Configurar assinatura DKIM em ESA

Contents

Introdução

Este documento descreve como configurar a assinatura de DomainKeys Identified Mail (DKIM) em um Email Security Appliance (ESA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso ao Email Security Appliance (ESA).
- Acesso de edição de DNS para adicionar/remover registros TXT.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Verifique se a assinatura DKIM está desativada

Você precisa garantir que a assinatura DKIM esteja desativada em todas as políticas de fluxo de e-mail. Isso permite que você configure a assinatura DKIM sem nenhum impacto no fluxo de e-mail:

1. Navegação para **Políticas de e-mail > Políticas de fluxo de e-mail**.
2. Navegue para cada política de fluxo de mensagens e verifique se a **assinatura DKIM/chave de domínio** está definida como **Desativada**.

Criar uma chave de assinatura DKIM

Você precisa criar uma nova chave de assinatura DKIM no ESA:

1. Navegue para **Políticas de e-mail > Chaves de assinatura** e selecione **Adicionar chave...**
2. Nomeie a **chave DKIM** e gere uma nova chave privada ou cole em uma chave atual.

   Observação: na maioria dos casos, é recomendável escolher um tamanho de chave privada de 2048 bits.

   ---

3. Confirme as alterações.

Gerar um novo perfil de assinatura DKIM e publicar o registro DNS no DNS

Em seguida, você precisa criar um novo perfil de assinatura DKIM, gerar um registro DNS DKIM a partir desse perfil de assinatura DKIM e publicar esse registro no DNS:

1. Navegue até **Políticas de e-mail > Perfis de assinatura** e clique em **Adicionar** perfil**.**
   1. Dê ao perfil um nome descritivo no campo **Nome do perfil**.
   2. Insira seu domínio no campo **Domain Name**.
   3. Digite uma nova string do seletor no campo **Seletor**.

      Observação: o seletor é uma sequência arbitrária usada para permitir vários registros DNS DKIM para um determinado domínio.

      ---

   4. Selecione a chave de assinatura DKIM criada na seção anterior no campo **Signing Key**.
   5. Clique em Submit.
2. A partir daqui, clique em **Gerar** na coluna **Registro de texto DNS** para o perfil de assinatura que você acabou de criar e copie o registro DNS que é gerado. Ele deve ser semelhante ao seguinte:

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

3. Confirme as alterações.
4. Envie o registro TXT DNS DKIM na etapa 2 para o DNS.
5. Aguarde até que o registro DKIM DNS TXT seja totalmente propagado.
6. Vá para **Políticas de e-mail > Perfis de assinatura**.
7. Na coluna **Test Profile**, clique em **Test** para o novo perfil de assinatura DKIM. Se o teste for bem-sucedido, continue com este guia. Caso contrário, confirme se o registro DKIM DNS TXT foi totalmente propagado.

Ativar assinatura DKIM

Agora que o ESA está configurado para mensagens de assinatura DKIM, podemos ativar a assinatura DKIM:

1. Navegue até **Políticas de e-mail > Políticas de fluxo de e-mail**.
2. Vá para cada política de fluxo de e-mail que tenha o **Comportamento de Conexão** de **Retransmissão** e torne **On** a **Assinatura de DKIM/Chave de Domínio**.

> **Observação**: por padrão, a única política de fluxo de e-mail com um **Comportamento de Conexão de Relay é a política de fluxo de e-mail chamada Relayed.** Você precisa certificar-se de que somente as mensagens de assinatura DKIM sejam enviadas.

3. Confirme as alterações.

Testar o fluxo de e-mail para confirmar a aprovação do DKIM

Neste ponto, o DKIM está configurado. No entanto, você precisa testar a assinatura DKIM para garantir que ela esteja assinando mensagens de saída como esperado e que passe na verificação DKIM:

1. Envie uma mensagem pelo ESA e verifique se ele recebe a assinatura DKIM pelo ESA e se DKIM foi verificado por outro host.
2. Uma vez que a mensagem é recebida na outra extremidade, verifique os cabeçalhos da mensagem para o cabeçalho **Authentication-Results**. Procure a seção DKIM do cabeçalho para confirmar se ela passou na verificação DKIM ou não. O cabeçalho deve ser semelhante a este exemplo:
   <#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. Procure o cabeçalho "DKIM-Signature" e confirme se o seletor e o domínio corretos estão sendo usados:

   <#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
   ```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

No momento, não há nenhuma maneira específica de solucionar problemas dessa configuração.

Informações Relacionadas

- **Suporte técnico e downloads da Cisco**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.