Configure DKIM Signing on ESA

Contents

Introduction

This document describes how to configure DomainKeys Identified Mail (DKIM) signing on an Email Security Appliance (ESA).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Email Security Appliance (ESA) access.
- DNS edit access to add/remove TXT records.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Ensure that DKIM Signing is Off

You need to ensure that DKIM signing is off in all mail flow policies. This allows you to configure DKIM signing without any impact to mail flow:

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

Create a DKIM Signing Key

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

1. Navigate to **Mail Policies > Signing Keys** and select **Add Key...**
2. Name the **DKIM key** and either generate a new private key or paste into a current key.

   Note: In most cases, it is 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 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. Navigation to **Mail Policies > Signing Profiles** and click **Add Profile**.
   1. Give the profile a descriptive name in the field **Profile Name**.
   2. Enter your domain in the field **Domain Name**.
   3. Enter a new selector string into the **Selector** field.

      Note: The selector is an arbitrary string that is used to allow multiple DKIM DNS records for a given domain.

   4. Select the DKIM signing key created in the previous section in the field **Signing Key**.
   5. 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 must look similar to the following:

```
selector2._domainkey.domainsite IN TXT "v=DKIM1; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwMa
```

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. Navigate 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**. You need to make sure that only DKIM sign messages are

outbound.

3. Commit the changes.

Test Mail Flow to Confirm DKIM Passes

At this point, the DKIM is configured. However, you need to test DKIM signing to ensure that it is signing outbound messages as expected and that it passes DKIM verification:

1. Send a message through the ESA and ensure 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 must look similar to this example:
   <#root>

   ```
   Authentication-Results: mx1.domainsite; spf=SoftFail smtp.mailfrom=user1@domainsite;
   ```

   dkim=pass

   ```
    header.i=none; dmarc=fail (p=none dis=none) d=domainsite
   ```

3. Look for the header "DKIM-Signature" and confirm that the correct selector and domain are used:

   <#root>

   ```
   DKIM-Signature: a=rsa-sha256;
   ```

   d=domainsite

   ;

   s=selector2

   ;

   ```
      c=simple; q=dns/txt; i=@domainsite;
      t=1117574938; x=1118006938;
      h=from:to:subject:date;
      bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
      b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZ
               VoG4ZHRNiYzR
   ```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific way to troubleshoot for this configuration.

Related Information

- **Cisco Technical Support & Downloads**