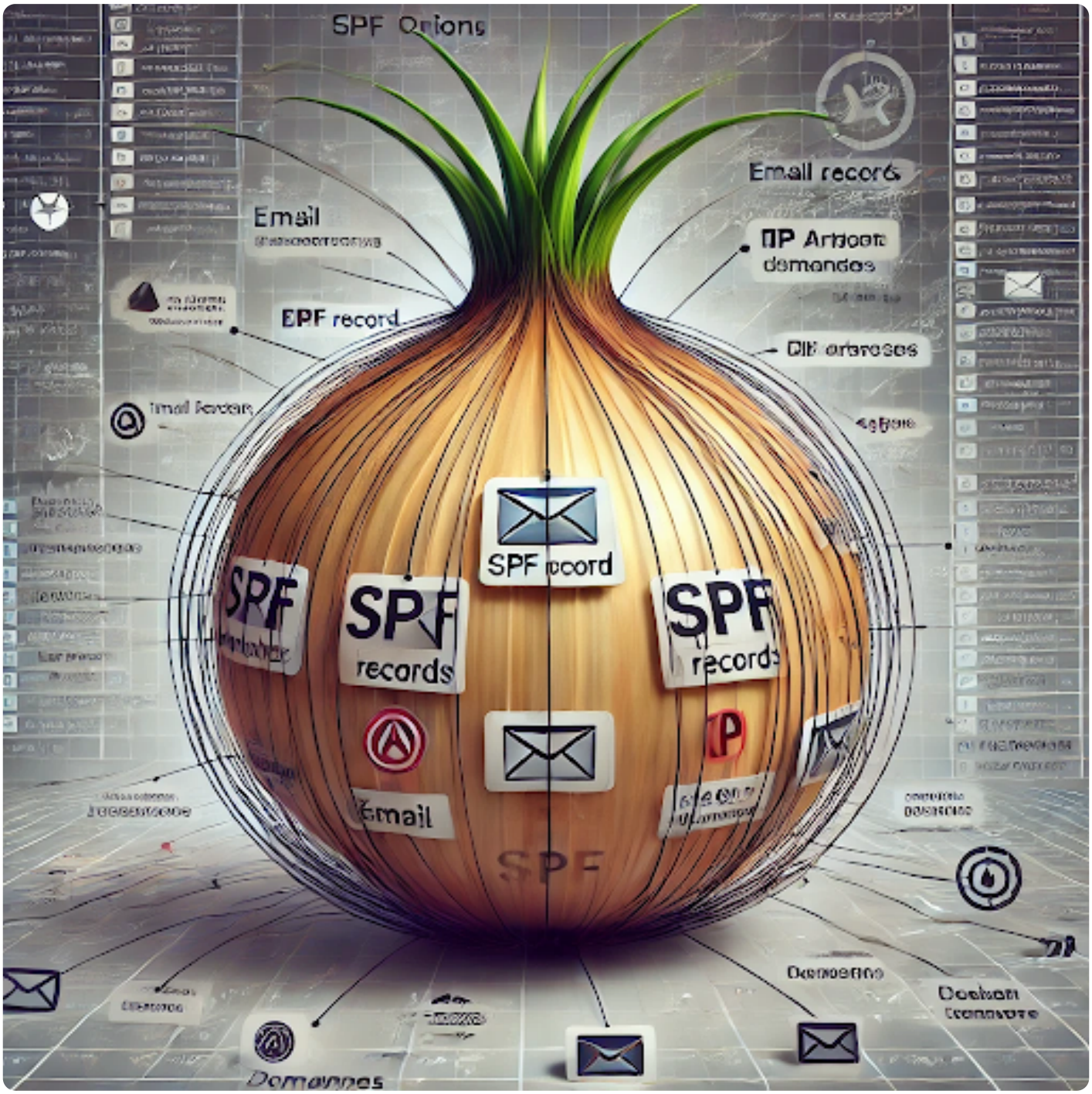
The SPF Onion: Enter the World of SPF Chaos

Posted on October 10, 2024


SPF Onions
Email
SPF record
Email records
SPF record
SPF
SPF
records
SPF
records
Email
SPF

Authors:
Ed Gibbs, Field CTO, WHOIS API Inc.
Jeff Vogelpohl

Introduction

It was late in the evening on September 25, 2024, when I received a suspicious email in my personal inbox. It was cleverly disguised as a message from an insurance company I currently do business with, but something felt off—the usual company icon didn't look quite right. Normally, I verify the sender by clicking on the icon to check the email address, but this time it wouldn't pop up. Sensing something was amiss, I decided to dig deeper.

After inspecting the message's transcript—you know, the long lines of SMTP data that almost require a PhD to decipher, yes those! Hidden among those lines was the sender's information and various security checks that had somehow passed inspection, allowing the message to slip through the many layers of protection that email providers typically use to keep spam and phishing attempts out of the inbox.

A quick check of the SPF, DKIM and DMARC - All passed.

Subject:	Review_Sign Document_Requires_Your Immediate Attention !
SPF:	PASS with IP 173.203.187.125 Learn more
DKIM:	'PASS' with domain dominionlending.ca Learn more
DMARC:	'PASS' Learn more

Long story short, the body of the email contained non-printable characters, Base64 encoding, and other common tricks that bad actors use to evade detection. I spoke with several email security experts: one from a leading security firm who offered some insight into how this email bypassed security checks, and another who deals with these kinds of attacks daily. Both pointed to a well-known but often overlooked issue: SPF linking. Jeff Vogelpohl described it as the "**SPF Onion**"—a complex web of linked IP addresses and domains that can quickly become unmanageable.

What Is a SPF Onion?

In the ever-evolving landscape of email security, the Sender Policy Framework (SPF) has long been a foundational tool. Designed to verify that an email claiming to come from a domain is sent by an authorized mail server, SPF helps prevent spoofing and phishing attacks. However, as organizations grow, their SPF records often evolve into something more complex—an intricate web of interlinked IP addresses and domains. This phenomenon, which we call the "SPF Onion," represents the layered, often unmanageable, structure of SPF records that can become both a security challenge and an operational nightmare.

The Layers of an SPF Onion

At its core, an SPF record is a simple text entry in a domain's DNS records. It typically includes mechanisms like `ip4`, `ip6`, and `include`, which specify the authorized IP addresses or domains that are allowed to send email on behalf of a domain. When properly managed, an SPF record is straightforward, containing only the necessary details for verification.

However, just like the many layers of an onion, SPF records can expand over time, becoming increasingly complex as more third-party services, email servers, and cloud providers are included. Each new layer, often added without much thought, can bring its own set of IP addresses and domains, leading to a tangled, multi-layered structure. As organizations outsource services—such as marketing, CRM, and customer support—their SPF records grow in depth and complexity. Each third-party service might have its own SPF record, which can be referenced

using the `include` directive. This creates what we call "SPF chaining," where one SPF record includes another, which might include yet another, and so on. Soon enough, the record becomes an SPF Onion.

How Deep Can the Layers Go?

Technically, the SPF standard (RFC 7208) places a strict limit on the number of DNS lookups during SPF validation, which is capped at 10. This limit includes all `include`, `a`, `mx`, `ptr`, `exists`, and `redirect` mechanisms that result in a DNS lookup. As you can imagine, if a record references multiple external services, each performing DNS lookups, it's easy to exceed this limit.

For example, a company's SPF record might begin with the usual `ip4` or `ip6` mechanisms to define its authorized mail servers. But then it adds an `include` for a third-party email marketing service, which might have its own set of SPF records. That service, in turn, includes yet another domain for its own infrastructure. This can lead to SPF chains that stretch far beyond the 10-lookup limit, with layers buried within layers, making it almost impossible to untangle.

These buried layers can become a rotten SPF Onion.

The Security and Performance Implications

At first glance, these growing layers may seem harmless—after all, as long as the SPF record passes validation, the email should be delivered, right? Unfortunately, the deeper and more convoluted an SPF record becomes, the more fragile it gets.

Firstly, exceeding the 10-lookup limit will cause SPF checks to fail, which results in a "permerror" (permanent error). This failure can lead to legitimate emails being rejected or marked as spam, especially when sent from services relying on a deeply nested SPF record.

Secondly, managing these multi-layered SPF records introduces significant security risks. An SPF Onion might include external domains that the organization has no control over. If one of those third-party domains is compromised, the attack surface widens, allowing bad actors to exploit the weak links in the chain. In essence, the more layers an SPF record has, the greater the chances of

exposure to threats outside the organization's direct oversight.

Most importantly, SPF management involves a persistent and proactive approach to protect a domain from unauthorized communication stemming from these so-called rotten SPF records that make up the SPF Onion.

The Management Nightmare

Beyond security risks, maintaining an SPF Onion becomes an operational headache. IT administrators must track which third-party services are included, ensure they stay updated, and check for any potential vulnerabilities. The challenge becomes even greater when these services change their infrastructure, deprecate IP addresses, or modify their SPF records. Suddenly, what should have been a simple update turns into peeling back layers of an ever-growing SPF Onion—each requiring more investigation and attention.

Moreover, every added `include` directive extends the SPF chain, which makes it difficult to troubleshoot problems when email delivery issues arise. It's often not clear which layer of the onion is causing the problem, leaving administrators to sift through logs and query DNS records to pinpoint the error.

Peeling Back the Layers: How to Manage an SPF Onion

Effectively managing an SPF Onion requires a proactive approach. Here are a few key strategies to keep SPF records lean and manageable:

1. Consolidate Services: Instead of relying on multiple third-party services, consider consolidating them under a single provider where possible. This reduces the need for multiple `include` directives and simplifies SPF management.

2. Monitor DNS Lookups: Regularly audit your SPF record to check the number of DNS lookups it triggers. If it's approaching the limit, find ways to streamline the record.

3. Use Subdomains: For complex organizations, splitting SPF records across subdomains may be a good strategy. By delegating different functions (e.g., marketing, CRM) to separate subdomains,

you can maintain more control over the number of lookups each record requires.

4. Employ DMARC and DKIM: While SPF is crucial, it's not the only email authentication tool available. Deploying DMARC (Domain-based Message Authentication, Reporting & Conformance) and DKIM (DomainKeys Identified Mail) alongside SPF can provide a more robust security posture without putting all the pressure on SPF validation alone.

Examples of SPF Onions

In this example, we'll take a domain name that we'll just say, maybe "***Not Suitable for Work***", and look at its SPF record: Try following that… we'll wait.

```
v=spf1 ip4:89.185.250.240/28 ip4:66.232.98.202 ip4:104.156.55.80/28 ip4:162.213.194.160/29 ip4:19
```

Message Header Example

In this example, which arrived just as this document was being reviewed, there's obvious signs this is a phishing attempt, but let's take a look at the headers below:

```
Received: from SJ2PR20MB6118.namprd20.prod.outlook.com (2603:10b6:a03:4f8::15)
 by SA1PR20MB4418.namprd20.prod.outlook.com with HTTPS; Fri, 27 Sep 2024
 15:36:18 +0000
Received: from BN9PR03CA0600.namprd03.prod.outlook.com (2603:10b6:408:10d::35)
 by SJ2PR20MB6118.namprd20.prod.outlook.com (2603:10b6:a03:4f8::15) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7982.25; Fri, 27 Sep
 2024 15:36:16 +0000
Received: from BL6PEPF00020E5F.namprd04.prod.outlook.com
 (2603:10b6:408:10d:cafe::8e) by BN9PR03CA0600.outlook.office365.com
 (2603:10b6:408:10d::35) with Microsoft SMTP Server (version=TLS1_2,
```

cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.8005.23 via Frontend
Transport; Fri, 27 Sep 2024 15:36:15 +0000
Authentication-Results: spf=pass (sender IP is 188.227.164.91)
smtp.mailfrom=24904564.opencart-service.ru; dkim=pass (signature was
verified) header.d=ogcge.opencart-service.ru;dmarc=pass action=none
header.from=ogcge.opencart-service.ru;compauth=pass reason=100
Received-SPF: Pass (protection.outlook.com: domain of
24904564.opencart-service.ru designates 188.227.164.91 as permitted sender)
receiver=protection.outlook.com; client-ip=188.227.164.91; helo=etic.yt; pr=C
Received: from etic.yt (188.227.164.91) by
BL6PEPF00020E5F.mail.protection.outlook.com (10.167.249.20) with Microsoft
SMTP Server id 15.20.8005.15 via Frontend Transport; Fri, 27 Sep 2024
15:36:15 +0000
X-IncomingTopHeaderMarker:
OriginalChecksum:5C75AC633D6DA757061532193EB4D587C12CFDE940952FDD7EB27181D4300
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=selector1; d=ogcge.opencart-service.ru;
h=From:Sender:Subject:Date:To:Cc:Content-Type; i=office@ogcge.opencart-service.ru;
bh=jKvW+CEE8o2gJOlqzpJhhtSURgo=;
b=nY512wg6SuLWmuuKJF2VHOxR+G65+aOH4QcOKSmHU5AxBazPe0Vax9vC6CxEv2AAmWZSyV
sgC7DHq3iiURBDDaMN0=
DomainKey-Signature: a=rsa-sha1; c=nofws; q=dns; s=selector1; d=ogcge.opencart-service.ru;
b=LZVX+ay5Y+sj19ShHwOxRs7VlbdkZX2dr6CgkuTqSnMwniDrwgjpulOXmp4JNb9iBQOpoo9/vQPU
lCNX83QPbkts5/b52nRpYF4bTsmaaw7cmvzofQ2dvRQEi8phEt5eW8wXwSwm0CWTsOoiWmIV4R
MG9wmOrYI5O+GJjOMdY=;
From: "[Tractor Supply]",NOP_idl1Jl/NOP<office@ogcge.opencart-service.ru>
Sender: "ogcge--"<office@ogcge.opencart-service.ru>
Subject: '-=?UTF-8?b?X19GaW5hbF9OMHRpY2VfQ29taW5nX0Ywcl9hX1lldF9Dcm9zc3JvYWRzX0J
Date: Fri, 27 Sep 2024 10:36:54 -0400 (EDT)
To: <redacted>@outlook.com
Cc: <redacted>@outlook.com
Content-Disposition: inline
Content-Type: text/html; charset=utf-8

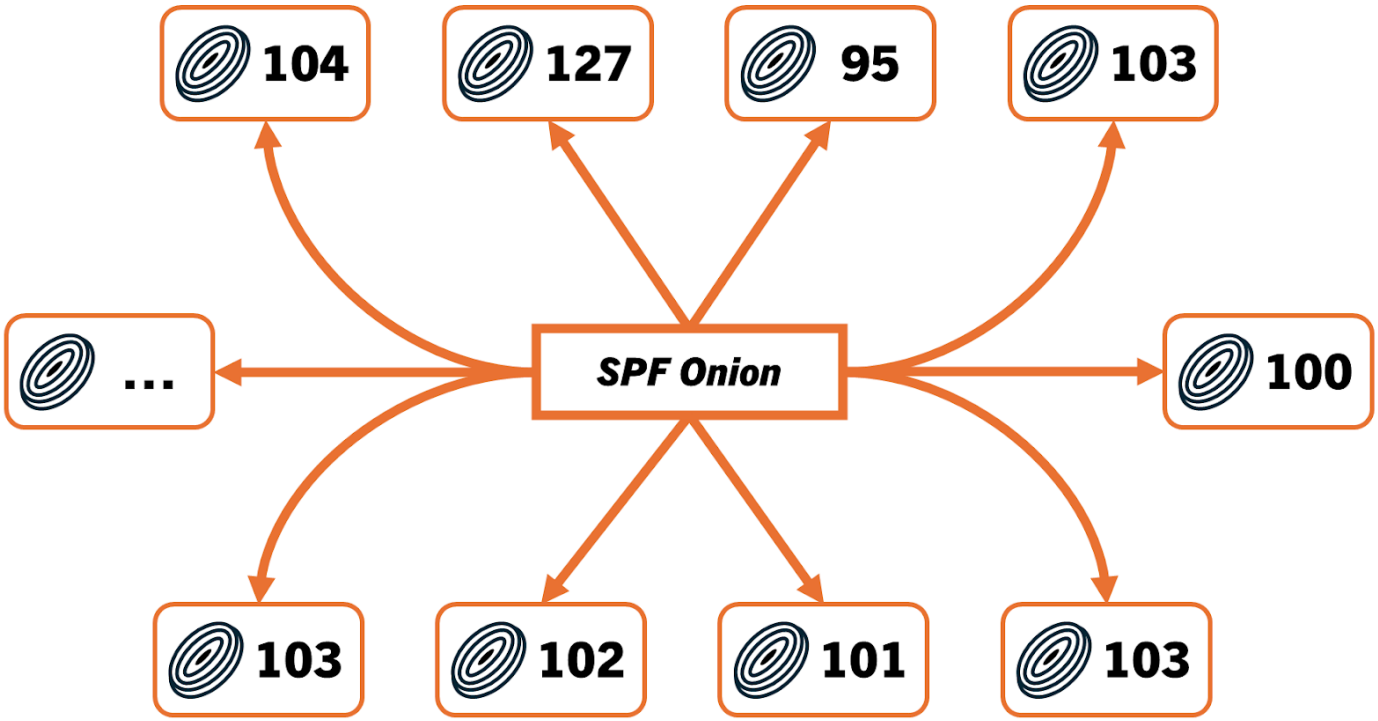
X-IncomingHeaderCount: 10

Let’s begin looking at the onion layers:

ogcge.opencart-service.ru
v=spf1 include:instanttranslates.dynu.net include:informationshout.dynu.net -all

instanttranslates.dynu.net
v=spf1 include:justifyintegrated.accesscam.org include:handlerhedriver.accesscam.org include:occupa

The following chart summarizes the initial layers and their detected SPF entries—obviously obfuscating with intended confusion:



dkim:ogcge.opencart-service.ru:selector1 Show

Dkim Public Record:

```
v=spf1 include:instanttranslates.dynu.net include:informationshout.dynu.net -all
```

Dkim Signature:

```
v=1; a=rsa-sha1; c=relaxed/relaxed; s=selector1; d=ogcge.opencart-service.ru; h=From:Sender:Subject:Date:T
```

spf:24904564.opencart-service.ru:188.227.164.91 Hide

```
v=spf1 include:instanttranslates.dynu.net include:informationshout.dynu.net -all
```

Prefix	Type	Value	PrefixDesc	Description
Prefix	Typev	Valuespf1	PrefixDesc	DescriptionThe SPF record version
Prefix+	Typeinclude	Valueinstanttranslates.dynu.net	PrefixDescPass	DescriptionThe specified domain is searched for an 'allow'.
Prefix+	Typeinclude	Valueinformationshout.dynu.net	PrefixDescPass	DescriptionThe specified domain is searched for an 'allow'.
Prefix-	Typeall	Value	PrefixDescFail	DescriptionAlways matches. It goes at the end of your record.

	Test	Result
Status ✗	NameSPF Included Lookups	ResponseToo many included lookups (26) Too many DNS Lookups? Solve this problem with SPF Flattening
Status ✓	NameSPF Record Published	ResponseSPF Record found
Status ✓	NameSPF Record Deprecated	ResponseNo deprecated records found
Status ✓	NameSPF Multiple Records	ResponseLess than two records found
Status ✓	NameSPF Alignment	ResponseDomain found in SPF
Status ✓	NameSPF Contains characters after ALL	ResponseNo items after 'ALL'.
Status ✓	NameSPF Syntax Check	ResponseThe record is valid
Status ✓	NameSPF Type PTR Check	ResponseNo type PTR found
Status ✓	NameSPF Void Lookups	ResponseNumber of void lookups is OK
Status ✓	NameSPF MX Resource Records	ResponseNumber of MX Resource Records is OK
Status ✓	NameSPF Record Null Value	ResponseNo Null DNS Lookups found
Status ✓	NameSPF Authentication	ResponseSPF Passed for IP

It’s easy to get lost in the numerous layers of the SPF Onion, so at what point should we trust another domain’s SPF record and its layers?

Insights from SPF Record Analysis: A Year in Review

Our recent analysis of SPF records over the past 365 days, using data from our passive DNS TXT record database, has revealed striking insights into the state of email security. We analyzed a total of **736,363,363** DNS TXT records, of which a significant **464,975,836** were identified as SPF records. These numbers underscore the widespread adoption of SPF as a vital tool in email authentication and spam prevention.

However, the complexity of these SPF records tells a deeper story. Our research found that **1,808,746** SPF records had more than 10 entries (combo of IP addresses and domain names), indicating an overly complex configuration. These "SPF Onions," as we call them, represent a growing concern in email security, as the more layers an SPF record has, the harder it becomes to manage, monitor, and troubleshoot. Each layer adds potential vulnerabilities, increases DNS lookup times, and may introduce errors that prevent proper email validation.

On the other hand, the majority of the SPF records—**463,167,090**—had 10 or fewer entries, suggesting that most domains maintain a manageable level of SPF complexity. Still, this doesn't necessarily mean they are free from security risks, as even simpler SPF records can be misconfigured or insufficient to fully protect against phishing and spoofing attacks.

The longest SPF record we encountered had **166 entries**, an outlier that demonstrates the extreme potential for SPF record bloat. Such records are not only difficult to maintain but also likely to exceed the standard DNS lookup limits, leading to potential delivery failures or security vulnerabilities.

These findings highlight the importance of continuous monitoring and management of SPF records to maintain email security and performance. The data underscores the need for organizations to regularly audit and streamline their SPF configurations to ensure they are not only compliant but also optimized for security.

What are the Recommendations for SPF Records

According to the ***Sender Policy Framework*** (SPF) specification (RFC 7208), the limit is primarily around the number of DNS lookups rather than the number of individual entries (IP addresses or mechanisms) in an SPF record. The SPF protocol allows up to 10 DNS-based mechanisms or modifiers that perform DNS lookups (e.g., `a`, `mx`, `ptr`, `include`, `exists`, `redirect`), excluding mechanisms that do not result in DNS lookups, such as `ip4` or `ip6`.

Key limits:

- DNS Lookup Limit: SPF implementations must limit the number of DNS lookups to 10 to prevent SPF-based denial-of-service attacks. This includes lookups performed by `a`, `mx`, `ptr`, `include`, `exists`, and `redirect`.
- Record Size: The entire SPF record should not exceed 512 bytes (some older mail servers may have stricter limits), though the DNS protocol allows up to **65535 bytes for a TXT record.
- Number of Mechanisms/Entries: There's no strict limit on the number of mechanisms like `ip4` or `ip6` because they don't require DNS lookups. However, SPF should remain simple to avoid errors and stay within the recommended size constraints.

What happens if there are more than 10 DNS lookups?

If an SPF check results in more than 10 DNS lookups, the lookup fails with a "permerror" (permanent error), meaning the SPF check will not succeed, and the mail may be rejected or flagged as potentially fraudulent, depending on the recipient's mail server policies.

Leveraging WhoisXML API's Suite of Tools to Combat SPF Onion Complexity

In the ongoing battle to manage the complexities of email security and SPFrecords, having access to reliable data sources and tools is critical. As we delve deeper into our research on the "SPF Onion"—a phenomenon where SPF records become convoluted due to excessive layering of

domains, IP addresses, and third-party services—WHOISXMLAPI.com emerges as a key player in providing essential resources for uncovering, managing, and securing SPF records.

WHOISXMLAPI.com offers a powerful suite of APIs that can provide valuable insights into DNS records, ownership information, IP geolocation, and historical DNS data. Below, we explore four key products from WHOISXMLAPI.com that can significantly enhance our ability to analyze and mitigate the challenges posed by SPF record complexity.

1. DNS Lookup API: Reveal the DNS TXT Record for SPF Analysis

The first step in understanding an SPF Onion is to retrieve the DNS TXT record for a given domain. WHOISXMLAPI.com's DNS Lookup API is an indispensable tool for this task. This API allows us to query any domain for its DNS records, including the all-important TXT records that store SPF information.

By using the DNS Lookup API, we can programmatically obtain the SPF records of domains, which is the foundational layer of our SPF Onion analysis. These records can reveal which IP addresses and domains are authorized to send emails on behalf of a given domain, helping us to map out the chain of included domains and identify when SPF records have become overly complex. This API is critical for real-time analysis as it ensures we have the most up-to-date SPF information available.

2. WHOIS API: Identify the Owners of SPF-Linked Domains

When dealing with SPF Onions, especially those involving multiple third-party services, it's essential to know who controls the domains being referenced in the SPF record. This is where the WHOIS API from WHOISXMLAPI.com becomes invaluable. The WHOIS API provides detailed ownership information for domains, including the registrant's contact details, registration dates, and administrative information.

With this data, we can identify the organizations behind the domains referenced in the SPF records, making it easier to evaluate whether these domains are trustworthy or if they introduce unnecessary risks into the email authentication process. Additionally, understanding the ownership

of domains can help us pinpoint which third-party services are contributing to SPF bloat and work with them to simplify or optimize their records. By leveraging the WHOIS API, we gain visibility into the entities responsible for each layer of the SPF Onion.

3. IP Geolocation API: Trace the Geographic Footprint of SPF Records

Understanding the geographic distribution of the IP addresses referenced in SPF records is another key aspect of our analysis. The IP Geolocation API offered by WHOISXMLAPI.com enables us to obtain detailed information about each IP address, including the physical location, ISP (Internet Service Provider), country, and even the time zone associated with the IP.

This information is vital in several ways. First, it allows us to verify whether the IP addresses included in an SPF record align with the expected regions of legitimate email senders. If an SPF record includes IP addresses from unexpected regions or suspicious ISPs, it could be a sign of misconfiguration or potential abuse. By mapping out the geographic footprint of SPF records, we can detect inconsistencies, identify potential vulnerabilities, and ensure that the IP addresses are in line with the organization's legitimate email-sending infrastructure.

4. DNS Premium Data Feed: Conduct Extensive Research with Passive DNS

One of the most powerful resources available from WHOISXMLAPI.com is its DNS Premium Data Feed, a passive DNS database that provides historical DNS data from across the Internet. This tool is a game-changer for conducting in-depth research on TXT records globally, including SPF records.

The DNS Premium Data Feed allows us to look beyond a single domain's SPF record and examine patterns across many domains. We can query the passive DNS database to identify other domains that reference the same third-party services in their SPF records, helping us understand how widespread certain SPF configurations are and identify common trends or vulnerabilities. This level of insight is critical for uncovering emerging SPF Onion patterns that may not be immediately apparent from a single domain's DNS records.

Additionally, passive DNS data allows us to conduct historical analysis on SPF records. We can

track changes over time to see how a domain's SPF record has evolved, which domains have been added or removed, and whether any security risks have been introduced along the way. This data is particularly useful for investigating potential security breaches or understanding how complex SPF records have become over time.

How These Tools Can Be Applied to Our SPF Onion Project

By leveraging WHOISXMLAPI.com's suite of tools, we can take a comprehensive approach to analyzing and managing SPF records as part of our SPF Onion research. Here's how each API can contribute:

- DNS Lookup API: Provides real-time access to the SPF records of any domain, allowing us to map out the interconnected layers of IP addresses and domains.
- WHOIS API: Identifies the ownership of domains referenced in SPF records, helping us trace the entities responsible for SPF configurations and evaluate their trustworthiness.
- IP Geolocation API: Gives us insights into the geographic locations and ISPs associated with the IP addresses in SPF records, helping detect anomalies and potential misconfigurations.
- DNS Premium Data Feed: Offers historical and passive DNS data, enabling us to conduct large-scale research on SPF records across the Internet and detect patterns of SPF bloat and abuse.

Together, these tools provide us with a powerful set of resources to manage and mitigate the risks associated with SPF Onions. By understanding the full scope of SPF complexity, we can develop strategies to streamline SPF records, improve email security, and reduce the risks of spoofing and phishing attacks.

Conclusion

You should check your SPF record to ensure that it doesn't exceed this DNS lookup limit, even if it

has more than 10 mechanisms or IP addresses.

- It’s okay to have more than 10 IP addresses or mechanisms like `ip4` and `ip6` in your SPF record.

- The critical limit is on DNS lookups**, which must be 10 or fewer.

Please contact us at sales@whoisxmlapi.com and be sure to visit our website for more information and a free account to access our APIs.