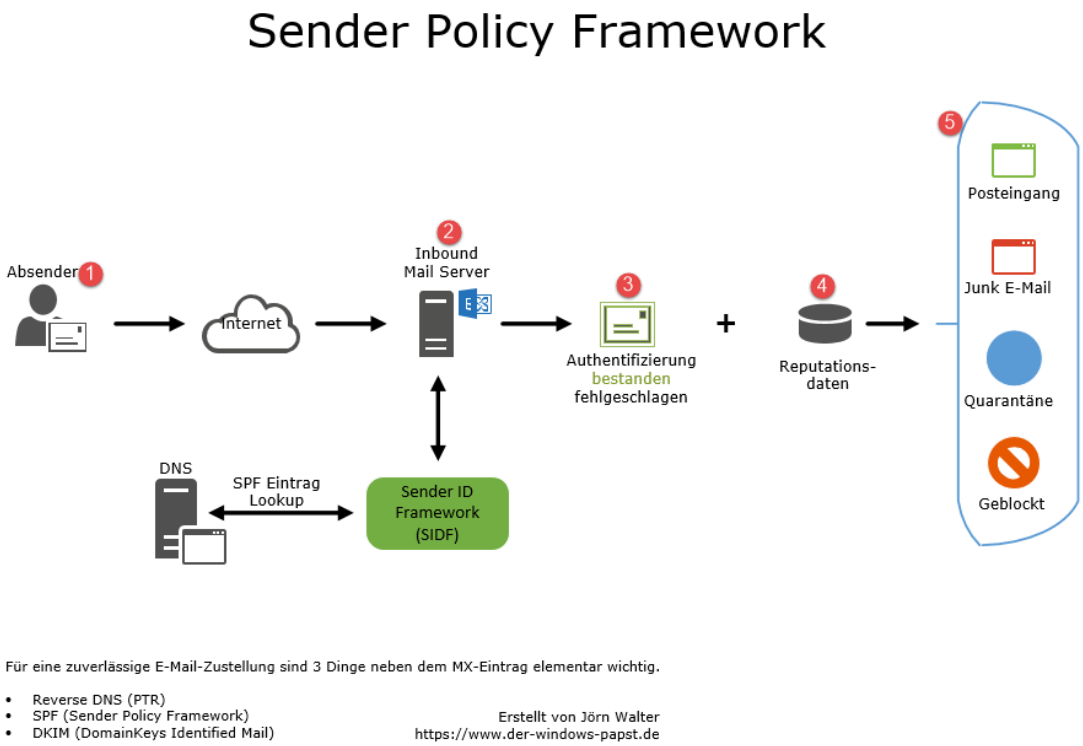
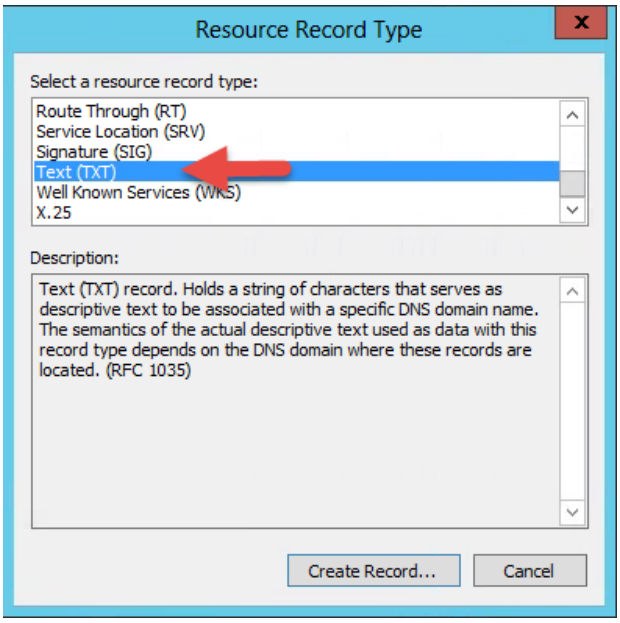


Das SPF (Sender Policy Framework) ist ein Verfahren zur Sender-Authentifizierung und räumt dem empfangenden Mailserver die Möglichkeit ein, zu überprüfen, ob die E-Mail tatsächlich von einem berechtigten Mailserver (Absender) stammt oder nicht. Der Domaininhaber bestimmt durch einen Eintrag in seiner DNS Zone wer als valider Absender infrage kommt.

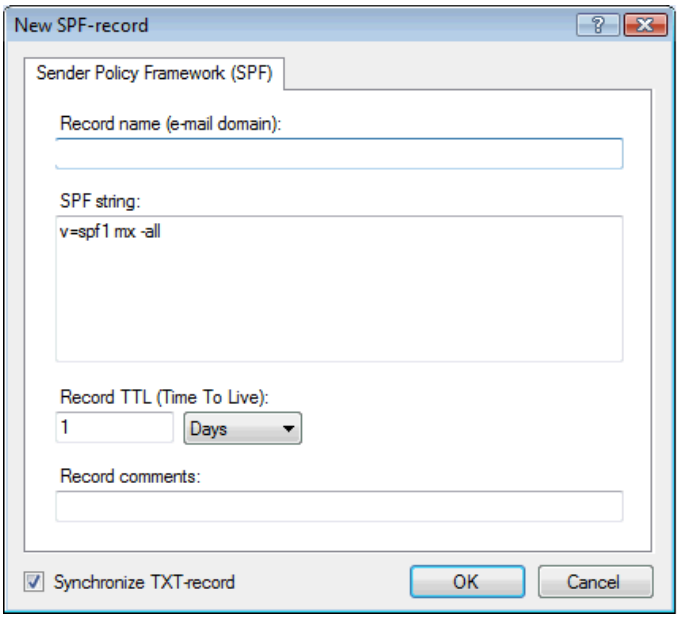
Hinweis: Ein SPF schützt nicht vor Spam.

Früher reichte es aus einen einfachen TXT Eintrag zu setzen.



Sender ID Framework (SDIF)

Seit der Standarisierung gibt es zusätzlich im DNS einen eigenen „Type".

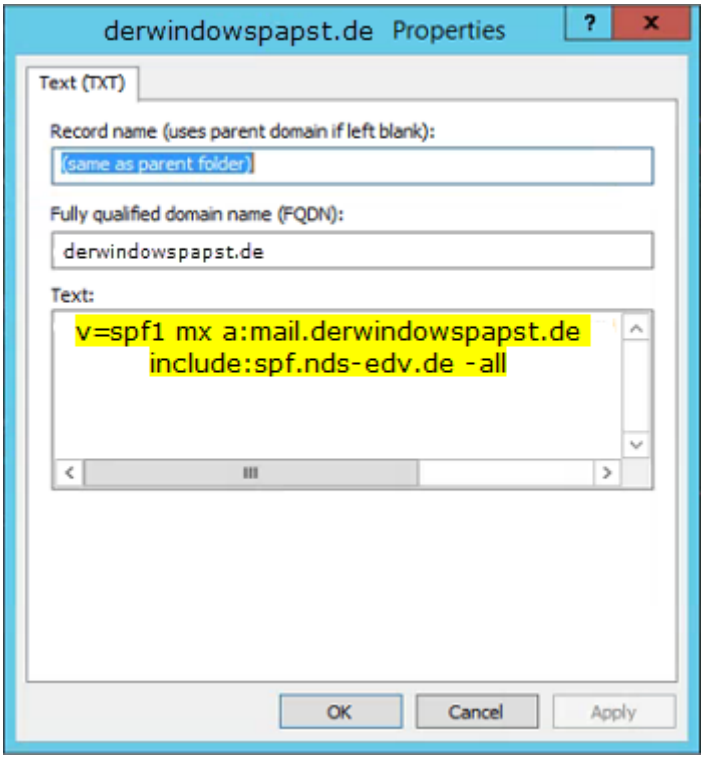


Die Einträge unterscheiden sich von der Syntax aber nicht.

Hier ein Beispiel:

Mit diesem Eintrag erlaube ich dem Absender nds-edv.de in meinem Namen E-Mails zu versenden. Gerade dann wichtig, wenn eine Agentur (flexmail.eu) in meinem Namen Werbung oder Serienbriefe versenden soll.

v=spf1 mx a:mail.derwindowspapst.de include:spf.nds-edv.de –all
v=spf1 mx a:mail.derwindowspapst.de include:spf.flexmail.eu include:nds-edv.de -all



Sender ID Framework (SDIF)

Kurz erklärt:

Erklärung: „v=spf1 mx -all“

v=spf1	beschreibt den SPF Type = 1, zur Zeit gibt es nur den einen
mx	legt fest, dass die IP des Absenders mit der IP des MX der Domain übereinstimmen muss.
a	steht für die aktuelle Domäne
-all	das -all ist eine Anweisung alle nicht aufgeführten Mailserver auszuschließen.

Der erste Mailserver ist mein eigener und der andere (include) Mailserver wird entsprechend berechtigt im Namen der Domain derwindowspapst E-Mail senden zu dürfen.

Setzen wir den Eintrag ohne include „v=spf1 mx a:mail.derwindowspapst.de –all“ gilt es nur für die aktuelle Domäne.

Worauf ist zu achten?

Wenn E-Mails von Exchange A Domäne X nach Exchange B Domäne Y weitergeleitet werden, ist eine Überprüfung der Übereinstimmung nicht mehr möglich. In diesem Fall würden die E-Mails wegen der fehlgeschlagenen Überprüfung verworfen werden.

SPF Checker:

http://www.openspf.org/Why

Sender ID Framework (SDIF)

Für eine zuverlässige E-Mail-Zustellung sind 3 Dinge neben dem MX-Eintrag elementar wichtig.

- Reverse DNS (PTR)
- SPF (Sender Policy Framework)
- DKIM (DomainKeys Identified Mail)

Reverse DNS (PTR):

Ein rDNS (PTR) macht genau das Gegenteil eines DNS-A Eintrags, er löst die IP wieder in einen Namen auf. Ohne einen gültigen rDNS Eintrag werden viele ISPs (Internet Service Provider) E-Mails blockieren.

Konventionelle DNS-Auflösung:
www.der-windows-papst.de **>** 217.160.2.251

Reverse DNS-Auflösung:
www.der-windows-papst.de **<** 217.160.2.251

PTRs werden in der Regel vom ISP gesetzt. Ein PTR Eintrag ist eine 1:1 Zuordnung zum Domänen Eintrag. Sollte im Header einer E-Mail die interne IP-Adresse stehen, so ist der PTR Eintrag zu kontrollieren.

SPF (Sender Policy Framework):

Wie oben bereits beschrieben, ist der SPF-Eintrag entweder ein TXT-Typ-Eintrag oder nach dem Standard ein SPF-Typ-Eintrag, der angibt, welche Server E-Mails im Namen einer Domäne senden dürfen.

Hier die Erklärung zum obigen Bild:

1. Der Absender (flexmail.eu) versendet eine E-Mail in meinem Auftrag
2. Der empfangende E-Mail Server nimmt die E-Mail an und prüft ob es zum Absender (flexmail.eu) einen gültigen SPF Eintrag im DNS Eintrag von derwindowspapst.de gibt.
3. Ist das Ergebnis „bestanden" oder „fehlgeschlagen
4. entscheidet der Filter
5. ob die E-Mail zugestellt oder blockiert wird

Sender ID Framework (SDIF)

DKIM (DomainKeys Identified Mail):

DKIM arbeitet auf Basis eines privaten Schlüssels. Jede E-Mail Nachricht wird mit einer digitalen Signatur versehen. Der empfangene Server prüft den DNS Eintrag des Absenders, ob dort der öffentliche Schlüssel der Signatur hinterlegt ist. Ist das Ergebnis positiv, so geht der Mailserver davon aus, das die E-Mail nicht manipuliert wurde und stellt diese dem Empfänger zu.

Beispiel für einen DKIM DNS Datensatz:

Default._domainkey.derwindowspapst.de. 1800 IN TXT
"v=DKIM1;k=rsa;p=MIGfMA0GCSqGSIb3DQEBAQUAA3GNADCBiQKBgQC/VMzpi2yfvnzVX
CzPawWRC5LtnlzD0f7a3
/NI+oDfxiBAOlVISxps7sv0UPBK1D+rJAhCt4KB+eJcTFtEgXVWQmUMQLcAEHSwHHlbmZd3
B8fMs4jYaoeJfPIy1bB0cZ1zh95dOfcMD8QFDsRlVFjrmwanvqOaJZ4FtkbfqZe5hQIDAQAB"