ESA - Configure DKIM Signing

Contents

Introduction

This document describes how to configure DKIM signing on an ESA.

Requirements

1. Access to the Email Security Appliance (ESA).
2. Access to DNS to add/remove TXT records.

Ensure that DKIM signing is off

Before we make any changes, we want to ensure that DKIM signing is off in all mail flow policies. This will allow us to configure DKIM signing without any impact to mail flow:

1. Go to Mail Policies > Mail Flow Policies.
2. Go to each mail flow policy and ensure that "Domain Key/DKIM Signing" is set to "Off."

Create a 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.

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.*
   Select the DKIM signing key created in the previous section in the field "Signing Key."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.
6. Go to Mail Policies > Signing Profiles.
7. Under the column "Test Profile", click "Test" for the new DKIM signing profile. If the test is successful, continue with this guide. If not, confirm that the DKIM DNS TXT record has been fully propagated.

Turn DKIM signing on

Now that the ESA is configured to DKIM sign messages, we can turn DKIM signing on:

1. Go to Mail Policies > Mail Flow Policies.
2. Go to each mail flow policy that has the "Connection Behavior" of "Relay" and turn "Domain Key/DKIM Signing" to "On."
   Note: *By default, the only mail flow policy with a "Connection Behavior" of "Relay" is the mail flow policy called "Relayed." The important thing to remember here is that we only want to DKIM sign messages that are outgoing.*
3. Commit the changes.

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
```