ESA - Replace Existing DKIM Key with no downtime

Contents

Introduction

This document describes how to replace the existing DKIM signing key on an ESA and DKIM public key in DNS with no downtime.

Requirements

1. Access to the Email Security Appliance (ESA).
2. Access to DNS to add/remove TXT records.
3. The ESA must already be signing messages with a DKIM profile.

Create a new DKIM signing key

You will first need to create a new DKIM signing key on the ESA:

1. Go to Mail Policies > Signing Keys and select "Add Key..."
2. Name the DKIM key and either generate a new private key or paste in an existing one. **Note**: *In most cases, it's recommended that you choose a 2048 bits private key size*.
3. Commit the changes.
   Note: This change won't affect DKIM signing or mail flow. We are just adding a DKIM signing key and not applying it to any DKIM signing profile yet.

Generate a new DKIM signing profile and publish the DNS record to DNS

Next, you will need to create a new DKIM signing profile, generate a DKIM DNS record from that DKIM signing profile and publish that record to DNS:

1. Go to Mail Policies > Signing Profiles and click "Add Profile..." Give the profile a descriptive name in the field "Profile Name."Enter your domain in the field "Domain Name."Enter a new selector string into the field "Selector."

Note: *The selector is an arbitrary string that is used to allow multiple DKIM DNS records for a given domain. We are going to utilize the selector to allow more than one DKIM DNS record in DNS for your domain. It is important to use a new selector that is different from the already existing DKIM signing profile.*
Select the DKIM signing key created in the previous section in the field "Signing Key."At the very bottom of the signing profile, add a new "User." This user should be an unsused placeholder email address. **Caution**: *It is important that you add an unused email address as a user for this signing profile. Otherwise, this profile may sign outbound messages before the DKIM TXT record is published causing DKIM verification to fail. Adding an unused email address as a user ensures that this signing profile doesn't sign any outbound messages.*Click Submit.

2. From here, click "Generate" in the column "DNS Text Record" for the signing profile you just created and copy the DNS record that is generated. It should look similar to the following:

```
selector2._domainkey.example.com. IN TXT "v=DKIM1;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwMaX6wMAk4iQoLNWiEkj0BrIRMDHXQ7743OQUOYZQqEXS
s+jMGomOknAZJpjR8TwmYHVPbD+30QRw0qEiRY3hYcmKOCWZ/hTo+NQ8qj1CSc1LTMdV0HWAi2AGsVOT8BdFHkyxg40
oyGWgktzc1q7zIgWM8usHfKVWFzYgnattNzyEqHsfI7lGilz5gdHBOvmF8LrDSfN"
"KtGrTtvIxJM8pWeJm6pg6TM/cy0FypS2azkrl9riJcWWDvu38JXFL/eeYjGnB1zQeR5Pnbc3sVJd3cGaWx1bWjepyN
QZ1PrS6Zwr7ZxSRa316Oxc36uCid5JAq0z+IcH4KkHqUueSGuGhwIDAQAB;"
```

3. Commit the changes.
4. Submit the DKIM DNS TXT record in step 2 to DNS.
5. Wait until the DKIM DNS TXT record has been fully propagated.

Delete the old signing profile and remove the placeholder user from the new signing profile

Once the DKIM TXT record has been submitted to DNS and you ensured that it has been propagated, the next step will be to delete the old signing profile and remove the placeholder user from the new signing profile:

Note: *It is highly recommended that you backup the ESA configuration file before proceeding with the following steps. This is because if you delete the old DKIM signing profile and there is a need to revert back to the previous configuration, you will be able to easily load the backed up configuration file.*

1. Go to Mail Policies > Signing Profiles, select the old DKIM signing profile and click "Delete."
2. Go into the new DKIM signing profile, select the current placeholder user and click "Remove."
3. Click "Submit."
4. Under the column "Test Profile" click "Test" for the new DKIM signing profile. If the test is successful, continue to the next step. If not, confirm that the DKIM DNS TXT record has been fully propagated.
5. Commit the changes made.

Test mail flow to confirm DKIM passes

At this point, you are done with configuring DKIM any further. However, you should test DKIM

signing to ensure that it's signing your outbound messages as expected and passing DKIM verification:

1. Send a message through the ESA ensuring that it gets DKIM signed by the ESA and DKIM verified by another host.
2. Once the message is received on the other end, check the headers of the message for the header "Authentication-Results." Look for the DKIM section of the header to confirm if it passed DKIM verification or not. The header should look similar to the following:
   ```
   Authentication-Results: mx1.example.net; spf=SoftFail smtp.mailfrom=user1@example.net;
   dkim=pass header.i=none; dmarc=fail (p=none dis=none) d=example.net
   ```
3. Look for the header "DKIM-Signature" and confirm that the correct selector and domain are being used:

   ```
   DKIM-Signature: a=rsa-sha256; d=example.net; s=selector2;
     c=simple; q=dns/txt; i=@example.net;
     t=1117574938; x=1118006938;
     h=from:to:subject:date;
     bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
     b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZ
              VoG4ZHRNiYzR
   ```
4. Once you are satisfied that DKIM is working as intended, wait at least one week before removing the old DKIM TXT record. This ensures that all messages signed by the old DKIM key have been processed.