Prática recomendada para autenticação de e-mail - formas ideais de implantar SPF, DKIM e DMARC

Contents

Introduction

Este guia descreve três tecnologias predominantes de autenticação de e-mail em uso atualmente - SPF, DKIM e DMARC, e discute vários aspectos de sua implementação. Várias situações de arquitetura de e-mail reais são discutidas e diretrizes para implementá-las no conjunto de produtos Cisco Email Security. Como este é um guia prático de melhores práticas, alguns dos materiais mais complexos serão omitidos. Quando necessário, certos conceitos podem ser simplificados ou condensados para facilitar a compreensão da matéria apresentada.

Requisitos de conhecimento do produto

Este guia é um documento de nível avançado. Para acompanhar o material apresentado, o leitor deve possuir o conhecimento do produto do Cisco Email Security Appliance no nível da certificação Cisco Email Security Field Engineer. Além disso, os leitores devem ter um forte comando de DNS e SMTP e sua operação. A aquisição dos conceitos básicos de SPF, DKIM e DMARC é um plus.

Autenticação de e-mail - Uma breve visão geral

Estrutura de política de remetente (SPF)

A Sender Policy Framework foi publicada pela primeira vez em 2006, como RFC4408. A versão atual é especificada no RFC7208 e atualizada no RFC7372. Em essência, ele fornece uma maneira simples para um proprietário de domínio anunciar suas fontes de e-mail legítimas aos destinatários que usam DNS. Embora o SPF autentique principalmente o endereço do caminho de retorno (MAIL FROM), a especificação recomenda (e fornece mecanismo) para também autenticar o argumento SMTP HELO/EHLO (FQDN do gateway do remetente como transmitido durante a conversação SMTP).

O SPF usa registros de recursos DNS do tipo TXT de sintaxe bastante simples:

```
spirit.com       text = "v=spf1 mx a ip4:38.103.84.0/24 a:mx3.irit.com
a:mx4.irit.com include:spf.protection.outlook.com ~all"
```

O registro da Spirit Airlines acima permite que o e-mail de endereços @irit.com venha de uma sub-rede /24 específica, duas máquinas identificadas por um FQDN e o ambiente Office365 da Microsoft. O qualificador "~all" no final instrui os receptores a considerar qualquer outra fonte como Soft Fail - um dos dois modos de falha do SPF. Observe que os remetentes não especificam o que os receptores devem fazer com mensagens com falha, apenas até que ponto elas falharão.

A Delta, por outro lado, emprega um esquema SPF diferente:

```
delta.com text = "v=spf1 a:smtp.hosts.delta.com
include:_spf.vendor.delta.com -all"
```

Para minimizar o número de consultas de DNS necessárias, a Delta criou um único registro "A" listando todos os seus gateways SMTP. Eles também fornecem um registro SPF separado para seus fornecedores em "_spf.vendor.delta.com". Eles também incluem instruções para **Falha** no **disco rígido** em mensagens não autenticadas pelo qualificador SPF ("-all"). Podemos pesquisar ainda mais o registro SPF do fornecedor:

```
_spf.fornecedor.delta.com texto = "v=spf1 include:_spf-delta.vrli.com
include:_spf-ncr.delta.com a:delta-spf.niceondemand.com
include:_spf.airfrance.fr include:_spf.qemailserver.com
include:skytel.com include:epsl1.com tudo"
```

Assim, os e-mails dos remetentes @delta.com podem vir legitimamente de, por exemplo, gateways de e-mail da Air France.

Por outro lado, a United usa um esquema SPF muito mais simples:

```
texto united.com = "v=spf1 include:spf.enviaremails.com.br
include:spf.usa.net include:coair.com ip4:161.215.0.0/16
ip4:209.87.112.0/20 ip4:74.112.71.93 ip4:74.209.251.0/24 mx ~all"
```

Além de seus próprios gateways de correio corporativo, eles incluem seus provedores de marketing por e-mail ("eua.net" e "enviaremails.com.br"), gateways da Continental Air Lines legados, assim como tudo listado em seus registros MX ("mecanismo MX"). Observe que o MX (um gateway de correio **de entrada** para um domínio) pode não ser o mesmo que **de saída**. Embora, para empresas menores, elas geralmente sejam as mesmas, empresas maiores terão uma infraestrutura separada para lidar com e-mails recebidos e manusear separadamente a entrega de saída.

Além disso, vale a pena observar que todos os exemplos acima fazem uso extensivo de referências de DNS adicionais (mecanismos de "inclusão"). No entanto, por razões de desempenho, a especificação SPF limita o número total de pesquisas de DNS necessárias para recuperar um registro final para **dez**. Qualquer pesquisa de SPF com mais de 10 níveis de recursão de DNS falhará.

E-mail identificado das chaves de domínio (DKIM)

O DKIM, especificado nos RFCs 5585, 6376 e 5863, é uma fusão de duas propostas históricas: DomainKeys da Yahoo e o Internet Mail identificado da Cisco. Ele fornece uma maneira simples para os remetentes assinarem criptograficamente mensagens de saída e incluir as assinaturas (juntamente com outros metadados de verificação) em um cabeçalho de e-mail ("DKIM-Signature"). Os remetentes publicam sua chave pública no DNS, facilitando assim que qualquer receptor recupere a chave e verifique assinaturas. A DKIM não autentica a origem das mensagens físicas, mas se a origem estiver na posse da chave privada da organização do remetente, ela estará implicitamente autorizada a enviar um e-mail em seu nome.

Para implementar o DKIM, a organização de envio geraria um ou mais pares de chaves públicas e publicaria as chaves públicas no DNS como registros TXT. Cada par de chaves seria referenciado por um "seletor" para que os verificadores DKIM possam diferenciar entre chaves. As mensagens de saída seriam assinadas e o cabeçalho DKIM-Signature inserido:

```
Assinatura DKIM: v=1; a=rsa-sha1; c=relaxado/relaxado; s=unidos;
d=news.united.com;h=MIME-Version:Content-Type:Content-Transfer-
Encoding:Date:To:From:Reply-To:Subject:List-Unsubscribe:Message-ID;
i=MileagePlus@news.united.com; bh=IBSWR4yzI1PSRYtWLx4SRDSWII4=;

b=HrN5QINgnXwqkx+Zc/9VZys+yhikrP6wSZVu35KA0jfgYzhzSdfA2nA8D2JYIFTNLO8j4D
GmKhH1MMTyYqT
01EwL0V8MEY1MzxTrzijkGLPqt/sK1WZt9pBacEw1fMWRQLf3BxZ3jaYtLoJMRwxtgoWdfHU
35CsFG2CNYLo=
```

O formato da assinatura é bastante simples. "a" tag especifica os algoritmos usados para assinatura, "c" especifica o(s) esquema(s) de canonicalização usado(s) [1], "s" é o seletor ou a referência da chave, "d" é o domínio de assinatura. O restante deste cabeçalho DKIM-Signature é específico da mensagem: "h" lista cabeçalhos assinados, "i" lista a identidade do usuário assinante e, finalmente, o cabeçalho termina com dois hashes separados: "bh" é um hash de cabeçalhos assinados, enquanto "b" é o valor de hash para o corpo da mensagem.

Ao receber uma mensagem assinada por DKIM, o receptor procurará a chave pública construindo a seguinte consulta DNS:

```
<seletor>._domainkey.<domínio de assinatura>
```

conforme especificado no cabeçalho DKIM-Signature. Para o exemplo acima, nossa consulta seria "united._domainkey.news.united.com":

```
unido._domainkey.news.united.com texto = "g=*\; k=rsa\; n=" "Contato"
"postmaster@responsys.com" "com" "qualquer" "pergunta" "relativa" a
"esta" "assinatura" "\;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/Vh/xq+sSRLhL5CRU1drFTGMXX/Q2Kk
Wgl35hO4v6dTy5Qmxcuv5Awqx
Liz9d0jBaxtuvYALjlGkxmk5MemgAOcCr97GlW7Cr11eLn87qdTmyE5LevnTXxVDMjIfQJt6
OFzmw6Tp1t05NPWh0PbyUohZYt4qpcbiz9Kc3UB2IBwIDAQAB\;"
```

O registro DNS retornado contém a chave, assim como outros parâmetros opcionais. [2]

O principal problema com a DKIM é que a especificação inicial não permitia a publicidade que um remetente usa DKIM. Assim, se uma mensagem vem sem uma assinatura, não há uma maneira fácil de um receptor saber que ela deveria ter sido assinada e que, nesse caso, provavelmente não é autêntica. Como uma única organização pode (e na maioria das vezes usará) vários seletores, não é trivial "adivinhar" se um domínio está habilitado para DKIM. Um padrão separado, as Práticas de Assinatura de Domínio Autor, foi desenvolvido para cobrir isso, mas devido ao baixo uso e outros problemas foram obsoletos em 2013 sem sucessor.

Autenticação de Mensagens, Relatórios E Conformidade Baseados Em Domínio (DMARC - Domain-Based Message Authentication, Reporting And Conformance)

O DMARC é a mais nova das três tecnologias de autenticação de e-mail abordadas e foi desenvolvido especificamente para lidar com as deficiências de SPF e DKIM. Ao contrário dos outros dois, autentica o cabeçalho de uma mensagem e vincula-se às verificações executadas anteriormente pelos outros dois. O DMARC é especificado no RFC7489.

O valor agregado de DMARC sobre SPF e DKIM inclui:

- Certificar-se de que todas as identidades disponíveis (domínio de assinatura HELO, MAIL FROM e/ou DKIM) estejam alinhadas (exatamente correspondendo ou subordinadas) com o cabeçalho De
- Fornecer um meio para que o proprietário do domínio do remetente especifique uma política para os receptores sobre como eles **devem** lidar com mensagens com falha
- Fornecer um recurso de feedback para que os proprietários de domínio do remetente sejam informados sobre quaisquer mensagens com falha, facilitando assim a identificação de campanhas de phishing ou erros na atribuição de políticas SPF/DKIM/DMARC

O DMARC também usa um mecanismo de distribuição de política simples baseado em DNS:

```
_dmarc.aa.com texto = "v=DMARC1\; p=nenhum\; fo=1\; ri=3600\;
Rua=mailto:american@rua.agari.com,mailto:dmarc@aa.com\;
ruf=mailto:american@ruf.agari.com,mailto:dmarc@aa.com"
```

A única marca obrigatória na especificação de política DMARC é "p", especificando a política a

ser usada em mensagens com falha. Pode ser um dos três: nenhum, quarentena, rejeição.

Os parâmetros opcionais usados com mais frequência têm a ver com relatórios: "Rua" especifica um URL (um endereço postal: ou um URL http:// usando o método POST) para enviar relatórios agregados diários sobre todas as mensagens com falha que se supõem vir de um domínio específico. "ruf" especifica um URL para enviar relatórios detalhados imediatos de falhas em cada mensagem com falha.

De acordo com as especificações, um receptor **deve** aderir à política anunciada. Caso contrário, eles **devem** notificar o proprietário do domínio do remetente no relatório agregado.

O conceito central de DMARC é o chamado alinhamento de identificador. O alinhamento do identificador define como uma mensagem pode passar na verificação de DMARC. Os identificadores SPF e DKIM são alinhados separadamente, e uma mensagem precisa passar **qualquer** deles para passar o DMARC no geral. No entanto, há uma opção de política DMARC na qual o remetente pode solicitar que um relatório de falha seja gerado mesmo que um alinhamento seja aprovado, mas o outro falhe. Podemos ver isso no exemplo acima com a marca "fo" definida como "1".

Há duas maneiras de as mensagens aderirem ao alinhamento do identificador DKIM ou SPF, rigoroso e relaxado. Adesão estrita significa que o FQDN do cabeçalho De deve corresponder totalmente ao ID de domínio de assinatura ("tag"d") da assinatura DKIM ou FQDN do comando MAIL FROM SMTP para SPF. Relaxado, por outro lado, permite que o cabeçalho de FQDN seja um subdomínio dos dois anteriores. Isso tem implicações importantes ao delegar seu tráfego de e-mail a terceiros, que serão discutidas posteriormente no documento.

Considerações sobre a implantação do SPF

SPF para destinatários

A verificação SPF é trivial para configurar no Cisco Email Security Appliance ou nos dispositivos virtuais Cloud Email Security. Para o resto deste documento, qualquer referência ao SEC também incluirá o CES.

A verificação SPF é configurada em Políticas de fluxo de e-mail - a maneira mais fácil de executá-la globalmente é ativá-la na seção Parâmetros de política padrão dos ouvintes apropriados. Se você estiver usando o mesmo ouvinte para coleta de e-mails de entrada e saída, verifique se a política de fluxo de e-mail "RELAYED" tem a verificação SPF definida como "Off".

Como o SPF não permite a especificação de ação de política, a verificação SPF (assim como o DKIM, como veremos mais adiante) verifica apenas a mensagem e insere um conjunto de cabeçalhos para cada verificação SPF executada:

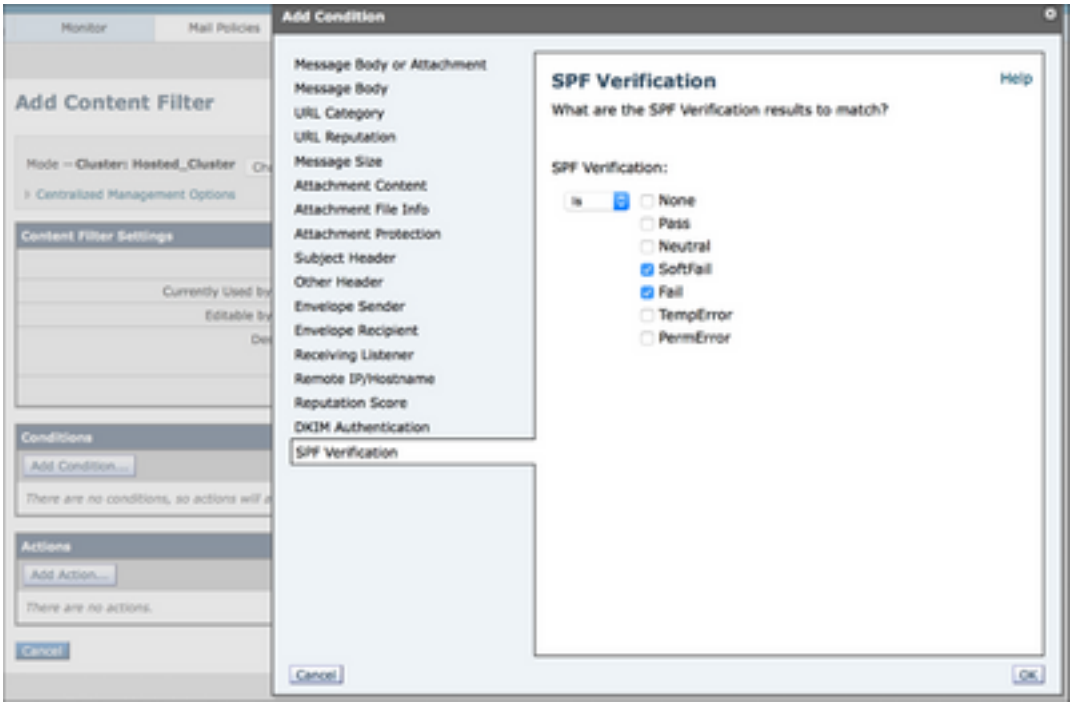
```
SPF recebido: Aprovado (mx1.hc4-93.c3s2.smtpi.com: domínio de

  united.5765@envfrm.rsys2.com designa 12.130.136.195 como

  remetente permitido) identity=mailfrom;

  client-ip=12.130.136.195; receptor=mx1.hc4-93.c3s2.smtpi.com;

  envelope de="united.5765@envfrm.rsys2.com";
```

```
  x-sender="united.5765@envfrm.rsys2.com";

  x-conformance=sidf_compatible; x-record-type="v=spf1"

SPF recebido: Nenhum (mx1.hc4-93.c3s2.smtpi.com: sem remetente

  informações de autenticidade disponíveis no domínio de

  postmaster@omp.news.united.com) identity=helo;

  client-ip=12.130.136.195; receptor=mx1.hc4-93.c3s2.smtpi.com;

  envelope de="united.5765@envfrm.rsys2.com";

  x-sender="postmaster@omp.news.united.com";

  x-conformance=sidf_compatible
```

Observe que, para esta mensagem, duas "identidades" foram verificadas pelo SPF: "mailfrom", conforme exigido pela especificação, e "helo", como recomendado pelo mesmo. A mensagem passará formalmente o SPF, já que apenas o primeiro é relevante para a conformidade do SPF, mas alguns receptores podem sancionar os remetentes que não incluem registros SPF para suas identidades de HELO também. Portanto, é uma boa prática incluir os nomes de host dos gateways de e-mail de saída em seus registros SPF.

Depois que as Políticas de fluxo de e-mail verificarem uma mensagem, cabe aos administradores locais configurar uma ação a ser executada. Isso é feito usando a regra SPF-status() [3] do Filtro de Mensagens ou criando um Filtro de Conteúdo de Entrada usando o mesmo e aplicando-o às Políticas de Correio de Entrada apropriadas.

Figura 1: Condição do filtro de conteúdo de verificação SPF



As ações de filtro recomendadas são descartar as mensagens com falha ("-all" no registro SPF) e colocar em quarentena as mensagens com falha ("~all" no registro SPF) em uma Quarentena de

política, no entanto, isso pode variar de acordo com seus requisitos de segurança. Alguns receptores apenas marcam mensagens com falha ou não tomam nenhuma ação visível, mas relatam aos administradores.

Recentemente, houve um aumento significativo na popularidade do SPF, mas muitos domínios publicam registros SPF incompletos ou incorretos. Para estar no lado seguro, você pode querer colocar em quarentena todas as mensagens com falha de SPF e monitorar a quarentena por um tempo, para garantir que não haja "falsos positivos".

Se Você Fornecer Serviços De E-Mail Para Outros Domínios Ou Terceiros

Se você fornecer serviços de entrega de e-mail ou hospedagem para terceiros, eles terão que adicionar nomes de host e endereços IP que você usa para entregar suas mensagens aos seus próprios registros SPF. A maneira mais fácil de fazer isso é que o provedor crie um registro SPF "guarda-chuva" e faça com que os clientes usem o mecanismo "include" em seus registros SPF.

```
texto suncountry.com = "v=spf1 mx ip4:207.238.249.242 ip4:146.88.177.148
ip4:146.88.177.149 ip4:67.109 .66.68 ip4:198.179.134.238
ip4:107.20.247.57 ip4:207.87.182.66 ip4:199.66.248.0/22 include:cust-
spf.exacttarget .com ~all"
```

Como podemos ver, a Sun Country tem alguns de seus e-mails sob seu próprio controle, mas seus e-mails de marketing são terceirizados para terceiros. A expansão do registro mencionado revela uma lista de endereços IP atuais usados por seu provedor de serviços de e-mail de marketing:

```
cust-spf.exacttarget.com texto = " v=spf1 ip4:64.132.92.0/24
ip4:64.132.88.0/23 ip4:66.231.80.0/20 ip4:68.232.192.0/20
ip4:199.122.120.0/21 ip4:207.67.38.0/24 ip4:207.67.98.192/27
ip4:207.250.68.0/24 ip4:209 .43.22.0/28 ip4:198.245.80.0/20
ip4:136.147.128.0/20 ip4:136.147.176.0/20 ip4:13.111.0.0/18 -all"
```

Essa flexibilidade permite que os provedores de serviços de e-mail escalem sem precisar entrar em contato com cada cliente para modificar seus registros de DNS.

Se você usar serviços de e-mail de terceiros

Da mesma forma que o parágrafo anterior, se você estiver usando qualquer serviço de e-mail de terceiros e quiser estabelecer um fluxo de e-mail totalmente verificado por SPF, deverá incluir seus próprios registros SPF no seu.

```
texto descritivo "v=spf1 include:_spf.qualtrics.com ?all"
```

A JetBlue usa o serviço de análise Qualtrics, e a única coisa que eles precisavam fazer era incluir um registro SPF correto da Qualtrics. Da mesma forma, a maioria dos outros ESPs fornece registros SPF para serem incluídos nos registros de seus clientes.

Se o seu ESP ou profissional de e-mail não fornecer registros SPF, você terá que listar seus gateways de saída de e-mail diretamente no seu. No entanto, é sua responsabilidade manter esses registros precisos e, se o provedor adicionar gateways adicionais ou alterar endereços IP ou nomes de host, seu fluxo de e-mail pode estar comprometido.

O perigo adicional de terceiros que não estão conscientes do SPF vem do compartilhamento de recursos: Se um ESP usa o mesmo endereço IP para entregar e-mails de vários clientes, é tecnicamente possível que um cliente gere uma mensagem válida de SPF fingindo ser outro cliente que está entregando através da mesma interface. É por isso que, antes de implementar qualquer restrição SPF, você deve investigar as políticas de segurança do MSP e conhecer a autenticação de e-mail. Se eles não tiverem respostas para suas perguntas, considerando que o SPF é um dos mecanismos básicos de confiança na Internet, você será altamente aconselhável reconsiderar sua escolha de MSP. Não se trata apenas de segurança - SPF, DKIM, DMARC e outras práticas recomendadas de remetentes [4] empregadas pelos MSPs são uma garantia de entrega. Se o seu MSP não segui-los ou segui-los incorretamente, isso diminuirá a confiabilidade deles com grandes sistemas de recebimento e possivelmente atrasará ou até bloqueará suas mensagens.

(Sub)Domínios sem tráfego de e-mail

A maioria das empresas hoje possui vários domínios para fins de marketing, mas usa apenas um ativamente para o tráfego de e-mail corporativo. Mesmo que o SPF seja implantado corretamente no domínio de produção, agentes mal-intencionados ainda podem usar outros domínios que não são usados ativamente para um e-mail para falsificar a identidade de uma empresa. O SPF pode impedir que isso ocorra por meio de um registro SPF especial "deny all" - para qualquer um de seus domínios (e subdomínios!) que não gerem tráfego de e-mail, publique "v=spf1 -all" no DNS. Um excelente exemplo é openspf.org - o site do Conselho SPF.

Como a delegação SPF é válida somente para um único domínio, é importante publicar também registros SPF "deny all" para quaisquer subdomínios que você esteja usando que possam não gerar um e-mail. Mesmo que o domínio de produção tenha um registro SPF "regular", faça um esforço extra para adicionar registros "deny all" a seus subdomínios sem tráfego. E novamente - não se esqueça de que receber não equivale a enviar: Um domínio pode muito bem estar recebendo e-mails, mas nunca será uma origem. Isso é muito verdadeiro para domínios de marketing de curto prazo (por exemplo, eventos, promoções de tempo limitado, lançamentos de produtos...), em que emails recebidos para esses domínios serão entregues ao seu domínio de produção, e quaisquer respostas a esses emails serão fornecidas do domínio de produção. Esses domínios de curto prazo terão um registro MX válido, mas devem ter um registro SPF que os identifique como nenhuma **fonte** de e-mail também.

Considerações sobre implantação DKIM

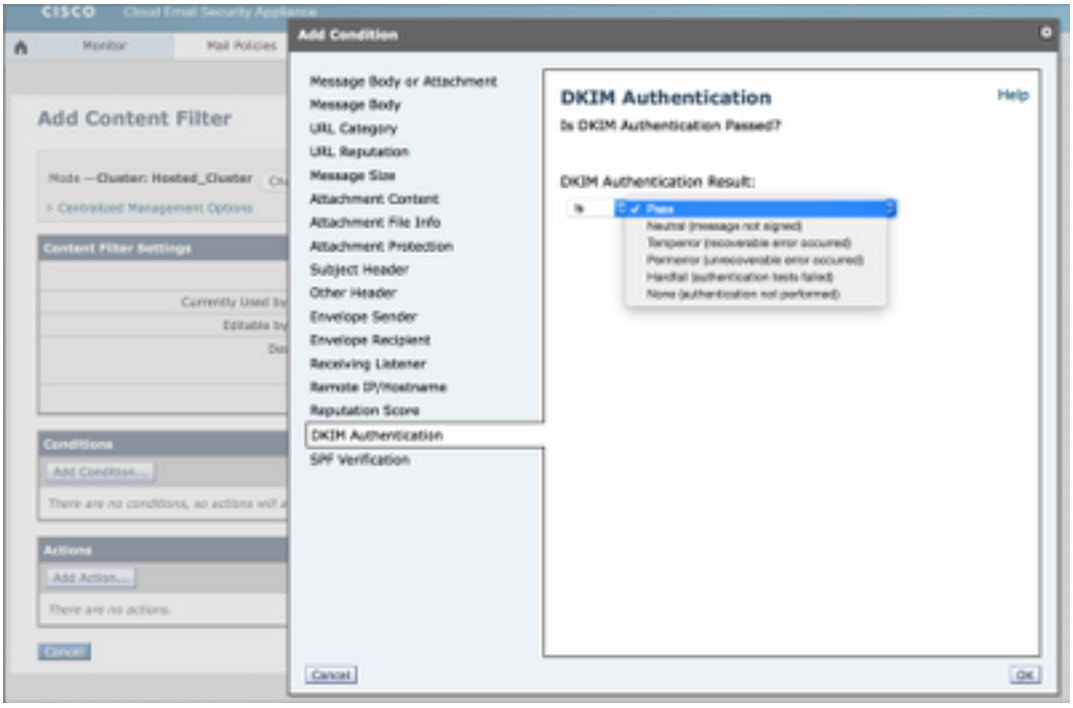
DKIM para destinatários

Configurar a verificação DKIM no ESA é semelhante à verificação SPF. Nos Parâmetros de política padrão das políticas de fluxo de e-mail, basta ativar a verificação DKIM. Novamente, como o DKIM não permite nenhuma especificação de política, isso apenas verificará a assinatura e inserirá um cabeçalho "Authentication-Results":

```
Resultados da autenticação: mx1.hc4-93.c3s2.smtpi.com; dkim=pass
(assinatura verificada) header.i=MileagePlus@news.united.com
```

Todas as ações baseadas nos resultados da verificação DKIM devem ser executadas pelos filtros de conteúdo:

Figura 2: Condição do filtro de conteúdo de verificação DKIM



Ao contrário do SPF, que é direto, o DKIM manipula o texto real da mensagem, portanto alguns parâmetros podem ser limitados. Opcionalmente, você pode criar perfis de verificação DKIM e atribuir perfis de verificação diferentes a diferentes políticas de fluxo de e-mail. Eles permitem limitar os tamanhos de chaves das assinaturas que você aceitará, definir ações de falha de recuperação de chave e configurar a profundidade da verificação DKIM.

Àmedida que uma mensagem passa por vários gateways, ela pode ser assinada várias vezes e, portanto, transportar várias assinaturas. Para que uma mensagem seja aprovada na verificação DKIM, **qualquer** assinatura precisa ser verificada. Por padrão, o ESA verificará até cinco assinaturas.

Devido à abertura histórica do SMTP e do e-mail e à relutância da Internet em se adaptar a mudanças (positivas), ainda há várias situações em que as assinaturas DKIM podem falhar legitimamente, como quando os gerentes de lista de correspondência retransmitem e modificam mensagens diretamente ou quando as mensagens são encaminhadas diretamente, em vez de como anexos a novas mensagens. É por isso que, em geral, a melhor prática para mensagens que falhem no DKIM ainda seria colocar em quarentena ou marcar, em vez de soltá-las.

Preparando-se para assinar com o DKIM

Antes de poder ativar a assinatura DKIM em sua política de fluxo de e-mail RELAYED, você precisa gerar/importar as chaves, criar perfis de assinatura DKIM e publicar as chaves públicas no DNS.

Se você estiver assinando um único domínio, o processo será direto. Gere o par de chaves, crie seu perfil de assinatura único na seção Chaves de domínio das Políticas de e-mail e clique na opção "Gerar" em "Registro de texto DNS" quando seu perfil estiver pronto. Publique a chave como gerada em seu DNS. Finalmente, ative a assinatura DKIM em sua política de fluxo de e-mail.

Émais complicado se você estiver assinando vários domínios distintos. Nesse caso, você tem duas opções:

1. Use um único perfil de assinatura para assinar todos os domínios. Você armazenará a chave pública (única) na zona DNS do domínio "primário" e suas assinaturas DKIM farão referência a essa chave. Esta técnica era muitas vezes utilizada pelos PEE no passado - permitia-lhes assinar em larga escala, sem terem de interagir com o espaço DNS de clientes individuais [5].
2. Crie um perfil de assinatura separado para cada domínio no qual você se conecta. Isso torna a configuração inicial mais complexa, mas oferece muito mais flexibilidade avançando. Crie um par de chaves para cada domínio, crie um perfil especificando apenas um domínio (e seus subdomínios) na seção "Usuários de perfil" e publique a chave pública relevante na zona DNS desse domínio específico.

Embora a opção nº 1 seja mais fácil de começar, lembre-se de que acabará quebrando o DMARC. Como o DMARC exige que o ID de domínio de assinatura esteja alinhado com o cabeçalho de remetente, o alinhamento do identificador com o DKIM falhará. Você poderá se safar se configurar seu SPF corretamente e contar com o alinhamento do identificador SPF para passar na verificação de DMARC.

No entanto, ao implementar a opção nº 2 desde o início, você não precisa se preocupar com o DMARC e é muito fácil revogar ou reconfigurar o serviço de assinatura para apenas um único domínio. Além disso, se você fornecer **alguns** serviços de e-mail para um domínio de terceiros, provavelmente precisará obter a chave para usar deles (e importá-la para seu ESA). Essa chave será específica do domínio, portanto você precisará criar um perfil separado.

Se você usar serviços de e-mail de terceiros

Em geral, se você usar a assinatura DKIM e descarregar parte do seu processamento de e-mail (por exemplo, e-mails de marketing) para terceiros, você não vai querer que eles usem as mesmas chaves que você usa na produção. Essa é uma das principais razões para a existência de Seletores na DKIM. Em vez disso, você deve gerar um novo par de chaves, publicar a parte pública em sua zona DNS e entregar a chave secreta para a outra parte. Isso também permitirá que você revogue rapidamente essa chave específica em caso de problemas, mantendo sua infraestrutura DKIM de produção intocada.

Embora não seja necessário para o DKIM (as mensagens para o mesmo domínio podem ser assinadas com várias chaves diferentes), é uma boa prática fornecer um subdomínio separado para qualquer e-mail tratado por terceiros. Isso facilitará o rastreamento das mensagens e permitirá uma implementação muito mais limpa do DMARC posteriormente. Por exemplo, considere estes cinco cabeçalhos DKIM-Signature de várias mensagens da Lufthansa:

```
Assinatura DKIM: v=1; a=rsa-sha1; c=relaxado/relaxado; s=lufthansa;
d=newsletter.milesandmore.com;

Assinatura DKIM: v=1; a=rsa-sha1; c=relaxado/relaxado; s=lufthansa2;
d=newsletter.lufthansa.com;

Assinatura DKIM: v=1; a=rsa-sha1; c=relaxado/relaxado; s=lufthansa3;
d=lh.lufthansa.com;

Assinatura DKIM: v=1; a=rsa-sha1; c=relaxado/relaxado; s=lufthansa4;
d=e.milesandmore.com

Assinatura DKIM: v=1; a=rsa-sha1; c=relaxado/relaxado; s=lufthansa5;
```

```
d=fly-lh.lufthansa.com;
```

Podemos ver que a Lufthansa está usando cinco chaves diferentes (seletores) divididas em cinco subdomínios separados de dois domínios de produção primários (lufthansa.com e milesandmore.com). Isso significa que cada um deles pode ser controlado de forma independente, e cada um pode ser terceirizado para um provedor de serviços de mensagens diferente.

Considerações sobre implantação de DMARC

DMARC para destinatários

A verificação de DMARC no ESA é baseada em perfil, mas ao contrário do DKIM, o perfil padrão deve ser editado para ser compatível com a especificação. O comportamento padrão do ESA é nunca descartar nenhuma mensagem, a menos que seja explicitamente instruído pelo cliente, portanto, o perfil de verificação DMARC padrão terá todas as ações definidas como "Nenhuma ação". Além disso, para habilitar a geração correta de relatórios, você precisará editar "Configurações globais" da seção DMARC de "Políticas de e-mail".

Depois que um perfil tiver sido configurado, a verificação DMARC, assim como as outras duas, será definida na seção Configurações de política padrão das Políticas de fluxo de e-mail. Certifique-se de marcar a caixa para enviar relatórios de feedback agregado - este é provavelmente o recurso mais importante do DMARC para o remetente. No momento da elaboração, o ESA não suporta a geração de relatórios de falha por mensagem (tag "ruf" da política DMARC).

Como as ações da política DMARC são aconselhadas pelo remetente, ao contrário do SPF ou do DKIM, não há ações específicas configuráveis fora da configuração do perfil. Não é necessário criar nenhum filtro de conteúdo.

A verificação DMARC adicionará campos adicionais ao cabeçalho Authentication-Results:

```
Resultados da autenticação: mx1.hc4-93.c3s2.smtpi.com; dkim=pass
(assinatura verificada) header.i=MileagePlus@news.united.com; dmarc=pass
(p=none dis=none) d=news.united.com
```

No exemplo acima, vemos que o DMARC foi verificado com base no alinhamento do identificador DKIM, e o remetente solicitou uma política de "nenhum". Isso indica que eles estão atualmente na fase de "monitoramento" da implantação do DMARC.

Se Você Fornecer Serviços De E-Mail Para Outros Domínios Ou Terceiros

A maior preocupação dos ESPs com relação à conformidade com DMARC é alcançar o alinhamento de identificador adequado. Ao planejar o DMARC, certifique-se de que o SPF esteja configurado corretamente, que todos os outros domínios relevantes tenham seus gateways de saída em seus registros SPF e que eles não enviem mensagens que falhem no alinhamento, principalmente usando domínios diferentes para identidade MAIL FROM e Header From. Esse erro é feito com mais frequência por aplicativos que enviam notificações por e-mail ou avisos porque os autores de aplicativos não estão mais cientes das consequências da inconsistência de suas identidades de e-mail.

Como descrito anteriormente, certifique-se de usar um perfil de assinatura DKIM separado para cada domínio e de que seu perfil de assinatura faça referência adequada ao domínio para o qual você está entrando, como usado no cabeçalho De. Se estiver usando seus próprios subdomínios, você **pode** assinar com uma única chave, mas certifique-se de definir sua adesão ao DKIM para relaxar na política de DMARC ("adkim="r").

Em geral, se você estiver fornecendo serviços de e-mail para um número maior de terceiros sobre os quais não tem controle direto, é recomendável escrever um documento de diretrizes sobre como enviar um e-mail que provavelmente será entregue. Como o e-mail de usuário para usuário é geralmente bem comportado, ele servirá principalmente como um documento de política para autores de aplicativos nos exemplos mencionados acima.

Se você usar serviços de e-mail de terceiros

Se você usar terceiros para entregar parte do seu tráfego de e-mail, a melhor maneira é delegar um subdomínio separado (ou um domínio completamente diferente) ao provedor de terceiros. Dessa forma, eles podem gerenciar os registros SPF conforme necessário, ter uma infraestrutura de assinatura DKIM separada e não interferir no tráfego de produção. Em seguida, a política DMARC para e-mails terceirizados pode ser diferente da política interna. Como já mencionado, ao considerar o e-mail fornecido por terceiros, certifique-se sempre de que seus identificadores serão alinhados, e sua adesão ao DKIM e ao SPF será definida de forma adequada em sua política de DMARC.

(Sub)Domínios sem tráfego de e-mail

Outra melhoria do DMARC em relação às tecnologias de autenticação de e-mail anteriores é como ele lida com subdomínios. Por padrão, a política DMARC de um determinado domínio se aplica a todos os seus subdomínios. Ao recuperar registros de política DMARC, se não for possível encontrar nenhum registro no cabeçalho do nível FQDN, os receptores são obrigados a determinar o domínio organizacional [6] do remetente e procurar um registro de política ali.

No entanto, a política de DMARC para um Domínio Organizacional também pode especificar uma política de subdomínio ("sp" tag de um registro DMARC) separada que será aplicada para qualquer subdomínio que não tenha uma política de DMARC explícita publicada.

No cenário discutido anteriormente no capítulo SPF, você:

1. Publicar um registro DMARC explícito para quaisquer subdomínios que **sejam** fontes legítimas de correio eletrônico.
2. Publicar uma política de Subdomínio de "rejeitar" no registro de política de Domínio Organizacional para rejeitar automaticamente todos os emails que não enviam domínios

Esse tipo de estruturação da sua autenticação de e-mail oferece a melhor proteção possível da sua infraestrutura e marca.

Problemas específicos do DMARC

Há vários problemas em potencial com o DMARC, todos oriundos da natureza e das deficiências de outras tecnologias de autenticação para as quais ele depende. O problema é que o DMARC trouxe esses problemas à tona, empurrando ativamente uma política para rejeitar o e-mail e correlacionando todos os diferentes identificadores de remetente em uma mensagem.

A maioria dos problemas ocorre com listas de correspondência e software de gerenciamento de listas de correspondência. Quando um e-mail é enviado a uma lista de correspondência, ele é redistribuído para todos os seus destinatários. No entanto, o e-mail resultante, com um endereço de remetente do remetente original, será entregue pela infraestrutura de hospedagem do gerente da lista de distribuição, portanto, falha nas verificações SPF para o Cabeçalho De (a maioria dos gerentes da lista de endereçamento usa o endereço da lista como Envelope De (MAIL DE) e o endereço do remetente original como Cabeçalho De).

Como o DMARC falhará no SPF, podemos confiar no DKIM, entretanto, a maioria dos gerentes de lista de correspondência também adicionam rodapés a mensagens, ou marcam assuntos com o nome da lista, quebrando a verificação de assinatura DKIM.

Os autores da DKIM sugerem várias soluções para o problema, todas elas se resumem aos gerentes da lista de distribuição que precisam usar o endereço da lista em todos os endereços de remetente e indicam o endereço original do remetente por outro meio.

Problemas semelhantes surgem de mensagens que são encaminhadas apenas copiando a mensagem original sobre SMTP para o novo destinatário. No entanto, a maioria dos agentes de usuário de email em uso hoje formará corretamente uma nova mensagem e incluirá a mensagem encaminhada em linha ou como um anexo à nova. As mensagens encaminhadas dessa forma passarão o DMARC se o usuário de encaminhamento passar (claro, a autenticidade da mensagem original não pode ser estabelecida).

Exemplo de plano de ação para implementar a autenticação de e-mail

Embora as tecnologias em si sejam simples, o caminho para implementar uma infraestrutura completa de autenticação de e-mail pode ser longo e contínuo. Para organizações menores e com fluxos de correio controlados, será bastante simples, enquanto ambientes maiores podem achar um desafio excepcional. Não é raro as grandes empresas contratarem serviços de consultoria para gerir o projeto de implementação.,

Passo 1: DKIM

O DKIM é relativamente não intrusivo, pois as mensagens não assinadas não terão nenhuma rejeição. Antes da aplicação efetiva, ter em conta todos os pontos anteriormente mencionados. Entre em contato com terceiros para os quais você possa delegar a assinatura, certifique-se de que os terceiros suportem a assinatura DKIM e considere sua estratégia de gerenciamento de seletores. Algumas organizações manteriam chaves (seletores) separadas para diferentes unidades organizacionais. Você pode considerar a rotação periódica das chaves para segurança adicional, mas não exclua suas chaves antigas até que todas as mensagens em trânsito sejam entregues.

Deve ser dada especial atenção às dimensões das chaves. Embora, em geral, "mais é melhor", você deve levar em conta que criar duas assinaturas digitais por mensagem (incluindo canonicalização, etc.) é uma tarefa muito cara para a CPU e pode influenciar o desempenho dos gateways de e-mail de saída. Devido à sobrecarga de computação, 2048 bits é o maior tamanho prático de chave que pode ser usado, mas para a maioria das implantações, as chaves de 1024 bits fazem um bom comprometimento entre desempenho e segurança.

Para a implementação subsequente bem-sucedida do DMARC, você deve:

1. identificar todos os domínios enviados como, incluindo subdomínios
2. gerar chaves DKIM e criar perfis de assinatura para cada domínio
3. fornecer chaves privadas relevantes a terceiros
4. publicar todas as chaves públicas em zonas DNS relevantes
5. verificar se terceiros estão prontos para iniciar a assinatura
6. ative a assinatura DKIM em RELAYED Mail Flow Policy em todos os ESAs
7. notificar terceiros para iniciar a assinatura

Passo 2: SPF

A implementação correta do SPF provavelmente será a parte mais demorada e pesada de qualquer implementação da infraestrutura de autenticação de e-mail. Como o e-mail era muito simples de usar e gerenciar, e completamente aberto do ponto de vista de segurança e acesso, as empresas historicamente não aplicavam políticas rígidas sobre quem e como usá-lo. Isso resultou em que a maioria das empresas atualmente não tem uma visão completa de todas as diferentes fontes de e-mail, tanto internas quanto externas. O maior problema na implementação do SPF é descobrir quem está, no momento, enviando e-mails legitimamente em seu nome.

Coisas a procurar:

1. destinos óbvios - Exchange ou outros servidores de groupware ou gateways de e-mail de saída
2. quaisquer soluções DLP ou outros sistemas de processamento de e-mail que possam gerar notificações externas
3. Sistemas CRM que enviam informações interagindo com os clientes
4. vários aplicativos de terceiros que podem enviar e-mails
5. laboratório, teste ou outros servidores que possam enviar e-mail
6. computadores pessoais e dispositivos configurados para enviar um e-mail externo diretamente

A lista acima não está completa, pois as empresas têm ambientes diferentes, mas deve ser considerada uma diretriz geral sobre o que procurar. Depois que (a maioria) de suas fontes de e-mail tiver sido identificada, talvez você queira dar um passo para trás e, em vez de autorizar cada fonte existente, limpar a lista. Idealmente, todos os seus emails de saída devem ser entregues através dos gateways de saída de e-mail com algumas exceções justificadas. Se você tiver a sua própria solução ou usar uma solução de e-mail de marketing de terceiros, deverá usar uma infraestrutura separada que não os gateways de e-mail de produção. Se sua rede de entrega de e-mail for excepcionalmente complicada, você poderá continuar documentando o estado atual em seu SPF, mas levará tempo para limpar a situação no futuro.

Se você atende vários domínios na mesma infraestrutura, pode querer criar um único registro SPF universal e referenciá-lo em domínios individuais usando o mecanismo "include". Certifique-se de que seus registros SPF não sejam muito amplos; Por exemplo, se apenas cinco máquinas em uma rede /24 enviarem SMTP, adicione esses cinco endereços IP individuais ao seu SPF, em vez de toda a rede. Procure que seus registros sejam o mais específicos possível para minimizar as chances de e-mails mal-intencionados comprometerem sua identidade.

Comece com uma opção de falha de software para remetentes não correspondentes ("~all"). Altere-o para hardfail (-all) somente depois de ter 100% de certeza de que identificou **todas** suas fontes de e-mail, caso contrário, você corre o risco de perder e-mails de produção. Mais tarde, depois de implementar o DMARC e executá-lo no modo de monitor por um tempo, você será

capaz de identificar todos os sistemas perdidos e atualizar seus registros SPF para serem concluídos. Somente então será seguro definir o SPF como hardfail.

Passo 3: DMARC

Quando o DKIM e o SPF estiverem configurados o mais completos possível, é hora de criar suas políticas de DMARC. Considere todas as diferentes situações mencionadas nos capítulos anteriores e prepare-se para implantar mais de um registro DMARC se você tiver uma infraestrutura de e-mail complexa.

Crie aliases de email que receberão relatórios ou crie um aplicativo da Web que possa ingeri-los. Não há endereços de e-mail estritamente definidos para serem usados para isso, mas ele ajuda se eles forem descritivos, por exemplo, rua@domain.com, dmarc.rua@domain.com, mailauth-rua@domain.com, etc. Verifique se há um processo em vigor para que um operador monitore esses endereços e modifique a configuração SPF, DKIM e DMARC de forma apropriada, ou alerte a equipe de segurança em caso de campanha de falsificação. Inicialmente, a carga de trabalho será substancial à medida que você ajustar os registros para cobrir qualquer coisa que você tenha perdido durante a configuração de SPF e DKIM. Após alguns instantes, os relatórios provavelmente indicarão apenas tentativas de falsificação.

Inicialmente, defina sua política de DMARC como "none" e sua opção forense para enviar relatórios para qualquer verificação com falha ("fo=1") - isso descobrirá rapidamente quaisquer erros no SPF e no DKIM sem influenciar o tráfego. Quando estiver satisfeito com o conteúdo dos relatórios enviados, altere a política para "quarentena" ou "rejeição", dependendo da sua política de segurança e preferência. Novamente, certifique-se de que você tenha operadores analisando continuamente seus relatórios DMARC recebidos para obter falsos positivos.

Implementar o DMARC completa e corretamente não é uma tarefa pequena ou curta. Embora alguns resultados (e a "implementação" formal do DMARC) possam ser obtidos com a publicação de um conjunto incompleto de registros e de uma política de "nenhum", é do melhor interesse tanto da organização remetente quanto da Internet como um todo que todos o implementem em toda a extensão de seus recursos.

Em relação às linhas do tempo, aqui está um esboço muito detalhado de etapas individuais para um projeto típico. Novamente, como cada organização é diferente, elas estão longe de ser precisas:

1. Planejamento e preparação de DKIM	2 a 4 semanas
2. Execuções de teste de DKIM	2 semanas
3. SPF - identificação legítima do remetente	2 a 4 semanas
4. preparação de política DMARC	2 semanas
5. Execução de teste de registros SPF e DMARC	4 a 8 semanas
6. Execução do teste SPF com hardfail	2 semanas
7. Execução de teste de DMARC com quarentena/rejeição	4 semanas
8. Monitoramento de relatórios DMARC e adaptação de SPF/DKIM de acordo	contínuo

Empresas menores provavelmente terão uma duração menor na maioria das etapas, especialmente nas etapas 3 e 4. Não importa a simplicidade da sua infraestrutura de e-mail, aloque sempre bastante tempo durante as execuções de teste e monitore os relatórios de

feedback com atenção para qualquer coisa que você tenha perdido.

Organizações maiores podem experimentar uma duração ainda maior das mesmas etapas, com requisitos de teste mais rigorosos. Não é raro empresas com infraestrutura complexa de e-mail contratarem ajuda externa, não apenas para o aspecto técnico da implementação da autenticação de e-mail, mas também para gerenciar todo o projeto e coordenar equipes e departamentos.

Referências adicionais

- O site de referência do SPF: http://www.openspf.org
- O Conselho DKIM: http://www.dkim.org
- Site principal do DMARC, executado pelo The Trusted Domain Project: http://www.dmarc.org
- dmarcian - um site de ajuda e recursos administrado por Tim Draegen, um dos autores do DMARC. Visite a seção "Ferramentas": http://www.dmarcian.com
- Ferramenta de validação de registros da Online Trust Alliance: https://otalliance.org/resources/spf-dmarc-record-validator
- Assistente de gravação DMARC - outra ferramenta útil para ajudá-lo a criar seus registros DMARC: http://www.kitterman.com/dmarc/assistant.html
- Ferramentas de Teste de Gravação SPF: http://www.kitterman.com/spf/validate.html
- "Não seja um phish: Mergulhe fundo nas técnicas de autenticação de e-mail", uma apresentação do Cisco Live 2014 BRKSEC-3770: https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=76627

[1] A canonicalização está além do escopo deste documento. Consulte o material na seção "Referências adicionais" para obter mais informações sobre a canonicalização DKIM.

[2] Os parâmetros de registro DKIM DNS também estão fora do escopo deste documento.

[3] A criação de filtros de mensagens está além do escopo deste documento. Consulte os guias do usuário do AsyncOS para e-mail para obter assistência.

[4] A M3AAWG definiu um excelente conjunto de melhores práticas aplicadas e honradas pela maior parte do setor. O documento de melhores práticas comuns para o remetente está disponível em https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Senders_BCP_Ver3-2015-02.pdf

[5] Esse comportamento aproveita o fato de que originalmente, a DKIM não verifica a origem da mensagem como declarado em MAIL FROM ou Header From. Ele só verifica se o parâmetro Signing Domain ID ("d" da assinatura DKIM e o parâmetro "Domain Name" no seu perfil de assinatura) está, de fato, hospedando a chave pública do par usado para assinar a mensagem. A autenticidade do remetente é implícita com a assinatura do cabeçalho "De". Apenas certifique-se de listar todos e todos os domínios (e subdomínios) em que você está conectado na seção "Usuários com perfil".

[6] Normalmente, um nível de domínio abaixo do TLD ou prefixo ccTLD relevante (.ac.uk, .com.sg etc...)