

DMARC-Training

PATRICK BEN KOETTER <P@SYS4.DE>

2022-08-30

SPF-Policies

Host

Allow IPv4 for your host and tempfail everything else

Host: Solution

```
"v=spf1 ip4:164.92.150.174/32 ~all"
```

Send test message

```
swaks -t switch-training@sys4.de -s 127.0.0.1 \  
-f user@zNN.dane.onl
```

Border Filter

Additionally allow `2001:DB8::/128` and `192.0.2.1/32`

Border Filter: Solution

```
"v=spf1 ip4:164.92.150.174/32 ip4:192.0.2.1/32  
ip6:2001:DB8::/128 -all"
```

Email Service Provider / Subdomain

ESP is a third party that provides additional email services for your domain.

Include

Include SPF-Policy from `_spf.sys4.de` to your Border Filter Policy

Include: Solution

```
"v=spf1 ip4:164.92.150.174/32 ip4:192.0.2.1/32  
ip6:2001:DB8::/128 include:_spf.sys4.de -all"
```

Delegation

Redirect to SPF-Policy from `_spf.sys4.de`.

Delegation: Solution

```
"v=spf1 redirect:_spf.sys4.de"
```

DKIM-Signing

Creating key material

- Use `223012-rsa` and `223012-ed25519` as selector
- Use `rspamadm` to create key material for **RSA** and **Ed25519**

Creating key material: Solution

```
rspamadm dkim_keygen -s '223012-rsa' -b 2048 \  
-d zNN.dane.onl \  
-k /etc/rspamd/dkim/zNN.dane.onl-rsa.private \  
> zNN.dane.onl-rsa.txt
```

```
rspamadm dkim_keygen -s '223012-ed25519' -t ed25519 \  
-d zNN.dane.onl \  
-k /etc/rspamd/dkim/zNN.dane.onl-ed25519.private \  
> zNN.dane.onl-ed25519.txt
```

Publishing the public key in a ZONE

- Publish keys in your DNS zone
- Specify a **TTL** of 30 seconds

Publishing...: Solution

```
223012-ed25519._domainkey 30 IN TXT ( "v=DKIM1; k=ed25519; "
"p=35i+rTUcpfuG6BLJ8/oNA7TI1ZMpgpoeEQGaew+OK+4=" ) ;
```

```
223012-rsa._domainkey 30 IN TXT ( "v=DKIM1; k=rsa; "
  "p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA \
  9SDP3XaWSBErIT0XIVXFXLY2wi4FTj8cbcEXKBNIK+uwObi \
  +ucBT2vg7mH/IOM9TjJlph+mjHyNFzQZXslj/upsw/QxRMq \
  GAKxequbNioeGXKp9fWsNCDiinSz/1E5hAGtBdkriUKJSG+ \
  wiVF/XerTzofHiemYTwfhxUgr/ngBl/griBwx00j0SIGtSo \
  wmtux3QVTFWZytxBDpaI4"
  "ph6vZC3qB8GH5exK0E1TpYGm/emXoPiPzhfExsCbXkmBrg \
  1tp0Gm9M7tsmGDb0tqg1PV4VdU01Ggkz3JZyjgauQwrcdUf \
  WCOwLoN0MreBxelwTkAHgKFbw+xvFE7ME/Pg02MwIDAQAB"
) ;
```

Enable DKIM-Signing

- Use keys and `223012-rsa` and `223012-ed25519` as selector
- Edit `/etc/rspamd/local.d/dkim_signing.conf`
- Add keys and selectors to your subdomain

Enable DKIM-Signing: Solution

```
domain {
  zNN.dane.onl {
    selectors [
      {
        path: "/etc/rspamd/dkim/zNN.dane.onl-rsa.private";
        selector: "223012-rsa";
      },
      {
        path: "/etc/rspamd/dkim/zNN.dane.onl-ed25519.private";
        selector: "223012-ed25519";
      },
    ]
  }
}
```

Send test message

```
swaks -t switch-training@sys4.de -s 127.0.0.1 \  
-f user@zNN.dane.onl \  
--header 'From: Tessi Testinger <user@zNN.dane.onl>'
```

DMARC

DMARC-Policy

- Add a DMARC policy to your subdomain
- Set the policy to **none**
- Request Aggregate Reports for `dmARC@zNN.dane.onl`

DMARC-Policy: Solution

```
dig +short TXT _dmarc.zNN.dane.onl  
"v=DMARC1; p=none; rua=mailto:dmarc@zNN.dane.onl"
```

Verifying a DMARC-policy

```
swaks -t switch-training@sys4.de -s 127.0.0.1 \  
-f user@zNN.dane.onl \  
--header 'From: Tessi Testinger <user@zNN.dane.onl>'
```

Sunsetting a Maildomain

Set a Null-MX-Record for (sub)domain:

Null MX

```
example.com.          IN  MX  0  .
```

Sunsetting (continued...)

Set a negative SPF Record:

```
"v=spf1 -all"
```

Set a DMARC reject and report policy:

```
dig +short TXT _dmarc.zNN.dane.onl  
"v=DMARC1; p=reject; rua=mailto:dmarc@zNN.dane.onl"
```

Questions?