E-mail security

How to use e-mail security features in EXIM SMTP with BIND DNS.

SPF

Sender policy framework uses a DNS text entry within a domain detailing the authorised IP addresses and hosts that can send email for that domain.

BIND

Using the “a” directive, a receiving server will look up the IP4 or IPV6 address of the hostname and match it to the origin for validation.

Zone

```
1H IN TXT "v=spf1 a:HOSTNAME -all"
```

Test

```
dig in txt DOMAIN
```

If more than one source needs to be authorised the “include” directive can be used (refer to RFC 7208).

DKIM

DomainKeys Identified Mail is a signing process used when sending email to determine authenticity and detect tampering on the receiving server.

OPENSSL

Openssl can be used to generate the private signing key and public key published in DNS.

```
#! /bin/bash

rm -f private.pem public.pem public.der

# PEM printable encoding, RFC 7468
openssl genrsa -out private.pem 2048 1>/dev/null 2>&1
openssl rsa -in private.pem -pubout -out public.pem 1>/dev/null 2>&1

# Distinguished Encoding Rules, OPENSSL-FORMAT-OPTIONS(1SSL)
```

```
openssl rsa -in private.pem -pubout -outform der -out public.der 1>/dev/null
2>&1

# DKIM
base64 -w 0 public.der | awk '
{
        print "dkim._domainkey IN TXT (\"v=DKIM1; k=rsa; p=\""
        do {
                printf "\t\"" substr($0, 1, 64) "\""
                $0 = substr($0, 65)
                if (length)
                        printf "\n"
                else
                        print ")"
        }
        while (length)
}'
```

BIND

The sub-domain "_domainkey" is used to provide a "selector" to use with DKIM. In this example the selector is simply "dkim".

Zone

```
dkim._domainkey IN TXT ("v=DKIM1; k=rsa; p="
        "use output from above")
```

The "p" directive contains a base64 encoded public key which can be created by openssl in the previous section.

Test

```
dig in txt dkim._domainkey.DOMAIN
```

The text record format for BIND is explained in RFC 6376.

EXIM

Exim can provide transports which support DKIM selectively. This example will use DKIM signing for a specific domain.

routers

```
dnslookup_dkim_DOMAIN:
 driver          = dnslookup
 domains         = !+local_domains
 condition       = ${if eq{$sender_address_domain}{DOMAIN}}
```

```
 transport       = remote_smtp_dkim_DOMAIN
 ignore_target_hosts = 0.0.0.0:127.0.0.0/8
 no_more
```

transports

This transport signs the message using the private key and indicates which selector should be examined on delivery in DNS.

```
remote_smtp_dkim_DOMAIN:
 driver           = smtp
 helo_data        = HOSTNAME
 interface        = <;IPV4;IPV6
 dkim_domain      = DOMAIN
 dkim_selector    = dkim
 dkim_private_key = /etc/exim4/private.pem
```

For SPF the HOSTNAME must resolve to the specified IP address(es).

The DKIM domain needn't be the same as the sender domain.

DMARC

DMARC defines a policy and reporting facility for e-mails.

E-mails that fail SPF and DKIM tests may be processed according to this table.

Policy	Effect
none	Mail delivered normally
quarantine	Mail delivered to spam folder
reject	Mail rejected and not delivered

For reporting, providers such as google send details of e-mails that pass and fail. For google the reports originate from noreply-dmarc-support@google.com.

BIND

The simplest policy is to do nothing with failed e-mails, this can be used to determine if the feature is working before applying stricter rules which can tell a receiver to reject or quarantine.

Zone

```
_dmarc IN TXT "v=DMARC1; p=none; rua=mailto:postmaster@DOMAIN"
```

Once you are confident that you are sending e-mail from the correct server(s) in with the correct signature(s) then the policy can be made more strict.

Test

```
dig in txt _dmarc.DOMAIN
```

See RFC 7489 for more information.

Resources

DKIM validator

Export

PDF