Proofpoint Hosted Sender Policy Framework

Proofpoint Hosted Sender Policy Framework (SPF) is a DNS service that is available to customers of Proofpoint Email Fraud Defense. It leverages the advanced macro query provisions of the SPF standard. This allows for complex SPF records that the largest enterprise customers require. The service overcomes many of the challenges or limitations involved with determining who may and may not send for a given envelope domain.

Definition and value

SPF CHALLENGE OR LIMITATION	HOSTED SPF SOLUTION
SPF query performance	Geolocation-based DNS query routing improves service resiliency
Authorized senders visible to bad actors	Authorized senders hidden from bad actors
Risk of excessive permissiveness	Tight controls around sender permissions
DNS change control lead time	Near real-time updates
Limited number of allowed SPF includes	Support for SPF macro DNS queries to remove limit of 10 lookups

Specifications

FEATURE	DESCRIPTION
Customer portal	Easy-to-use interface for permitting and revoking sender rights
User security	Unique username and strong password
User rights	Configurable at both product and Proofpoint level (federated credential)
Multifactor authentication	Option to enforce MFA via customer's Identity Provider (IDP)
SPF mechanisms supported	IP, CIDR, include, A, MX, exists
SPF mechanisms not supported	PTR[1]
Protocol and port	UDP over port 53
Worldwide distributed hosting	Multiple Amazon Web Services (AWS) locations in the United States and European Union
Network access control	AWS Network Access Control
Application access control	AWS Identity and Access Management
DNS service redundancy	Local and regional redundancy
Load balancing	Amazon Network Load Balancer and Geoproximity DNS query routing
Monitoring	24/7/365 proactive monitoring

1 Per the SPF RFC (https://tools.ietf.org/html/rfc7208), including PTR references in SPF records is discouraged as it is "unnecessary and more reliable alternatives should be used instead."

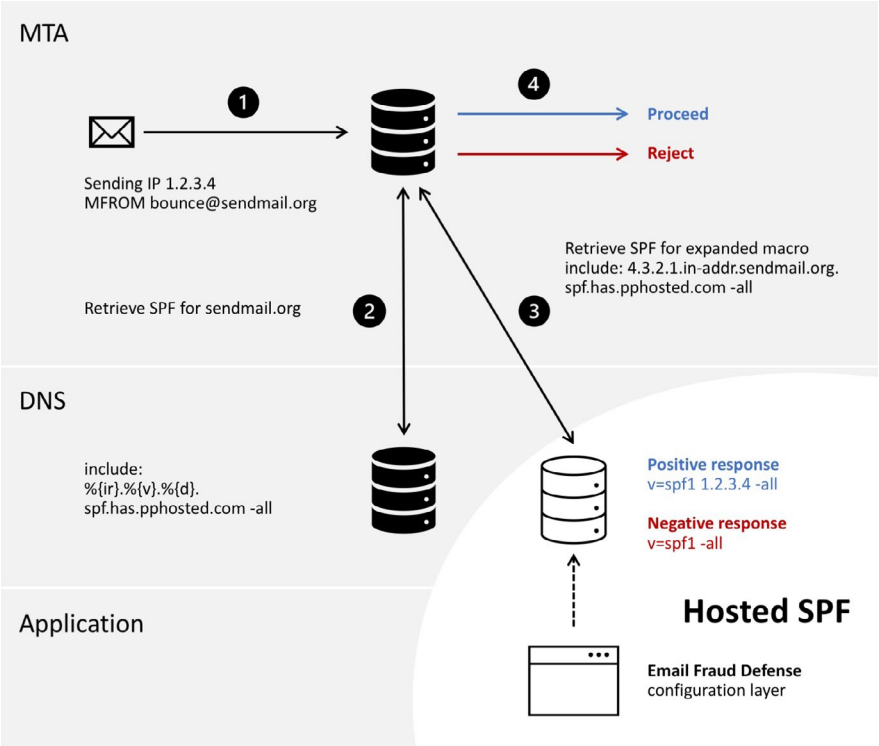

Figure 1: How Proofpoint Hosted SPF works.

High availability

Proofpoint Hosted SPF's architecture is redundant and scalable. So it operates at the highest levels of availability. In the unlikely event service is disrupted, failover to a different service location is automatic and seamless. Beyond SPF, DNS caching and message inspection can also offset the risk of legitimate email not being delivered.[2]

For more information, contact your account manager.

2 The exception to this is email sent from domains that have DMARC p=reject policies that are not signing and aligning with DKIM. Proofpoint discourages this behavior. In this unlikely situation, legitimate email may be blocked.

LEARN MORE

For more information, visit **proofpoint.com**.