mailboxes from cyberattacks such as Secure Email Gateway (SEG), Endpoint protection and DNS based protection (i.e. SPF, DKIM, DMARC).

   Secure Email Gateway helps you to filter out unwanted and malicious emails through the use of threat intelligence, encryption, and analysis on URLs and attachments.

   Endpoint protection, or more commonly known as anti-virus protection, helps to protect your computer from malware. For instance, without anti-virus, when someone accidentally opens or downloads something from a malicious email, the computer will be infected and confidential information may be accessed or corrupted.

   Although SEG and Endpoint protection are beneficial, it provides a different form of protection from LGA's anti-spoofing solution, which is **DNS based protection**. Our solution helps to prevent such malicious emails from reaching your inbox in the first place through analysing the legitimacy of an email by cross-checking against the records stored in the DNS server.

   In addition, we will help you to **configure the policies in your DNS** and **provide you with 24/7 support** to effectively protect your company's email from spoofing attacks. You are able to see the solution at work as you will have visibility into the attacks and with each mitigation, your DMARC compliance percentage will increase as well. Essentially, we will help you to optimise your DMARC compliance percentage to ensure well-rounded protection.

2. We only have less than 10 users in our company. Why do we need this?

   Research has shown **that hackers are increasingly targeting smaller businesses** and their attacks are getting more sophisticated. It just takes one person in the company to fall for such scams and result in serious business losses for the company. As a small company, such losses could cause a greater impact to the company's finances.

3. What is the difference between anti-spam and anti-spoofing?

   Spam is referred to as junk emails sent out in bulk to a mass recipient list. These emails are typically unsolicited, whereby the recipient did not consent for the message to be sent to them. It is a tactic typically used for commercial purposes, but it could also be used by spammers in attempt to gain access to your data through sending malicious links to spread malware. **Spoofing** on the other hand, deceives the recipient on the sender of the email and tricks them into exposing sensitive data. Although both are inbox-clogging nuisances, we can see that the motive behind each of them is very different.

Contact Us

LGA Telecom Pte Ltd
33 Ubi Avenue 3
#08-53 Vertex (Tower A)
Singapore 408868

Tel (65) 6892 2308
Email: sales@lgatelecom.net
Website: www.lgatelecom.net