DMARC

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

This is the second episode in a Zimbra webinar series that aims to demystify modern email authentication and email encryption 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

Overview Of Today's Webinar

- DMARC
  - What Is DMARC
  - Brief Review of SPF & DKIM
  - How To Setup DMARC
  - How Does DMARC Protect Your Domain
  - Zimbra Settings For DMARC Alignment
  - Understanding DMARC Reporting
  - Best Practices
- DMARC 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

- Earlier Topics
  - SPF & DKIM: these form the foundation on which modern email authentication operates and are the first key steps to protecting your outbound email and domain name’s reputation. Recording available at https://www.youtube.com/c/zimbra
- Upcoming Topics
  - 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 defend yourself 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 DMARC and Why Do You Need It?

- SPF & DKIM: evolutionary leap forward in email sender authentication, but more was needed.

- DMARC: Domain-based Message Authentication, Reporting, and Conformance.

- DMARC builds upon both SPF & DKIM by:
  - Adding a feedback loop for senders
  - Enables domain owners to provide explicit direction of what should happen when an email fails SPF and DKIM validation
  - Enforces anti-spoofing for the visible From address that email recipients see

SPF & DKIM Revisited

SPF

- Sender Policy Framework enables a domain / sub-domain owner to list the public IP addresses that may send email for the domain / sub-domain by using a DNS TXT record.

- Using the “-all” (fail) keyword at the end of your SPF record is a best practice, especially when using SPF in combination with DMARC. Using anything else, including “~all” (soft fail) weakens both your SPF & DMARC policies, creating an opening for an attacker to bypass.

SPF & DKIM Revisited

DKIM

- DomainKeys Identified Mail enables a sender to create two digital signatures (hashes): one hash of the body of an email, and a second hash of the body of the email + select email header fields.

- Regularly do DKIM keypair rotations that involve:
  - 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 in 1 week.

Deprecated Email Security Standards

- SenderID Records
  - Modern Successor: SPF
  - How To Locate:
    - These records will have a host name like: example.com
    - The DNS TXT record will contain keywords like: “spf2.0”

- DomainKey Policy Records
  - Modern Successor: DKIM
  - How To Locate:
    - These records will have a host name like: _domainkey.example.com
    - Not to be confused with modern DKIM records that use host names like: selector._domainkey.example.com
    - The DNS TXT record will contain keywords like: “o=-” or “o=~”

- If you have either SenderID or DomainKey policy records, consider deleting them to make future email delivery troubleshooting easier & avoid unexpected email delivery outcomes.

How To Setup DMARC By Example

How To Setup DMARC By Example

Chris' Company Domain Name: zimbra.tech

Photo by Jacinto Diego

How To Setup DMARC By Example

Chris' Company Domain Name: zimbra.tech

DMARC Record (DNS TXT record)

Host name: _dmarc.zimbra.tech

Content:

Photo by Jacinto Diego

How To Setup DMARC By Example

Chris' Company Domain Name: zimbra.tech

DMARC Record (DNS TXT record)

Host name: _dmarc.zimbra.tech

Content:
v=DMARC1;

Photo by Jacinto Diego

How To Setup DMARC By Example

Photo by Jacinto Diego

Chris' Company Domain Name: zimbra.tech

DMARC Record (DNS TXT record)

Host name: _dmarc.zimbra.tech

Content:
v=DMARC1; **p=none;**

Available Options

p=none : no DMARC policy is enforced. Solely intended for testing / monitoring purposes.
p=quarantine : the policy requires email that fails DMARC to be delivered to a recipient's spam / junk folder.
p=reject : the policy requires email that fails DMARC to be deleted and not delivered to the recipient.

How To Setup DMARC By Example

Photo by Jacinto Diego

Chris’ Company Domain Name: zimbra.tech

DMARC Record (DNS TXT record)

Host name: _dmarc.zimbra.tech

Content:
v=DMARC1; p=none; **rua=mailto:dmarc@zimbra.tech;**

Available Options

rua : reporting URI for aggregate reports

- Accepts one or more email addresses, but usually only 1-2 email addresses will be honored by recipient mail servers. Multiple addresses, separated by commas, can be used: rua=mailto:dmarc@zimbra.tech,mailto:chris@zimbra.tech;

How To Setup DMARC By Example

Chris' Company Domain Name: zimbra.tech

DMARC Record (DNS TXT record)

Host name: _dmarc.zimbra.tech

Content:
v=DMARC1; p=none; **rua=mailto:reports@example.com;**

Required Additional DNS TXT record:

Host name: zimbra.tech._report._dmarc.example.com

Content:
v=DMARC1;

Photo by Jacinto Diego

How To Setup DMARC By Example

Photo by Jacinto Diego

Chris' Company Domain Name: zimbra.tech

DMARC Record (DNS TXT record)

Host name: _dmarc.zimbra.tech

Content:
v=DMARC1; p=none; rua=mailto:dmarc@zimbra.tech; **ruf=mailto:dmarc@zimbra.tech;**

Available Options

ruf : reporting URI for forensic reports

- Accepts one or more email addresses, but usually only 1-2 email addresses will be honored by recipient mail servers. Multiple addresses, separated by commas, can be used: ruf=mailto:dmarc@zimbra.tech,mailto:chris@zimbra.tech;
- This keyword is often ignored by most mail servers due to privacy laws.

How To Setup DMARC By Example

Photo by Jacinto Diego

Chris' Company Domain Name: zimbra.tech

DMARC Record (DNS TXT record)

Host name: _dmarc.zimbra.tech

Content:
v=DMARC1; **p=quarantine;** rua=mailto:dmarc@zimbra.tech; ruf=mailto:dmarc@zimbra.tech; **sp=none;**

Sub-Domain Policy Options

sp=none : no DMARC policy is enforced. Solely intended for testing / monitoring purposes.
sp=quarantine : the policy requires email that fails DMARC to be delivered to a recipient's spam / junk folder.
sp=reject : the policy requires email that fails DMARC to be deleted and not delivered to the recipient.

How To Setup DMARC By Example

Photo by Jacinto Diego

Chris' Company Domain Name: zimbra.tech

DMARC Record (DNS TXT record)

Host name: _dmarc.zimbra.tech

Content:
v=DMARC1; **p=reject;** rua=mailto:dmarc@zimbra.tech; ruf=mailto:dmarc@zimbra.tech; **sp=reject;**

Host name: _dmarc.support.zimbra.tech

Content:
v=DMARC1; **p=none; sp=reject;**

For an app sending email with the sub-domain support.zimbra.tech that has no SPF or DKIM support available. Prevents email being accepted from spoofed sub-domains like: spammer@kc.support.zimbra.tech

How To Setup DMARC By Example

Photo by Jacinto Diego

Chris' Company Domain Name: zimbra.tech

DMARC Record (DNS TXT record)

Host name: _dmarc.zimbra.tech

Content:
v=DMARC1; p=none; rua=mailto:dmarc@zimbra.tech; ruf=mailto:dmarc@zimbra.tech; sp=none; **fo=1;**

Failure Reporting Options

fo=0 : requests DMARC reports when SPF & DKIM fail, and spoofing of an email From field is found.
fo=1 : requests DMARC reports when SPF fails, DKIM fails, or spoofing of an email From field is found.
fo=d : requests DMARC reports when only DKIM fails.
fo=s : requests DMARC reports when only SPF fails.

How Does DMARC Protect Your Domain

Sending An Email

1. You send an email from your computer or mobile device.

2. When your email reaches your mail server (Zimbra), your email is digitally signed by DKIM, and a DKIM signature is added to your message as an email header.

3. Your mail server then connects to the recipient’s mail server, and hands off your email for delivery.

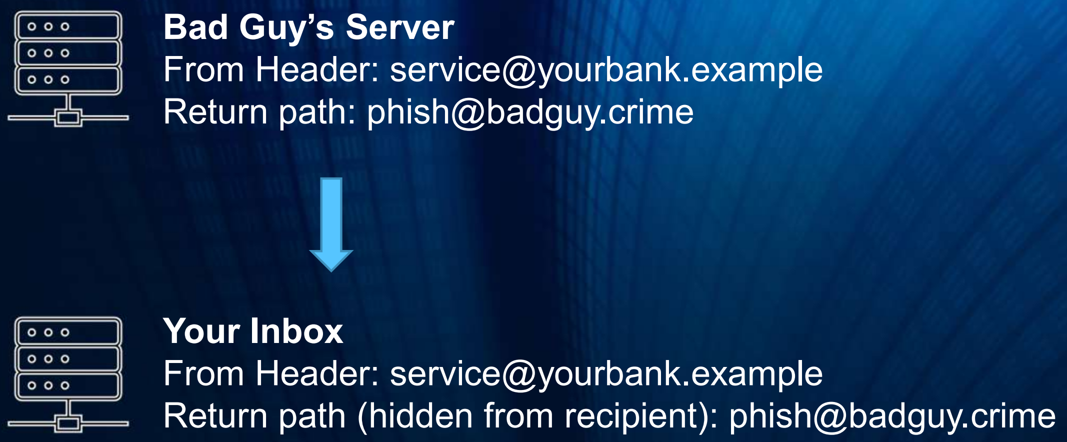
How Does DMARC Protect Your Domain

Receiving An Email

The recipient's mail server will perform these steps:

1. Check for the sender's SPF (DNS TXT) record, and if found, test it.
2. Check for a DKIM signature included in the email received, and if found, test it.
3. Check for the sender's DMARC (DNS TXT) record, and if found, perform DMARC alignment tests.
4. If the email passes SPF **or** DKIM, **and** passes DMARC alignment, deliver the email to the recipient.
5. If the email fails SPF **and** DKIM, **or** fails DMARC alignment, take the action provided in the sender's DMARC policy (p= or sp= keywords).

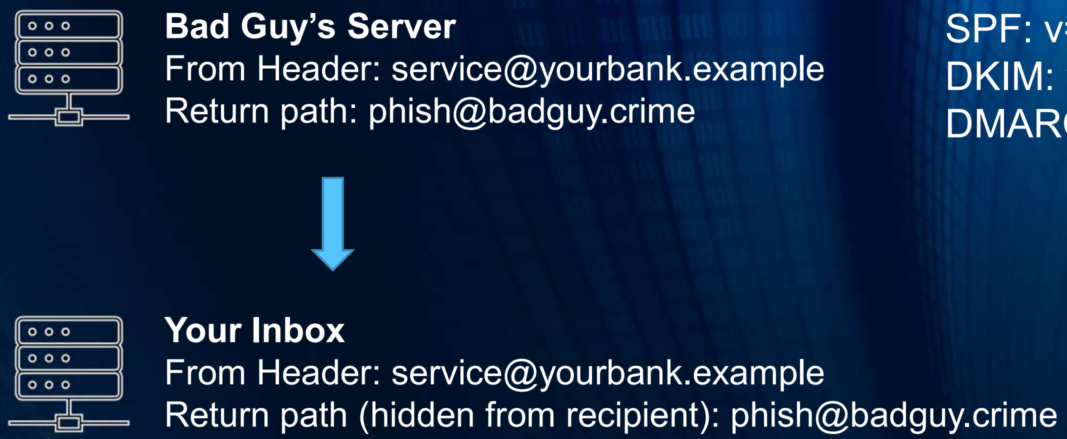
DMARC Identifier Alignment



Bad Guy's Server
From Header: service@yourbank.example
Return path: phish@badguy.crime

Your Inbox
From Header: service@yourbank.example
Return path (hidden from recipient): phish@badguy.crime

DMARC Identifier Alignment



Bad Guy's Server
From Header: service@yourbank.example
Return path: phish@badguy.crime

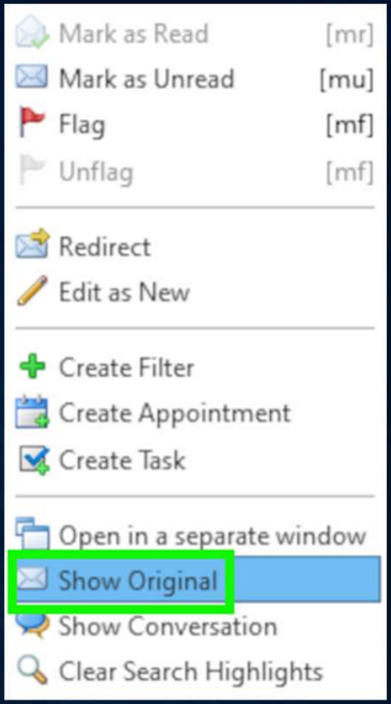
Your Inbox
From Header: service@yourbank.example
Return path (hidden from recipient): phish@badguy.crime

SPF: v=spf1 +all
DKIM: v=DKIM1; k=rsa; p=wdlei23kd…
DMARC: v=DMARC1; p=none;

DMARC Identifier Alignment

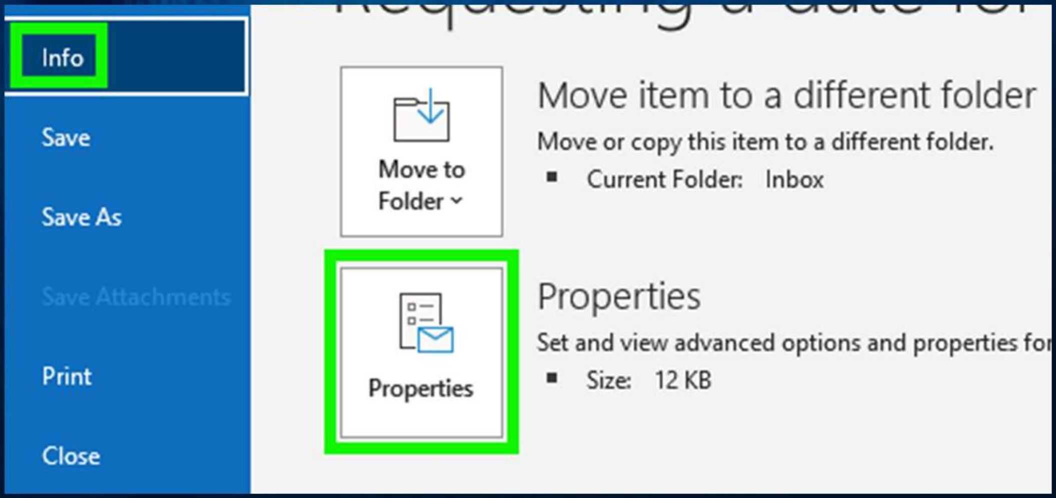
Zimbra Web Client

1. Right click on an email
2. Click on Show Original



Outlook

1. Double click on an email to open in a new window.
2. Click on the File tab, then click on Info.
3. Click on the Properties button.



Move item to a different folder

Move or copy this item to a different folder.

- Current Folder: Inbox

Properties

Set and view advanced options and properties fo

- Size: 12 KB

DMARC Identifier Alignment

Email Headers Sample

```
Return-Path: <chris@zimbra.tech>

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
          d=zimbra.tech; s=myselector; t=1649086243;
          bh=fNtVAJvf3QLrt3x9…
          h=Date:From:To:Message-ID:MIME-Version;
          b=dzL5+UhkQRwbYP+…

Date: Mon, 4 Apr 2022 10:30:40 -0500 (CDT)
From: "Chris Smith" <chris@zimbra.tech>
To: Randy Leiker <randy@skywaynetworks.com>
```

DMARC Record (DNS TXT record)

Host name: _dmarc.zimbra.tech

Content:
v=DMARC1; p=quarantine; sp=quarantine;

DMARC Identifier Alignment

Email Headers Sample

```
Return-Path: <chris@mail.zimbra.tech>

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=zimbra.tech; s=myselector; t=1649086243;
        bh=fNtVAJvf3QLrt3x9…
        h=Date:From:To:Message-ID:MIME-Version;
        b=dzL5+UhkQRwbYP+…

Date: Mon, 4 Apr 2022 10:30:40 -0500 (CDT)
From: "Chris Smith" <chris@zimbra.tech>
To: Randy Leiker <randy@skywaynetworks.com>
```

DMARC Record (DNS TXT record)

Host name: _dmarc.zimbra.tech

Content:
v=DMARC1; p=quarantine; sp=quarantine;

DMARC Identifier Alignment

Email Headers Sample

```
Return-Path: <chris@mail.zimbra.tech>

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=zimbra.tech; s=myselector; t=1649086243;
        bh=fNtVAJvf3QLrt3x9…
        h=Date:From:To:Message-ID:MIME-Version;
        b=dzL5+UhkQRwbYP+…

Date: Mon, 4 Apr 2022 10:30:40 -0500 (CDT)
From: "Chris Smith" <chris@zimbra.tech>
To: Randy Leiker <randy@skywaynetworks.com>
```

DMARC Record (DNS TXT record)

Host name: _dmarc.zimbra.tech

Content:
v=DMARC1; p=quarantine; sp=quarantine;
aspf=s;

DMARC Identifier Alignment

SMTP Sample From zimbra.tech mail server:

```
EHLO mail.zimbra.tech
MAIL FROM:<>
RCPT TO:<randy@skywaynetworks.com>
```

Email Headers Sample

```
Return-Path: <>

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=zimbra.tech; s=myselector; t=1649086243;
        bh=fNtVAJvf3QLrt3x9…
        h=Date:From:To:Message-ID:MIME-Version;
        b=dzL5+UhkQRwbYP+…

Date: Mon, 4 Apr 2022 10:30:40 -0500 (CDT)
From: "Chris Smith" <chris@zimbra.tech>
To: Randy Leiker <randy@skywaynetworks.com>
```

DMARC Record (DNS TXT record)

Host name: _dmarc.zimbra.tech

Content:
v=DMARC1; p=quarantine; sp=quarantine;

DMARC Identifier Alignment

Email Headers Sample

```
Return-Path: <chris@mail.zimbra.tech>

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
          d=zimbra.tech; s=myselector; t=1649086243;
          bh=fNtVAJvf3QLrt3x9…
          h=Date:From:To:Message-ID:MIME-Version;
          b=dzL5+UhkQRwbYP+…

Date: Mon, 4 Apr 2022 10:30:40 -0500 (CDT)
From: "Chris Smith" <chris@zimbra.tech>
To: Randy Leiker <randy@skywaynetworks.com>
```

DMARC Record (DNS TXT record)

Host name: _dmarc.zimbra.tech

Content:
v=DMARC1; p=quarantine; sp=quarantine;

DMARC Identifier Alignment

Email Headers Sample

```
Return-Path: <chris@mail.zimbra.tech>

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=zimbra.tech; s=myselector; t=1649086243;
        bh=fNtVAJvf3QLrt3x9…
        h=Date:From:To:Message-ID:MIME-Version;
        b=dzL5+UhkQRwbYP+…

Date: Mon, 4 Apr 2022 10:30:40 -0500 (CDT)
From: "Chris Smith" <chris@mail.zimbra.tech>
To: Randy Leiker <randy@skywaynetworks.com>
```

DMARC Record (DNS TXT record)

Host name: _dmarc.zimbra.tech

Content:
v=DMARC1; p=quarantine; sp=quarantine;
adkim=s;

DMARC Identifier Alignment

DMARC Record (DNS TXT record)

Host name: _dmarc.zimbra.tech

Content:
v=DMARC1; p=reject; sp=reject;

Row	SPF	SPF Alignment	DKIM	DKIM Alignment	DMARC Alignment	DMARC Policy Applied
1	Pass	Pass	Pass	Pass	Pass	None
2	Pass	Pass	Pass	Fail	Pass	None
3	Pass	Pass	Fail	Fail	Pass	None
4	Pass	Fail	Pass	Pass	Pass	None
5	Fail	Fail	Pass	Pass	Pass	None
6	Pass	Fail	Pass	Fail	Fail	Reject
7	Fail	Fail	Fail	Fail	Fail	Reject

Zimbra Settings For DMARC Alignment

Out Of Office Replies (Auto Responders)

- Check your zimbraAutoSubmittedNullReturnPath global setting to ensure it is set to false. As the Zimbra user (su - zimbra) run:
  - zmprov gcf zimbraAutoSubmittedNullReturnPath
  - zmprov mcf zimbraAutoSubmittedNullReturnPath FALSE

- If this is set to False, it will cause the Return Path address in Out Of Office Replies to an empty value like: <>
- This may cause SPF alignment to fail when your DMARC policy is set to quarantine or reject.
- Newer Zimbra versions should default this setting to False, but older installs may be using a value of True

Zimbra Settings For DMARC Alignment

Zimbra Web Client Personas

1. If you have mailbox setup of user@domain1.com, with an alias of user@domain2.com.

2. From the Zimbra Web Client, create a Persona for user@domain2.com.

3. When a message is sent with the user@domain2.com Persona selected, the following occurs:

   - The Return Path email address is set to: user@domain2.com
   - The From header email address is set to: user@domain1.com
   - If your DMARC policy is set to quarantine or reject, this will cause the SPF alignment test to fail.

To Change This Behavior:

- Set the zimbraSmtpRestrictEnvelopeFrom value to False for either an individual user, a domain, or a Class Of Service. For example, to change this setting for an individual user, as the Zimbra user (su - zimbra):

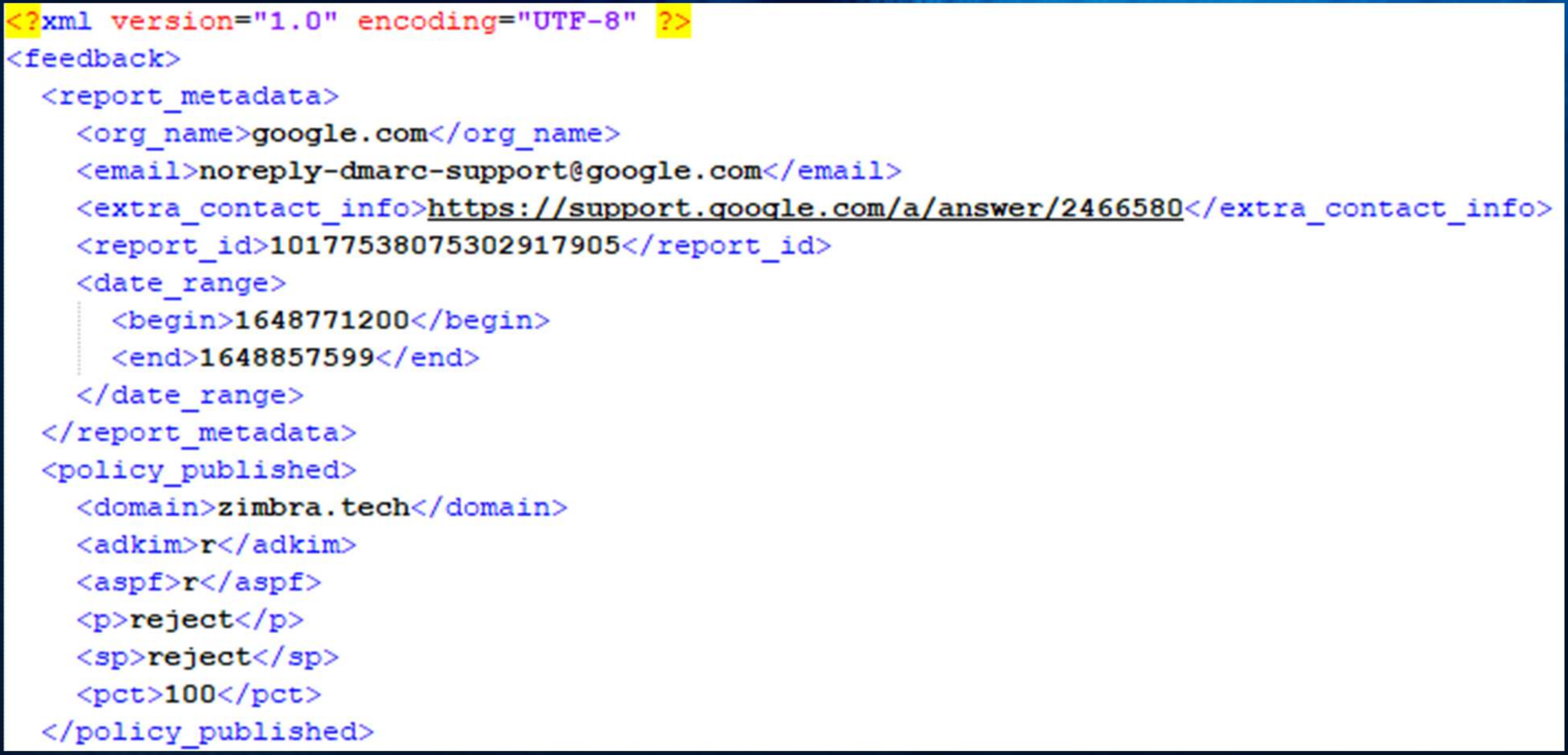
  - zmprov ma user@domain1.com zimbraSmtpRestrictEnvelopeFrom FALSE

Understanding DMARC Reporting

- In an earlier example, Chris setup his DMARC record like this:
  - v=DMARC1; p=none; rua=mailto:dmarc@zimbra.tech; ruf=mailto:dmarc@zimbra.tech; sp=none; fo=1;
- With this DMARC policy, Chris will begin receiving aggregate reports from recipient mail servers who have recently received an email from any zimbra.tech email addresses.
- These reports will typically arrive about every 24 hours.
- Chris could use the ri=(seconds) keyword in his DMARC report (example: ri=43200;) to specify a different interval to receive these reports, but this setting is not always honored by recipient mail servers.
- The reports will always be formatted in XML, and are often sent as a zip or tar-gzipped email attachment.
- To examine the reports, 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.

Understanding DMARC Reporting

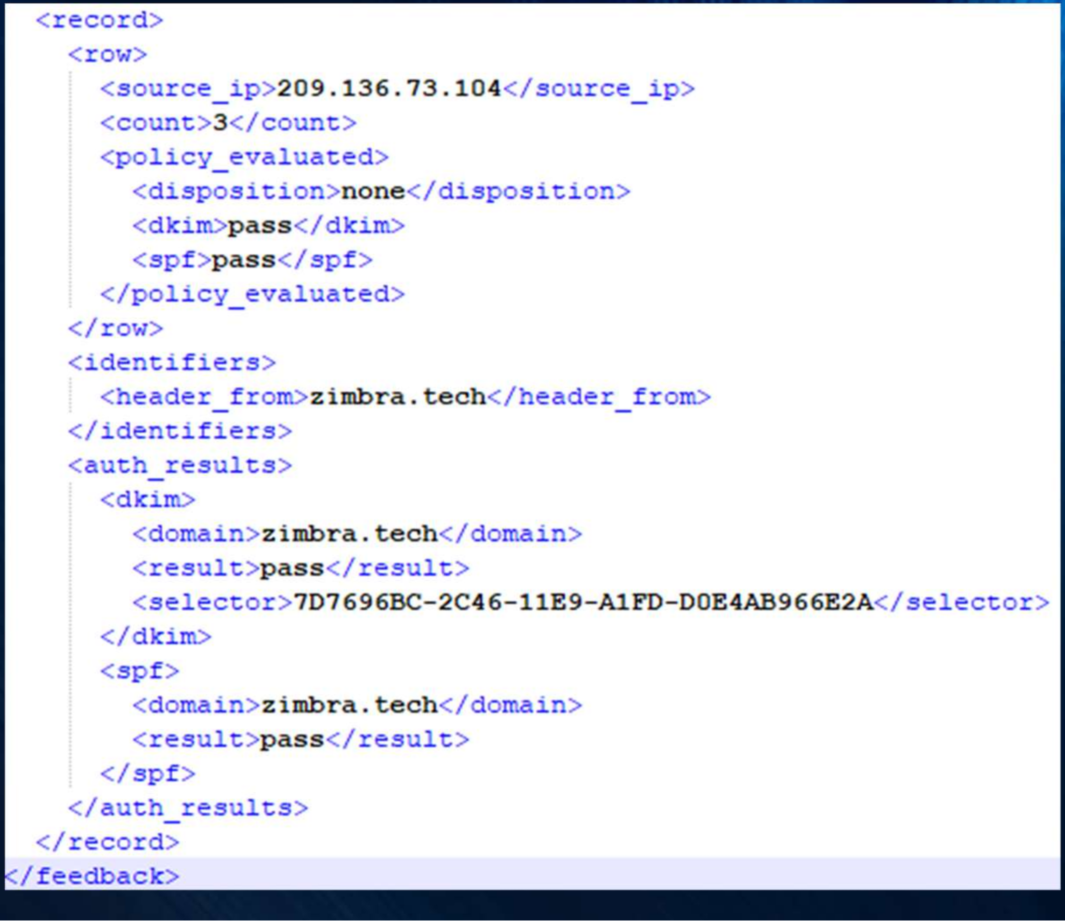
Sample DMARC Aggregate Report, Part 1 of 2:



```xml
<?xml version="1.0" encoding="UTF-8" ?>
<feedback>
  <report_metadata>
    <org_name>google.com</org_name>
    <email>noreply-dmarc-support@google.com</email>
    <extra_contact_info>https://support.google.com/a/answer/2466580</extra_contact_info>
    <report_id>10177538075302917905</report_id>
    <date_range>
      <begin>1648771200</begin>
      <end>1648857599</end>
    </date_range>
  </report_metadata>
  <policy_published>
    <domain>zimbra.tech</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
    <p>reject</p>
    <sp>reject</sp>
    <pct>100</pct>
  </policy_published>
```

Understanding DMARC Reporting

Sample DMARC Aggregate Report, Part 2 of 2:



```
  <record>
    <row>
      <source_ip>209.136.73.104</source_ip>
      <count>3</count>
      <policy_evaluated>
        <disposition>none</disposition>
        <dkim>pass</dkim>
        <spf>pass</spf>
      </policy_evaluated>
    </row>
    <identifiers>
      <header_from>zimbra.tech</header_from>
    </identifiers>
    <auth_results>
      <dkim>
        <domain>zimbra.tech</domain>
        <result>pass</result>
        <selector>7D7696BC-2C46-11E9-A1FD-D0E4AB966E2A</selector>
      </dkim>
      <spf>
        <domain>zimbra.tech</domain>
        <result>pass</result>
      </spf>
    </auth_results>
  </record>
</feedback>
```

Understanding DMARC Reporting

Commercial Options

- 250ok
- Agari
- DMARC360
- DMARC Analyzer
- Dmarcian
- Red Sift
- Valimail

Free, Open Source Options

- https://github.com/search?q=dmarc

DMARC Best Practices

- **Best Practice # 1:** Before getting started with DMARC, you must have deployed either SPF, DKIM, or preferably both.
- Next, set your initial DMARC policy level for your organization’s domain to p=none and your sub-domain policy level to sp=none, along with setting the rua=mailto:you@domain.example .
- Analyze the DMARC aggregate reports you receive for any email sending IP addresses not already in your SPF DNS TXT record that should be authorized to send email for your domain. Update your SPF record as needed to ensure it is complete and accurate.
- Analyze the DMARC aggregate reports to look for DKIM validation failures. If you see any, check the DKIM configuration of the servers using the DKIM selector provided in the DMARC report to ensure they are configured correctly and that a valid DKIM keypair is being used.
- Analyze the DMARC aggregate reports for SPF Alignment or DKIM Alignment failures. If you see any, check the email sending servers to ensure both the Return Path and From header is being set correctly.

DMARC Best Practices

- **Best Practice # 2:** You must have only one DMARC (DNS TXT) record per domain name (zimbra.tech) or per sub-domain (support.zimbra.tech).

- In large DNS zones, multiple DMARC reports usually occur by accident, when a new DMARC record is being created, rather than editing an existing DMARC record.

- Publishing multiple DMARC records for a given domain or sub-domain will lead to unpredictable email delivery results

DMARC Best Practices

- **Best Practice # 3:** Your goal with DMARC is to reach a policy level of p=reject & sp=reject .

- Many organizations initially deploy DMARC in monitoring mode (p=none & sp=none), but they fail to complete their DMARC configuration and never reach an enforcing policy, effectively negating the benefits of using DMARC.

- Do not skip from p=none to p=reject or sp=none to sp=reject. Instead, progress from none, to quarantine, then to reject. This progression may take days for smaller email sending domains or months for larger email sending domains.

DMARC Best Practices

- **Best Practice # 4:** Any non-email sending domains or sub-domains are subject to abuse. For your non-sending domains / sub-domains, prevent abuse by setting these policies:
  - SPF: v=spf1 -all
  - DMARC: v=DMARC1; p=reject;
- You may want to consider including the rua= keyword in the DMARC policy too for monitoring for any potential attempts at abuse too.

DMARC Best Practices

- **Best Practice # 5:** Once you reach a DMARC policy of p=reject and sp=reject, your DMARC record is likely to remain stable and rarely in need of an update.

- However, DMARC is not set & forget. Keep a look out for these warning signs:

  - A noteworthy increase in the volume of email failing SPF Alignment or DKIM Alignment tests, possibly indicating abuse, or re-configuration needed. SPF records are the most likely to need attention.

  - The use of new, unexpected sub-domains that are sending email.

  - The use of new unexpected IP addresses sending emails on behalf of your domain. Ongoing use of these new IPs may indicate new third-party senders with a legitimate reason to send email using your domain.

DMARC Best Practices

- **Best Practice # 6:** You may have third-party vendors that send email on your domain’s behalf that always send email that fails DMARC Alignment when a policy of quarantine or reject is enforced.

- If you cannot work with these vendors to solve the problem, then isolate these vendors on a sub-domain of their own (example: vendor.zimbra.tech) with a DMARC policy of p=none and sp=reject.

- This enables you to enforce a DMARC policy for your domain and any other sub-domains, while allowing just the one sub-domain the vendor is using to send email without passing DMARC.

- Keep pressure on the vendor to fix the underlying cause of the DMARC Alignment failure, especially when their contracts are up for renewal.

DMARC Questions

Up Next: Key Takeaways

Key Take Aways

- Start slowly with DMARC with a policy of none, followed by quarantine, then reject. Avoid skipping from none to reject.

- Use an open source or commercial tool to parse & summarize the DMARC aggregate reports.

- Protect your non-email sending domains & sub-domains with SPF (v=spf1 -all) and DMARC (v=DMARC1; p=reject;)

- Take the time to understand how DMARC Alignment works. It can be one of the most common reasons for a DMARC policy to be applied.

- Do not allow vendors who cannot support SPF, DKIM, and DMARC to hold you back from securing your domain / sub-domains with DMARC. Use the strategy discussed earlier to isolate any non-compliant vendors on their own sub-domain, or seek vendor alternatives.

Thank You For Attending Today’s Webinar!

- Helpful Links
  - **For testing DMARC records:**
    - https://mxtoolbox.com/dmarc.aspx
    - https://dmarcian.com/dmarc-inspector/
    - https://duckduckgo.com/?q=dmarc+test

Speaker’s Contact Information

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