SPF and DKIM

EXPERT ADVICE ON GETTING STARTED, BEST PRACTICES, AND PIT FALLS TO AVOID

This is the first episode in a Zimbra webinar series that aims to demystify modern email authentication and encryption security for practical, everyday use.

A Brief Introduction

Randy Leiker

President and CEO of Skyway Networks

- 26 Years Of IT industry experience
- 23 Of Those Years at Skyway Networks
- Long history with Zimbra, dating back to Zimbra 5.0

Skyway Networks℠

Overview Of Today's Webinar

- SPF
- SPF Questions & Answers
- DKIM
- DKIM Questions & Answers
- Wrap Up & Key Takeaways

This webinar is being recorded and will be posted on the Zimbra YouTube Channel at https://www.youtube.com/c/zimbra

Email Security Webinar Series

- Upcoming Topics
  - DMARC & BIMI: supercharges SPF & DKIM by providing enforcement of your email policies, a powerful feedback mechanism, and a branding feature. This is a highly recommended follow-up to this webinar.
  - MTA-STS & TLS-RPT: advertise to email senders that you prefer strong encryption, provide a means for senders to verify your email servers, and gain important insights into any delivery failures.
  - DNSSEC: prevent your DNS infrastructure from being the weakest link in the security chain and defends from a variety of spoofing and man-in-the-middle attacks.
  - TLS & DANE: an overview of how email encryption works, and how to overcome inherent weaknesses with the Certificate Authorities that issue SSL certificates by using certificate pinning.

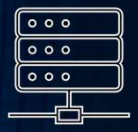
What Is SPF and Why Do You Need It?

- Early email approaches in the 1970s on ARPANET gave way to the introduction of SMTP (Simple Mail Transfer Protocol) in 1981.
- The initial SMTP standard included no thought given for security.
- Despite multiple revisions since 1981, SMTP remains inherently weak & trivial to abuse.
- SPF: Sender Policy Framework, first proposed in 2004.
  - Provides a domain owner with the means to define authorized senders by IP address.

How To Setup SPF By Example

How To Setup SPF By Example

Jill's Company Domain Name: zimbra.tech



Zimbra Email Server
mail.zimbra.tech

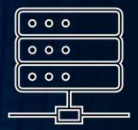
Web Server
https://zimbra.tech
https://blog.zimbra.tech

Newsletter Mailing Service
emailthem.corp

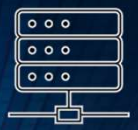
Photo by Mateus Campos Felipe

How To Setup SPF By Example

Jill's Company Domain Name: zimbra.tech



Zimbra Email Server
mail.zimbra.tech
64.200.180.2



Web Server
https://zimbra.tech
64.200.180.3
https://blog.zimbra.tech
64.200.180.4

Newsletter Mailing Service
emailthem.corp
209.136.72.2
2607:DA00:0401::7334

Photo by Mateus Campos Felipe

How To Setup SPF By Example

Jill's Company Domain Name: zimbra.tech

Zimbra Email Server
mail.zimbra.tech
64.200.180.2

Web Server
https://zimbra.tech
64.200.180.3
https://blog.zimbra.tech
64.200.180.4

Newsletter Mailing Service
emailthem.corp
209.136.72.2
2607:DA00:0401::7334

Jill's SPF Record (DNS TXT record)

Host name: zimbra.tech

Content:
v=spf1

An SPF record must always start with v=spf1 .

Photo by Mateus Campos Felipe

How To Setup SPF By Example

Jill's Company Domain Name: zimbra.tech

Zimbra Email Server
mail.zimbra.tech
64.200.180.2

Web Server
https://zimbra.tech
64.200.180.3
https://blog.zimbra.tech
64.200.180.4

Newsletter Mailing Service
emailthem.corp
209.136.72.2
2607:DA00:0401::7334

Jill's SPF Record (DNS TXT record)

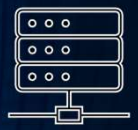
Host name: zimbra.tech

Content:
v=spf1 ip4:64.200.180.2 ip4:64.200.180.3 ip4:64.200.180.4 ip4:209.136.72.2 ip6:2607:DA00:0401::7334

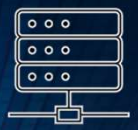
Photo by Mateus Campos Felipe

How To Setup SPF By Example

Jill's Company Domain Name: zimbra.tech



Zimbra Email Server
mail.zimbra.tech
64.200.180.2



Web Server
https://zimbra.tech
64.200.180.3
https://blog.zimbra.tech
64.200.180.4

Newsletter Mailing Service
emailthem.corp
209.136.72.2
2607:DA00:0401::7334

Photo by Mateus Campos Felipe

Jill's SPF Record (DNS TXT record)

Host name: zimbra.tech

Content:
v=spf1 ip4:64.200.180.2 ip4:64.200.180.3 ip4:64.200.180.4 ip4:209.136.72.2 ip6:2607:DA00:0401::7334 ~all

The ~ means "soft fail" and "all" refers to all IP addresses on the Internet. This SPF policy says all IP addresses that send email for zimbra.tech, not otherwise listed in Jill's SPF record, should soft fail as spam.

An SPF record must always end with the "all" keyword.

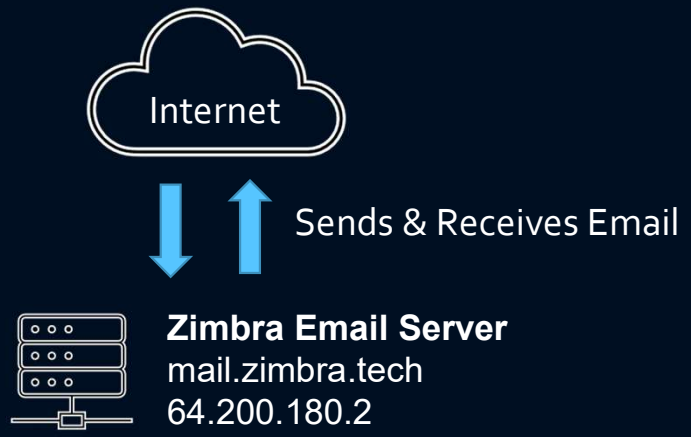
How To Setup SPF By Example

Photo by Mateus Campos Felipe

Jill's Existing DNS Records

Type: MX (Mail eXchanger)
Host name: zimbra.tech
Content: mail.zimbra.tech

Type: A (Address)
Host name: mail.zimbra.tech
Content: 64.200.180.2



How To Setup SPF By Example

Photo by Mateus Campos Felipe

Jill's Company Domain Name: zimbra.tech

Zimbra Email Server
mail.zimbra.tech
64.200.180.2

Web Server
https://zimbra.tech
64.200.180.3
https://blog.zimbra.tech
64.200.180.4

Newsletter Mailing Service
emailthem.corp
209.136.72.2
2607:DA00:0401::7334

Jill's SPF Record (DNS TXT record)

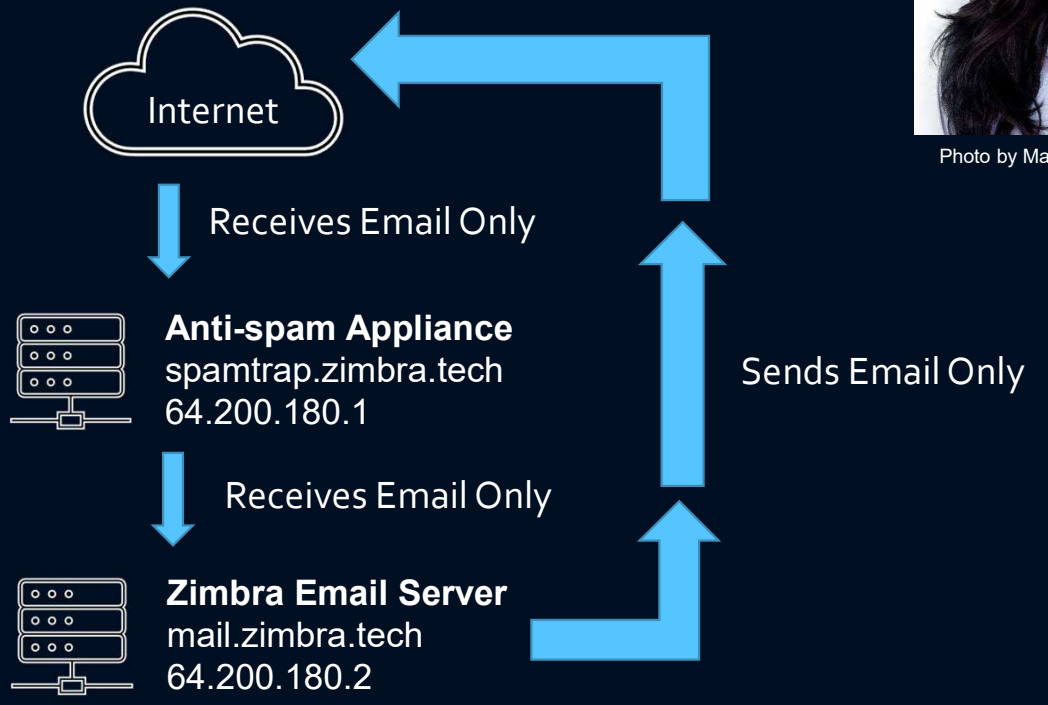
Host name: zimbra.tech

Content:
v=spf1 ~~ip4:64.200.180.2~~ ip4:64.200.180.3 ip4:64.200.180.4 ip4:209.136.72.2 ip6:2607:DA00:0401::7334 ~all

v=spf1 mx ip4:64.200.180.3 ip4:64.200.180.4 ip4:209.136.72.2 ip6:2607:DA00:0401::7334 ~all

How To Setup SPF By Example

Photo by Mateus Campos Felipe



How To Setup SPF By Example

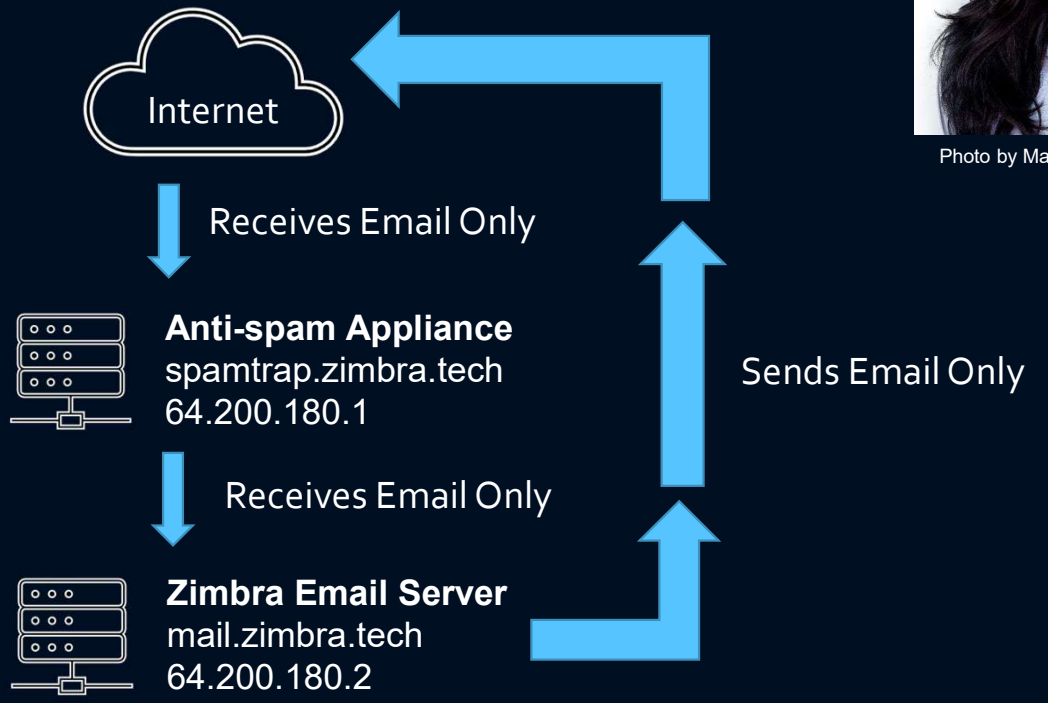
Photo by Mateus Campos Felipe

Jill's Existing DNS Records

Type: MX (Mail eXchanger)
Host name: zimbra.tech
Content: spamtrap.zimbra.tech

Type: A (Address)
Host name: spamtrap.zimbra.tech
Content: 64.200.180.1

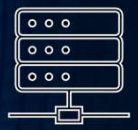
Type: A (Address)
Host name: mail.zimbra.tech
Content: 64.200.180.2



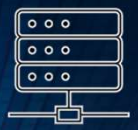
v=spf1 ~~mx~~ ip4:64.200.180.2 ip4:64.200.180.3 ip4:64.200.180.4 ip4:209.136.72.2 ip6:2607:DA00:0401::7334 ~all

How To Setup SPF By Example

Jill's Company Domain Name: zimbra.tech



Zimbra Email Server
mail.zimbra.tech
64.200.180.2



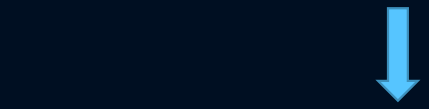
Web Server
https://zimbra.tech
64.200.180.3
https://blog.zimbra.tech
64.200.180.4

Newsletter Mailing Service
emailthem.corp
209.136.72.2
2607:DA00:0401::7334

Jill's SPF Record (DNS TXT record)

Host name: zimbra.tech

Content:
v=spf1 ~~ip4:64.200.180.2~~ ip4:64.200.180.3 ip4:64.200.180.4 ip4:209.136.72.2 ip6:2607:DA00:0401::7334 ~all



v=spf1 mx a ip4:64.200.180.4 ip4:209.136.72.2 ip6:2607:DA00:0401::7334 ~all

Photo by Mateus Campos Felipe

How To Setup SPF By Example

Photo by Mateus Campos Felipe

Jill's Company Domain Name: zimbra.tech

Zimbra Email Server
mail.zimbra.tech
64.200.180.2

Web Server
https://zimbra.tech
64.200.180.3
https://blog.zimbra.tech
64.200.180.4

Newsletter Mailing Service
emailthem.corp
209.136.72.2
2607:DA00:0401::7334

Jill's SPF Record (DNS TXT record)

Host name: zimbra.tech

Content:
v=spf1 ~~ip4:64.200.180.2~~ ~~ip4:64.200.180.3~~ ~~ip4:64.200.180.4~~
ip4:209.136.72.2 ip6:2607:DA00:0401::7334 ~all

v=spf1 mx a a:blog.zimbra.tech ip4:209.136.72.2
ip6:2607:DA00:0401::7334 ~all

How To Setup SPF By Example

Jill's Company Domain Name: zimbra.tech

Zimbra Email Server
mail.zimbra.tech
64.200.180.2

Web Server
https://zimbra.tech
64.200.180.3
https://blog.zimbra.tech
64.200.180.4

Newsletter Mailing Service
emailthem.corp
209.136.72.2
2607:DA00:0401::7334

Jill's SPF Record (DNS TXT record)

Host name: zimbra.tech

Content:
v=spf1 ~~ip4:64.200.180.2~~ ~~ip4:64.200.180.3~~ ~~ip4:64.200.180.4~~ ~~ip4:209.136.72.2~~ ~~ip6:2607:DA00:0401::7334~~ ~all

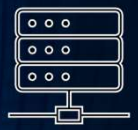
v=spf1 mx a a:blog.zimbra.tech include:_spf.emailthem.corp ~all

_spf.emailthem.corp SPF record:
v=spf1 ip4:209.136.72.2 ip4:209.136.72.3
ip6:2001:db4::8a2e:570:7334 ~all

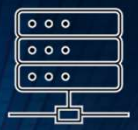
Photo by Mateus Campos Felipe

How To Setup SPF By Example

Jill's Company Domain Name: zimbra.tech



Zimbra Email Server
mail.zimbra.tech
64.200.180.2



Web Server
https://zimbra.tech
64.200.180.3
https://blog.zimbra.tech
64.200.180.4

Newsletter Mailing Service
emailthem.corp
209.136.72.2
2607:DA00:0401::7334

Jill's SPF Record (DNS TXT record)

Host name: zimbra.tech

Content:
v=spf1 mx a a:blog.zimbra.tech include:_spf.emailthem.corp -all

The - means "fail" and "all" refers to all IP addresses on the Internet. This SPF policy says all IP addresses, not otherwise listed in Jill's SPF record, should (hard) fail.

Photo by Mateus Campos Felipe

SPF Best Practices

- **Best Practice # 1:** You must have only one SPF record per domain name (zimbra.tech) or per sub-domain (research.zimbra.tech).
  - If your email address is you@zimbra.tech, publish one SPF (DNS TXT) record:
    - Host name: zimbra.tech
    - Content: v=spf1 ip4:209.136.72.1 -all
  - Or, if your email address ends in you@research.zimbra.tech, publish one SPF (DNS TXT) record:
    - Host name: research.zimbra.tech
    - Content: v=spf1 ip4:209.136.72.1 -all
- Publishing multiple SPF records for a given domain or sub-domain will likely be ignored by your email recipients and treated like you have no SPF record published at all.

SPF Best Practices

- **Best Practice # 2:** Before publishing an SPF record, compile a complete list of all public IP addresses that send email for your domain name. Never list private IP addresses (example: 192.168.0.1) in your SPF record.

SPF Best Practices

- **Best Practice # 2:** Before publishing an SPF record, compile a complete list of all public IP addresses that send email for your domain name. Never list private IP addresses (example: 192.168.0.1) in your SPF record.
  - For help with this task, use the reporting feature in DMARC. If your email addresses end with @zimbra.tech, create a DNS TXT record like this:
    - **Host name:** _dmarc.zimbra.tech
    - **Content:** v=DMARC1; p=none; rua=mailto:you@zimbra.tech;
    - Substitute zimbra.tech with your domain name and the you@zimbra.tech portion with your email address.
    - Ensure that the email address uses the same domain name as is used in the host name for your DMARC record. In this example, this means that you@zimbra.tech will work, but you@anotherdomain.com will not.
  - Within about 24 hours, you should begin receiving reports from recipient mail servers of email received from your domain name showing the IP addresses that were used to send email. Free tools like 7-Zip (https://www.7-zip.org) for opening the compressed files, and Notepad++ (https://notepad-plus-plus.org) can be helpful in reading these reports.

SPF Best Practices

- **Best Practice # 3:** When publishing your SPF record, if you are uncertain if you have a complete list of all IP addresses that send email for your domain name, end your SPF record initially with the ~all (soft fail) keyword rather than the stricter -all (fail) keyword.
- Your end goal is to use the -all (fail) keyword, so only use the ~all (soft fail) for a limited time while testing your SPF record.
- Never use the +all (pass) or ?all (neutral) keywords in your SPF record. This is like having no SPF record published, since both function similar to including all IP addresses on the Internet in your SPF record.

SPF Best Practices

- **Best Practice # 4:** If using one or more “include” keywords in your SPF record
  - v=spf1 mx a include:_spf.emailthem.corp -all
- And the DNS TXT record for _spf.emailthem.corp is:
  - v=spf1 ip4:209.136.72.2 ~all
- Then the ~all keyword in the included SPF record will usually be ignored, and your -all keyword has the final say.

SPF Best Practices

- **Best Practice # 5:** Protect your unused domain names with SPF policies too! For domains or sub-domains that will never send email, create SPF records for each that look like:
  - v=spf1 -all
- This prevents the bad guys from hijacking these non-email sending domains and damaging your online reputation.

SPF Best Practices

- **Best Practice # 6:** Avoid listing large blocks of IP addresses in your SPF record, such as every IP address in your network.
  - Example: v=spf1 ip4:209.136.72.0/24
- This means any IP address in the range of 209.136.72.1 - 209.136.72.254 may send email. While this may seem convenient or safe to avoid missing an email sender's IP address, it also gives unauthorized senders many IPs to choose from for hiding illegitimate email sent using your domain name, effectively creating security holes in your SPF policy.

SPF Best Practices

- **Best Practice # 7:** Beware of the SPF lookup & length limits.
- When using keywords in your SPF record like: “a”, “mx”, or “include”, each of these results in one or more DNS lookups that a recipient of your email must do. SPF allows no more than 10 lookups. Beyond this limit, the rest of your SPF policy is ignored.
  - Example # 1 with 3 lookups total:
    - Host name: zimbra.tech
    - Content: v=spf1 include:_spf.emailthem.corp a mx ip4:209.136.72.2 –all

_spf.emailthem.corp SPF record:
v=spf1 ip4:209.136.72.2 ip4:209.136.72.3 ip6:2001:db4::8a2e:570:7334 ~all

- “include” = 1 DNS lookup for _spf.emailthem.corp
- “a” = 1 DNS lookup for zimbra.tech
- “mx” = 1 DNS lookup for a single MX record for mail.zimbra.tech
- ip4 = no lookups
- ip6 = no lookups
- -all = no lookups

SPF Best Practices

- **Best Practice # 7:** Beware of the SPF lookup & length limits.
  - Example # 2 with 11 lookups total:
    - v=spf1 include:_spf.emailthem.corp a mx ip4:209.136.72.2 –all

_spf.emailthem.corp SPF record:
v=spf1 a mx a:blog.emailthem.corp
include:_spf.anothervendor.com ~all

- **“include”** = 2 DNS lookups for _spf.emailthem.corp and _spf.anothervendor.com
- **Nested “include”:** 5 more DNS lookups within _spf.anothervendor.com
- **“a”** = 2 DNS lookup for zimbra.tech and blog.emailthem.corp
- **“mx”** = 2 DNS lookup for mail.zimbra.tech and emailthem.corp
- **ip4** = no lookups
- **-all** = no lookups

SPF Best Practices

- **Best Practice # 7:** Beware of the SPF lookup & length limits.
- Your entire SPF record (v=spf1 …. -all) is limited to no more than 255 characters. If you reach this limit, use the “include” keyword to split your SPF record into multiple parts like:
  - v=spf1 include:_spf1.zimbra.tech include:_spf2.zimbra.tech -all

SPF Questions

Up Next: DKIM

What Is DKIM and Why Do You Need It?

- In the early 2000s, Yahoo and Cisco were working on independent approaches to tackle more security shortcomings in SMTP.
- In 2004, Yahoo and Cisco's efforts were combined into a new standard called DomainKeys Identified Mail, or DKIM for short.
- Before DKIM, there was no practical means to authenticate:
  - If a message originated from a sender's email server.
  - The integrity of an email to determine if it had been tampered with in transit.

How To Setup DKIM By Example

How To Setup DKIM By Example

Jill's Company Domain Name: zimbra.tech

Photo by Mateus Campos Felipe

Zimbra Email Server
mail.zimbra.tech

Web Server
https://zimbra.tech
https://blog.zimbra.tech

Newsletter Mailing Service
emailthem.corp

Two Steps For Setting Up DKIM In Zimbra

Step 1.) Generate a pair of encryption keys.

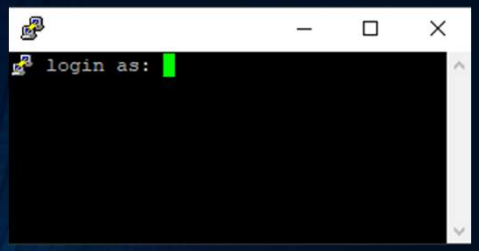
Step 2.) Publish the public encryption key as a new DNS TXT record.

How To Setup DKIM By Example

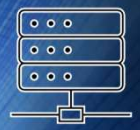
Photo by Mateus Campos Felipe

Setting Up Zimbra For DKIM

Step 1.) Generate a pair of encryption keys.



PuTTY
(SSH Client)



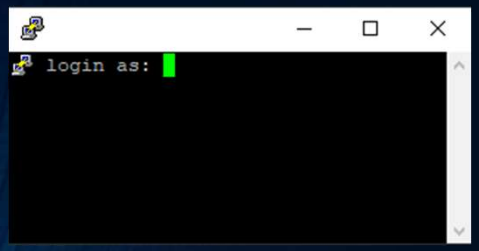
Zimbra Email Server
mail.zimbra.tech

How To Setup DKIM By Example

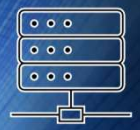
Photo by Mateus Campos Felipe

Setting Up Zimbra For DKIM

Step 1.) Generate a pair of encryption keys.



PuTTY
(SSH Client)



Zimbra Email Server
mail.zimbra.tech

Jill Runs These Commands:

- Ubuntu: sudo su - zimbra
- Or for Red Hat: su - zimbra

- /opt/zimbra/libexec/zmdkimkeyutil -a -d zimbra.tech

  - -a refers to adding a new domain for use with DKIM
  - -d refers to the domain name being setup for DKIM

How To Setup DKIM By Example

Photo by Mateus Campos Felipe

Setting Up Zimbra For DKIM

Step 1.) Generate a pair of encryption keys.

- /opt/zimbra/libexec/zmdkimkeyutil -a -d zimbra.tech

  - Generates a matching private & public keypair.
  - Enables DKIM for all zimbra.tech email sent.

On-Screen Output From Zimbra:

DKIM Data added to LDAP for domain zimbra.tech with selector 0E9F184A-9577-11E1-AD0E-2A2FBBAC6BCB
Public key to enter into DNS:
0E9F184A-9577-11E1-AD0E-2A2FBBAC6BCB._domainkey IN TXT "v=DKIM1;=rsa; “
“p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBg”
“DY5CBg15nZ2vYnRmrNub6Jn6ghQ2DXQbQgOJ/E5IGziUYEuE2OnxkBm1h3jived21uHjpNy0naOZjLj0xLyyjclVy”
“chrhSbsGAhe8HLXUsdXyfRvNTq8NWLsUnMEsoomtJCJ6LYWYU1whOQ9oKZVAwWHSovAWZpByqNMZmFg7QIDAQAB" ;
----- DKIM 0E9F184A-9577-11E1-AD0E-2A2FBBAC6BCB for zimbra.tech

How To Setup DKIM By Example

Photo by Mateus Campos Felipe

Setting Up Zimbra For DKIM

Step 2.) Publish the public encryption key as a new DNS TXT record.

On-Screen Output From Zimbra:

DKIM Data added to LDAP for domain zimbra.tech with selector 0E9F184A-9577-11E1-AD0E-2A2FBBAC6BCB
Public key to enter into DNS:
0E9F184A-9577-11E1-AD0E-2A2FBBAC6BCB._domainkey IN TXT "v=DKIM1;=rsa; “
“p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBg” “chrhSbsGAhe8HLXUsdXyfRvNTq8NWLsUnMEAQAB" ; ----- DKIM 0E9F184A-9577-11E1-AD0E-2A2FBBAC6BCB for zimbra.tech

Jill’s DKIM Record (DNS TXT record)

Host name: 0E9F184A-9577-11E1-AD0E-2A2FBBAC6BCB._domainkey.zimbra.tech

Content:

How To Setup DKIM By Example

Photo by Mateus Campos Felipe

Setting Up Zimbra For DKIM

Step 2.) Publish the public encryption key as a new DNS TXT record.

On-Screen Output From Zimbra:

DKIM Data added to LDAP for domain zimbra.tech with selector 0E9F184A-9577-11E1-AD0E-2A2FBBAC6BCB
Public key to enter into DNS:
0E9F184A-9577-11E1-AD0E-2A2FBBAC6BCB._domainkey IN TXT **"v=DKIM1;=rsa; "**
"p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBg" "chrhSbsGAhe8HLXUsdXyfRvNTq8NWLsUnMEAQAB" ; ----- DKIM
0E9F184A-9577-11E1-AD0E-2A2FBBAC6BCB for zimbra.tech

Jill's DKIM Record (DNS TXT record)

Host name: 0E9F184A-9577-11E1-AD0E-2A2FBBAC6BCB._domainkey.zimbra.tech

Content:
v=DKIM1;=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgchrhSbsGAhe8HLXUsdXyfRvNTq8NWLsUnMEAQAB

How To Setup DKIM By Example

Setting Up Zimbra For DKIM - Example Using a BIND DNS Server

Photo by Mateus Campos Felipe

Output From Zimbra:

DKIM Data added to LDAP for domain zimbra.tech with selector 0E9F184A-9577-11E1-AD0E-2A2FBBAC6BCB
Public key to enter into DNS:
0E9F184A-9577-11E1-AD0E-2A2FBBAC6BCB._domainkey IN TXT "v=DKIM1;=rsa; "
"p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBg" "chrhSbsGAhe8HLXUsdXyfRvNTq8NWLsUnMEAQAB" ; ----- DKIM 0E9F184A-9577-11E1-AD0E-2A2FBBAC6BCB for zimbra.tech

Jill's BIND DNS TXT Record:

0E9F184A-9577-11E1-AD0E-2A2FBBAC6BCB._domainkey IN TXT ("v=DKIM1;=rsa; "
"p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBg" "chrhSbsGAhe8HLXUsdXyfRvNTq8NWLsUnMEAQAB")

How To Setup DKIM By Example

Jill's Company Domain Name: zimbra.tech

Photo by Mateus Campos Felipe

Zimbra Email Server
mail.zimbra.tech

Web Server
https://zimbra.tech
https://blog.zimbra.tech

Newsletter Mailing Service
emailthem.corp

Next Steps:

Step 1.) Setup DKIM for Jill's Newsletter Mailing Service.

Step 2.) Setup DKIM for Jill's Web Server.

How To Setup DKIM By Example

Setup DKIM for Jill's Newsletter Mailing Service

Photo by Mateus Campos Felipe

DKIM Information From Jill's Vendor

DKIM Selector: client8382

Public Key:

v=DKIM1;=rsa;
p=VNRfoD8k0yY18cDfWKvGkK6UXA2v3Q1w7Jqy7pr
JKsecyHKNBQDblzYLsH3aM2fZ0Ft6IegZlxYrOuIqEGH
JVDurhWkO5RwBYSyMk0ihyAYjLkua10VtVJ2H2nBOS
MRVQB58O3COs9ZzFwmvWIcDHIBK6Q1figxlHIthRv
GlvJDemkeM6XYOXTmkyldT1pEPf6y5m2VqW0ca3H
4VhbyUCF3XQZpeQYXD4r65sHuFzncCbPJ27e

How To Setup DKIM By Example

Setup DKIM for Jill's Newsletter Mailing Service

Photo by Mateus Campos Felipe

DKIM Information From Jill's Vendor

DKIM Selector: client8382

Public Key:
v=DKIM1;=rsa;
p=VNRfoD8k0yY18cDfWKvGkK6UXA2v3Q1w7Jqy7pr
JKsecyHKNBQDblzYLsH3aM2fZ0Ft6IegZlxYrOuIqEGH
JVDurhWkO5RwBYSyMk0ihyAYjLkua10VtVJ2H2nBOS
MRVQB58O3COs9ZzFwmvWIcDHIBK6Q1figxlHIthRv
GlvJDemkeM6XYOXTmkyldT1pEPf6y5m2VqW0ca3H
4VhbyUCF3XQZpeQYXD4r65sHuFzncCbPJ27e

Jill's DKIM Record (DNS TXT record)

Host name: client8382._domainkey.zimbra.tech

Content:

How To Setup DKIM By Example

Setup DKIM for Jill's Newsletter Mailing Service

Photo by Mateus Campos Felipe

DKIM Information From Jill's Vendor

DKIM Selector: client8382

Public Key:

v=DKIM1;=rsa;
p=VNRfoD8k0yY18cDfWKvGkK6UXA2v3Q1w7Jqy7prJKsecyHKNBQDblzYLsH3aM2fZ0Ft6IegZlxYrOuIqEGHJVDurhWkO5RwBYSyMk0ihyAYjLkua10VtVJ2H2nBOSMRVQB58O3COs9ZzFwmvWIcDHIBK6Q1figxlHIthRvGlvJDemkeM6XYOXTmkyldT1pEPf6y5m2VqW0ca3H4VhbyUCF3XQZpeQYXD4r65sHuFzncCbPJ27e

Jill's DKIM Record (DNS TXT record)

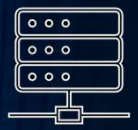
Host name: client8382._domainkey.zimbra.tech

Content:

v=DKIM1;=rsa;
p=VNRfoD8k0yY18cDfWKvGkK6UXA2v3Q1w7Jqy7prJKsecyHKNBQDblzYLsH3aM2fZ0Ft6IegZlxYrOuIqEGHJVDurhWkO5RwBYSyMk0ihyAYjLkua10VtVJ2H2nBOSMRVQB58O3COs9ZzFwmvWIcDHIBK6Q1figxlHIthRvGlvJDemkeM6XYOXTmkyldT1pEPf6y5m2VqW0ca3H4VhbyUCF3XQZpeQYXD4r65sHuFzncCbPJ27e

How To Setup DKIM By Example

Jill's Company Domain Name: zimbra.tech



Zimbra Email Server
mail.zimbra.tech

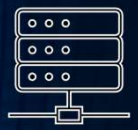
Web Server
https://zimbra.tech
https://blog.zimbra.tech

Newsletter Mailing Service
emailthem.corp

Photo by Mateus Campos Felipe

How To Setup DKIM By Example

Jill's Company Domain Name: zimbra.tech



Zimbra Email Server
mail.zimbra.tech

Web Server
https://zimbra.tech
https://blog.zimbra.tech

Newsletter Mailing Service
emailthem.corp

1. Create a new Zimbra account: website@zimbra.tech
2. Web site outbound email re-configuration:
   - SMTP server: mail.zimbra.tech
   - User name: website@zimbra.tech
   - Password: **********

Photo by Mateus Campos Felipe

How Does DKIM Protect Your Email

Sending An Email

1. When you send an email from your computer or mobile device, no DKIM protection has been applied yet.

2. When your email reaches your mail server (Zimbra), this is where the DKIM signing process happens, and occurs in these steps:

    1. Using your DKIM private key, a digital signature, known as a hash, is created of the body of your email message. A hash might look like this: 0C8cOB5PJQH4+KgkQXQ57TgXK20RF3

    2. The Zimbra server will select certain email header fields from your email like the Date, From, and To fields, combine them with the body of your message, then again use your DKIM private key to create another hash like this: gSkFx6xYEF2D4Tu5k1iIufZUw70BPRZzyUo+C7w7WeQK

    3. Both of these hashes are inserted into your email, then your email is delivered as normal to the recipient's mail server.

How Does DKIM Protect Your Email

Receiving An Email

1. When the recipient's mail server receives your email, they will find a DKIM signature embedded that looks like this:

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=zimbra.tech;
s=example; t=1646684079;
bh=QG03mIvFcKQYqGc=;
h=Date:From:To:Message-ID:MIME-Version;
b=gSkFx6xYEF2D4Tu5k1iIufZUw70BPRZzyUo+C7w7
WeQK4Vr/w+gWzuhXRwgU1brwd ldj+SspR11LPg==
```

2. This provides the recipient's mail server with the needed information to begin validating your email using DKIM.

The DKIM Signature Explained

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=zimbra.tech;
s=example; t=1646684079;
bh=QG03mIvFcKQYqGc=;
h=Date:From:To:Message-ID:MIME-Version;
b=gSkFx6xYEF2D4Tu5k1iIufZUw70BPRZzyUo+C7w7
WeQK4Vr/w+gWzuhXRwgU1brwd ldj+SspR11LPg==

v=1	The version of DKIM used to sign this message.
a=rsa-sha256	The encryption & hashing algorithms used to sign this message.
c=relaxed,relaxed	The canonicalization method used; defines if sub-domains are allowed.
d=zimbra.tech	The domain name that sent this email message.
s=example	The name of the DKIM selector; used to lookup the public DKIM key in a DNS TXT record.
t=16466840789	A timestamp of when the email was DKIM signed.
bh=QG03m….	The hash of the email body only.
h=Date:From:To….	The email headers that the sender included in their hash signature.
b=gSkFx6xYEF….	The hash of both the email headers and the email body.

The DKIM Signature Explained

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=zimbra.tech;
s=example; t=1646684079;
bh=QG03mIvFcKQYqGc=;
h=Date:From:To:Message-ID:MIME-Version;
b=gSkFx6xYEF2D4Tu5k1iIufZUw70BPRZzyUo+C7w7
WeQK4Vr/w+gWzuhXRwgU1brwd ldj+SspR11LPg==

DNS TXT Record
Host name: example._domainkey.zimbra.tech
Contains the sender's public DKIM key.

v=1	The version of DKIM used to sign this message.
a=rsa-sha256	The encryption & hashing algorithms used to sign this message.
c=relaxed,relaxed	The canonicalization method used; defines if sub-domains are allowed.
d=zimbra.tech	The domain name that sent this email message.
s=example	The name of the DKIM selector; used to lookup the public DKIM key in a DNS TXT record.
t=16466840789	A timestamp of when the email was DKIM signed.
bh=QG03m….	The hash of the email body only.
h=Date:From:To….	The email headers that the sender included in their hash signature.
b=gSkFx6xYEF….	The hash of both the email headers and the email body.

DKIM Best Practices

- **Best Practice # 1:** Use DKIM on every server that sends email for your domain name. This extra effort will pay off significantly when setting up DMARC, a topic to be discussed in the next episode in this webinar series.
- For servers that do not support DKIM, configure those servers to relay outbound email through another DKIM capable server, like your Zimbra server.
- If you configure your non-DKIM capable servers to relay outbound email through another DKIM capable server, then your non-DKIM capable servers should be removed from your SPF record, since they are no longer directly sending email to the Internet.

DKIM Best Practices

- **Best Practice # 2:** Consider creating a recurring scheduled process to change your DKIM keys periodically, known as key rotation.

- Key rotation involves:
  - Creating a new DKIM keypair.
  - Adding the new DKIM public key to a DNS TXT record.
  - Deleting the old DKIM keypair from your email & DNS server.

- When doing a key rotation, aim for creating a new DKIM selector. Should you need to troubleshoot why a message failed to validate with DKIM, it makes it easy to tell if an email was using your old or new DKIM keypair, based on the selector name that is in the email's DKIM signature.

- Create a DKIM key rotation schedule that makes sense for your organization's risk tolerance, not too aggressive, but not too relaxed either.

DKIM Best Practices

- **Best Practice # 3:** Keep your DKIM private key secret! Encrypt backups of your DKIM keypair and store the backups in a secure location.

DKIM Best Practices

- **Best Practice # 4:** Never share DKIM keypairs or selector names between multiple servers.
- If any servers sharing the same DKIM keypair or selector are compromised for any reason, then you would be forced to do an immediate key rotation on all affected servers simultaneously since the private key is no longer secret.
- Using unique DKIM keypairs and selector names for each server makes troubleshooting easier.

DKIM Questions

Up Next: Key Take Aways

Key Take Aways

- Deploy SPF and DKIM for every server that sends email for your domain names or sub-domains.
- Deploy SPF (v=spf1 -all) records to protect your non-email sending domains and sub-domains from abuse.
- Check your SPF and DKIM DNS records carefully for errors and use online testing tools (links available on the next slide) to ensure they are correct. This will confirm your SPF and DKIM records are usable by your recipients' mail servers.
- Watch out for the SPF limit of 10 DNS lookups. This occurs more frequently than you might expect, and can creep up unexpectedly, especially when using the "include" keyword.
- Copy & paste DKIM public keys into your DNS TXT records with care. Omitting or altering just one character in a public key will break your DKIM record and it can be difficult to identify the cause when troubleshooting.
- Avoid complacency and create a scheduled process that periodically does key rotation for your DKIM keypairs. The reasoning for this is the same basis of why SSL certificates for web sites have expiration dates.

Thank You For Attending Today's Webinar!

- Helpful Links
  - **For testing SPF records:**
    - https://mxtoolbox.com/spf.aspx
    - https://www.dmarcanalyzer.com/spf/checker/
    - https://duckduckgo.com/?q=spf+test
  - **For testing DKIM records:**
    - https://mxtoolbox.com/dkim.aspx
    - https://dmarcly.com/tools/dkim-record-checker
    - https://duckduckgo.com/?q=dkim+test

Speaker's Contact Information

Randy Leiker
Skyway Networks
randy@skywaynetworks.com
https://skywaynetworks.com