

SMTP

MX

MX **Mail Exchange** MX

MX

MX

```
└─(root kali)-[/opt/spoofcheck]
└─# dig MX qq.com +short
20 mx2.qq.com.
30 mx1.qq.com.
10 mx3.qq.com.

└─(root kali)-[/opt/spoofcheck]
└─# host -t MX qq.com
qq.com mail is handled by 20 mx2.qq.com.
qq.com mail is handled by 30 mx1.qq.com.
qq.com mail is handled by 10 mx3.qq.com.
```

SPF

SPF **Sender Policy Framework**

DNS

<https://emkei.cz/>

SPF A_Company Career
B_Company @acompany

noreply@acompany.com

SPF

```
v=spf1 ip4:209.225.8.0/24 ip4:209.225.28.0/24 ip4:24.196.48.42/32 ip4:24.217.29.16/32
ip4:24.176.92.28/32 ip4:142.136.234.128/27 ip4:142.136.235.128/27
include:et_spf.pardot.com include:spf-c.usa.striata.com include:everbridge.net ~all
```

IP

“ ”

<https://mxtoolbox.com/SuperTool.aspx>

SPF

SuperTool Beta7

charter.com

SPF Record Lookup

spf:charter.com

Find Problems

Solve Email Delivery Problems

spf

v=spf1 ip4:209.225.8.0/24 ip4:209.225.28.0/24 ip4:24.196.48.42/32 ip4:24.217.29.16/32 ip4:24.176.92.28/32 ip4:142.136.234.128/27 ip4:142.136.235.128/27 include:et_spf.pardot.com include:spf-c.usa.striata.com incl

Prefix	Type	Value	PrefixDesc	Description
	v	spf1		The SPF record version
+	ip4	209.225.8.0/24	Pass	Match if IP is in the given range.
+	ip4	209.225.28.0/24	Pass	Match if IP is in the given range.
+	ip4	24.196.48.42/32	Pass	Match if IP is in the given range.
+	ip4	24.217.29.16/32	Pass	Match if IP is in the given range.
+	ip4	24.176.92.28/32	Pass	Match if IP is in the given range.
+	ip4	142.136.234.128/27	Pass	Match if IP is in the given range.
+	ip4	142.136.235.128/27	Pass	Match if IP is in the given range.
+	include	et_spf.pardot.com	Pass	The specified domain is searched for an 'allow'.
+	include	spf-c.usa.striata.com	Pass	The specified domain is searched for an 'allow'.
+	include	everbridge.net	Pass	The specified domain is searched for an 'allow'.
~	all		SoftFail	Always matches. It goes at the end of your record.

1 SPF

SPF

v=spf1 ip4:113.110.223.0/24 183.110.226.0/24 183.110.255.0/24 59.110.132.0/24 -all

ip4

2

SPF

SPF

3

SPF

4 DNS

5

SPF ()

```

r—(root kali)-[ /opt/spoofcheck]
l—# host -t txt xx.com | grep spf
qq.com descriptive text "v=spf1 include:spf.mail.xx.com -all"

```

```

r—(root kali)-[ /opt/spoofcheck]
l—# dig TXT +short xx.com

```

```
"v=spf1 include:spf.mail.xx.com -all"
```

DKIM

Domain Keys Identified Mail DKIM DNS DNS

DNS Host name (TXT record name):

google._domainkey

TXT record value:

```
v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCrvLQjRjQjcXK3X80i7RZYP6J5OGTY8u2pzT
oK8QnCNevMLrz315VV6SHTL8MZuJhbHvwiLCTsq8I8T/GCZvc4KKIfvmD9sJ6mcUWVZvVCd1UDR
WVfF3RRaBwqUjG44SscUVb8k0Fihy174dYrOwd08CqEdGZE8wYjNIhN1jOfOwIDAQAB
```

DMARC

Domain-based Message Authentication, Reporting, and Conformance DMARC SPF
(SPF DKIM) DMARC

```
DMARC: v=DMARC1; p=quarantine; sp=none; aspf=r; adkim=r; pct=100;  
rua=mailto:dmarcAR@abc.com;
```

100%) SPF ~~relaxed~~ () dmarcAR@abc.com DMARC DMARC DMARC

```
└─(root kali)-[/opt/spoofcheck]
└─# dig _dmarc.xx.com TXT +short
"v=DMARC1; p=quarantine; rua=mailto:mailauth-reports@xx.com"

└─(root kali)-[/opt/spoofcheck]
└─# host -t txt _dmarc.xx.com | grep DMARC
_dmarc.xx.com descriptive text "v=DMARC1; p=quarantine; rua=mailto:mailauth-reports@xx.com"
```

Revision #7

Created 20 February 2023 15:22:00 by

Updated 21 February 2023 00:23:24 by